Chapter 9
Full-Duplex Transceivers for Defense and Security Applications

Karel Pärlin and Taneli Riihonen

Abstract The full-duplex (FD) radio technology that promises to improve the spectral efficiency of wireless communications was, however, initially used in continuous-wave (CW) radars by means of same-frequency simultaneous transmission and reception (SF-STAR). In this chapter, we explore how the recent advances in the FD technology, which have been mainly motivated by higher throughput in commercial networks, could in turn be used in defense and security applications, including CW radars and also electronic warfare (EW) systems. We suggest that, by integrating tactical communications with EW operations such as signals intelligence and jamming, multifunction military full-duplex radios (MFDRs) could provide a significant technical advantage to armed forces over an adversary that does not possess comparable technology. Similarly in the civilian domain, we examine the prospective benefits of SF-STAR concepts in security critical applications in the form of a radio shield.

9.1 Introduction

In contrast to classical half-duplex (HD) wireless communication models that divide transmission and reception in either time or frequency domain, full-duplex (FD), or otherwise referred to as same-frequency simultaneous transmit and receive (SF-STAR), has the potential to double the spectral efficiency of wireless communications by not requiring such division. In addition to the significant benefits that SF-STAR is capable of delivering in terms of increased throughput in commercial wireless networks, it also has potential uses in defense and security applications [1, 2]. Indeed, the first use of SF-STAR actually emerged from the defense domain in

K. Pärlin (✉)
Rantelon, Tallinn, Estonia
e-mail: karel.parlin@rantelon.ee

T. Riihonen
Unit of Electrical Engineering, Tampere University, Tampere, Finland
e-mail: taneli.riihonen@tuni.fi

H. Alves et al. (eds.), *Full-Duplex Communications for Future Wireless Networks*,
https://doi.org/10.1007/978-981-15-2969-6_9

the form of continuous-wave (CW) radars, which have been studied since at least the 1940s [3].

In order to receive echoes from targets simultaneously to transmitting, CW radars require the near-end local leakage, i.e., self-interference (SI), to be reduced similarly to FD wireless communication systems. This had initially been achieved by using separate antennas or circulators in single-antenna systems [3]. Such passive methods, however, provide only moderate isolation which consequently restricts the usable transmission power. In order to increase the radar's working range by amplifying the output power while also limiting the SI, active SI cancellation methods using analog circuitry were developed based on feed-through nulling which attenuated the SI by as much as 60 dB [4]. To potentially double the spectral efficiency in wireless networks, FD radio technology has from thereon evolved to yield wideband SI suppression of up to 100 dB through combination of passive and active methods.

These advances have been recognized by NATO's Science and Technology Organization as its exploratory team has recently completed its report that focuses on how the FD technology can alleviate spectral congestion issues in tactical communications [5, 6]. The report also identifies possible applications in electronic warfare (EW). Most notably, SF-STAR could deliver a paradigm shift in military communications by merging tactical communications with simultaneous electronic attack and defense capabilities, therefore enabling the spectrum resources to be used based on operational circumstances rather than technological limitations. However, a different set of requirements, such as operating frequencies and transmission powers, needs to be considered when designing military radios as opposed to commercial applications, for which the FD radio prototypes have been mostly developed.

Similarly to the potential paradigm shift in military communications, the FD technology can also become central to the security of civilian wireless communications. For example, in the form of a radio shield, simultaneous wireless reception and jamming could be used to prevent eavesdropping on wireless corporate or body area networks. Moreover, the radio shield could be used to prevent unauthorized usage of the radio spectrum to, e.g., restrict remotely controlled unmanned aerial vehicles (UAVs) from entering the airspace covered by the shield. In the security domain, an outstanding challenge is to introduce new capabilities while not requiring any changes to the legacy communication standards. Transferring the FD radio technology from its current state to the military and security domains therefore requires careful planning on how to benefit from SF-STAR operation but also on what are the technical prerequisites for applying FD technology in these domains.

The remainder of this chapter is organized as follows. In Sect. 9.2, we discuss the challenges in transferring the FD technology from its current civilian/commercial state to the military domain and the prospective applications of multifunction military full-duplex radios (MFDRs) in both communication and non-communication systems. In Sect. 9.3, we identify possible security applications of the FD radio technology in commercial systems in the form of a radio shield and briefly reflect

on the relation to the information-theoretic physical layer security aspects. Finally, Sect. 9.4 concludes the chapter.

9.2 Applications for Full-Duplex Radios in Military Communications

Most of the ongoing FD research focuses on improving SI cancellation methods, studying the physical layer security aspects from an information-theoretic viewpoint, or developing scheduling and routing algorithms that can leverage the SI cancellation for commercial applications by improving spectral efficiency. Unlike commercial systems, however, their military counterparts are required to perform in adverse propagation environments and hostile conditions. Such circumstances place generally more rigorous requirements on the radios but also present new applications for the FD technology in the form of MFDRs, including those illustrated and categorized in Figs. 9.1 and 9.2, respectively.

In the following, we first discuss the requirements for military radios in general and also from the viewpoint of the FD radio technology in particular. We then consider the advantages of MFDR radios over conventional HD military radios in combinations of tactical communications with EW and also in tactical communica-

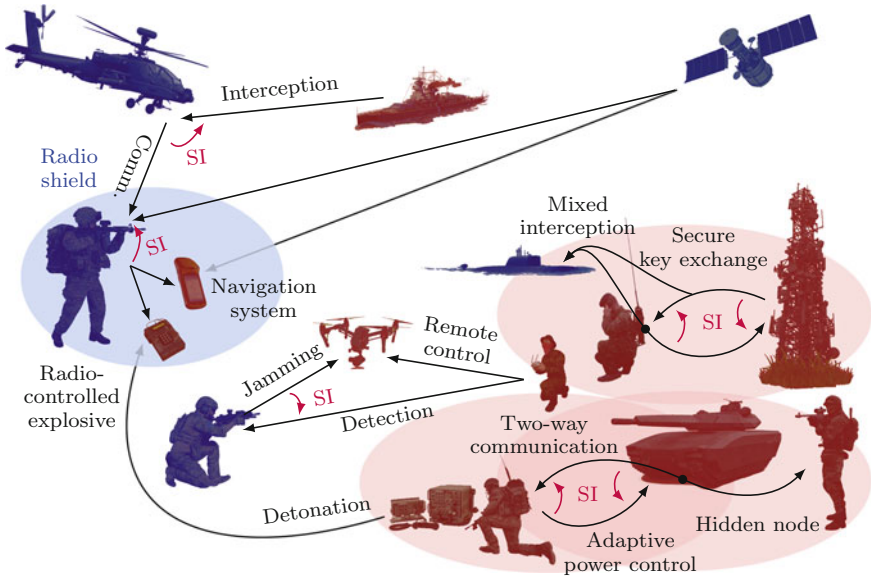

Fig. 9.1 Conceptual use of military full-duplex radios in the battlefield for communications and electronic battle. Self-interference is abbreviated as SI. © [2018] IEEE. Reprinted, with permission, from [2]

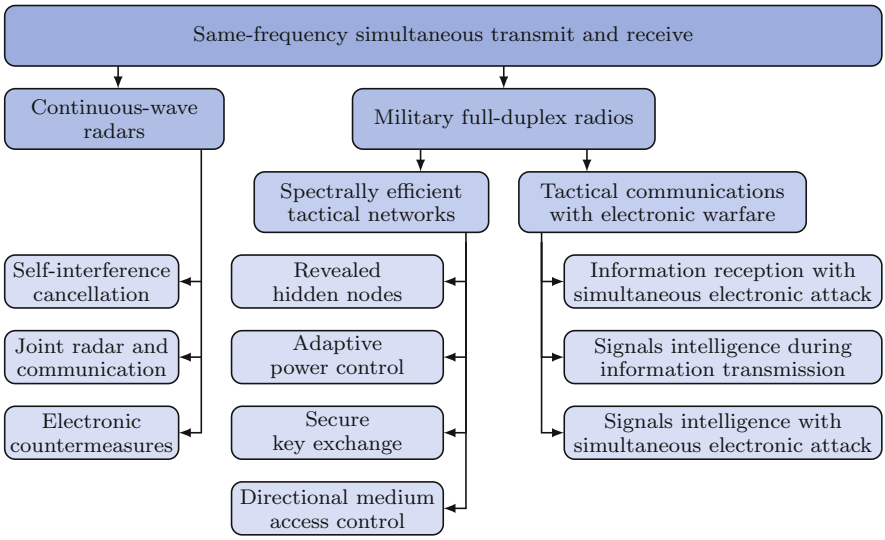

Fig. 9.2 Same-frequency simultaneous transmit and receive applications in the military domain

tion networks. We also present an overview of CW radars and multifunction radios together with potential uses of the FD radio technology in those applications.

9.2.1 Requirements for Military Radios

Typically military radios share the physical and electromagnetic (EM) environment with radars, EW applications, and navigation systems. Not to mention the interference from adversarial radio systems that further congest the EM spectrum. The environment, in which military radios are required to operate, therefore imposes considerable limitations to providing host forces the use of EM spectrum and at the same time preventing the adversary from doing likewise [7]. Military radios need to use the spectrum efficiently to fulfill the communication needs without compromising the reliability requirements [8]. By taking advantage of the recent advances in FD radio technology and SI cancellation in particular, spectral efficiency in military radios can possibly be improved.

However, so far most of the FD prototypes have been designed with commercial applications in mind. Main differences between military and civilian radios, in addition to the operating conditions, arise from the used frequency bands. Typically military radios operate in the very high frequency (VHF) or high frequency (HF) bands whereas nearly all academic FD prototypes demonstrate SI cancellation in the upper ultra high frequency (UHF) bands only. Additional studies are needed to confirm the feasibility of FD radios at military frequencies, but also at higher

transmission powers. Military radios can require much higher output powers than what has been proven usable in laboratory environments so far. Moreover, the inherent mobility of tactical units requires the radio's size, power consumption, and weight to be kept at minimum while other requirements include the need for higher bandwidth, lower latency, and security [8].

The security considerations in military radios are of paramount importance not only to their operation, but also to the integrity and survival of the physical systems that they support [9]. Hence it is desirable for military radios to have low probability of detection (LPD), low probability of interception (LPI), good jamming resistance, and means to obfuscate the communicated information from potential eavesdroppers. Classically, LPD, LPI, and jamming resistance have been achieved by the use of spread spectrum techniques and adaptive power control [10] while intelligence is typically obfuscated through the use of encryption, which relies on secure key exchange protocols and the adversary's limited computing power [11]. In addition to protecting one's own communications, hindering the enemy's radio correspondence is an important aspect to consider in the electronic battlefield.

Hostile operating conditions not only affect the point-to-point links between military radios but also impose stringent requirements on the networks in which those radios operate. Tactical networks have highly time-variant topologies and are expected to work in a self-forming, self-healing, infrastructure-less manner without sacrificing data rate, latency, nor node mobility. Such requirements have motivated the design of decentralized routing and scheduling protocols, which can in turn be enhanced by the FD radio technology. Still, developing cognitive algorithms that comprise of power control, spectrum management, electronic combat tasks, and network topology adjustment for tactical networks is one the most challenging aspects of designing radios for future military communications [12].

9.2.2 Tactical Communications with Electronic Warfare

In the military domain, EW provides means to oppose and resist hostile actions that involve the EM spectrum in all battle stages. It is an important avenue in advancing desired military objectives or, on the contrary, hindering undesired ones and improving the survivability of the host force [7]. Effective use of EW countermeasures relies on signals intelligence and reconnaissance while EW as a whole consists of the following interrelated operational functions:

- electronic attack (EA), which involves the offensive use of EM energy to reduce the enemy's battle capabilities;
- electronic protection (EP), which protects the host forces from the opponent's EAs through EM countermeasures;
- electronic support (ES), which combines surveillance and reconnaissance of the EM environment in order to provide information for EA and EP.

Classically, EW functions have been separated from tactical communications in time or frequency domain, so that the host forces' use of the EM spectrum for tactical communication is not obstructed. However, use of the SF-STAR capability in military radios would not only enable spectrally efficient two-way information exchange but also allow armed forces to merge tactical communications with EW and so introduce novel combat tactics. Through such combinations, the radios could either receive or transmit communication signals while at the same time conducting EW tasks in the opposite direction. As the pioneering works dedicated to exploring the potential benefits of MFDRs, [1, 2] provide insight into such combinations and how they could present armed forces with a significant technical advantage over an adversary that does not possess comparable technology. In the following, we consider those combinations in detail.

9.2.2.1 Simultaneous Communication and Jamming

Deploying EW systems, such as jammers, against radio-controlled (RC) improvised explosive devices (IEDs) or UAVs, can significantly help in protecting the personnel and platforms from those threats. However, jammers can inadvertently interfere with the host's communication systems that operate in the close vicinity [13]. Suppressing the EM interference in the communication systems caused by jamming is therefore a crucial challenge with high technical complexity and operational significance. Ordinarily, frequency-based separation with fixed filters or time division is used to alleviate the EM interference. Such methods, however, limit the spectral efficiency and, in case of frequency-division duplexing, require duplex filters to be changed in accordance to the environment and threats. Whenever jamming is carried out alternately in time with tactical communications, it presents the opponent with similar possibilities to use the EM spectrum. This results in inefficient use of the EM spectrum and can severely limit the efficiency of the EA.

It is therefore desirable to enable simultaneous same-frequency communication and jamming [13], which is exactly what recent advances in SI cancellation facilitate. The cancellation techniques allow a FD transceiver to simultaneously transmit a jamming signal and receive tactical communication signals on the exact same frequency, therefore preventing opponents in the FD transceiver's proximity from using the frequency band. Numerical results in [1] illustrate the gain margins which tactical forces could therefore achieve. Mitigation of in-band interference from co-located jammers through SI cancellation techniques at the communication system's receiver has been demonstrated to enhance the reception of signals of interest [14]. Such jamming could be used to block the enemy from detonating radio-controlled IEDs or operating UAVs while the host could still receive communications from allied forces. Another conceivable use case in the battlefield would be to jam or spoof the adversaries' reception of navigation satellite system signals while itself retaining the ability to receive such signals and consequently the positioning capabilities.

9.2.2.2 Simultaneous Interception and Communication

Similar to the above case, FD radio technology makes it also possible to combine signals intelligence with tactical communications. Compared to the combination of communication with jamming, this is a somewhat different task because communication systems' transmitters usually do not use as high output power as jammers. Therefore, the integration of current SI cancellation techniques to MFDRs could already suffice to achieve simultaneous interception and communication, given that those techniques can be transferred from the UHF to HF and VHF bands. Such combination would facilitate devices which perform spectrum monitoring and signal surveillance to, e.g., transmit the gathered intelligence to other tactical units without compromising the surveillance capabilities during transmission. Otherwise, when considering conventional HD radios that carry out surveillance and communications at the same frequency in an alternating pattern in time, the opponent would have a chance of hiding its communications by transmitting at the same time as the signal intelligence unit. It has been highlighted in [1] that performing simultaneous interception with information transmission does not degrade the host's communication link and therefore the interception comes almost at no cost if the transceiver has effective SF-STAR capability.

9.2.2.3 Simultaneous Interception and Jamming

Although not strictly a combination of tactical communications and EW, simultaneous interception and jamming can, e.g., be used to degrade the quality of a communication link between adversaries which is at the same time being intercepted. Reduction in communication link quality can lead the opponents to inadvertently increasing their transmission power in order to sustain the communication link. By carefully choosing the jamming power, it is therefore probable that the interception quality becomes better with simultaneous jamming despite the residual SI as a result of the opponent's countermove [1]. The feasibility of such strategy has already been demonstrated in a laboratory environment by successfully degrading the opponent's reception quality while retaining the ability to intercept it [15].

On the other hand, being able to receive and analyze the targeted communication link under jamming allows one to adapt the jamming waveform to the targeted signals. For example, *a priori* knowledge about UAV remote control systems has been shown to aid in designing effective jamming signals against those systems [16]. Instead of requiring the jammer to have the knowledge beforehand, similar effect could be achieved by gathering such knowledge while jamming through the use of SF-STAR. This would be especially beneficial against systems for which the reaction to jamming cannot be anticipated or known in advance. Thus, replacing conventional jammers which either transmit a wideband jamming signal or alternate between monitoring and jamming stages. Furthermore, by using such target aware jamming, it can become much more difficult for the opponent to detect that it is being jammed [17].

9.2.3 Tactical Communication Networks

Tactical communications in the battlefield result in highly time-varying topologies and typically ad hoc networks, such as the packet radio network (PRN) and mobile ad hoc network (MANET), are considered suitable for connecting tactical units. Ad hoc networking aims to provide a flexible method for establishing communications in scenarios that require rapid deployment of survivable and efficient dynamic networking [18]. Furthermore, ad hoc networks are attractive because they do not require infrastructure and tactical operations often take place in locations where infrastructure is lacking [19], or rendered inaccessible. Tactical MANETs are expected to provide completely self-forming, self-healing, and decentralized platforms for tactical units to join and leave swiftly.

Aside from the dynamic topologies, tactical networks typically also require LPD and LPI. To achieve that, impulse PRNs have been considered because impulse radios' ultra-wideband spectrum usage offers potentially covert operation [20]. Even before the recent advances in SI cancellation techniques, the idea of FD impulse PRNs was studied to combine the covertness of impulse radios with the increased network throughput of FD radios [21]. In order to allow bidirectional information transfer, the FD impulse PRN technology proposes to blank the receiving front-end during transmissions at the expense of some degradation in the received signals. However, due to the nature of impulse radios, as long as the transmitted and received pulses do not completely overlap, information can be exchanged.

Although the concept of FD impulse PRNs does not rely on the true FD radio technology as considered herein, the idea already emphasized the benefit that the true FD radio technology can bring in tactical networks in terms of improved throughput [22]. However, due to the typically asymmetrical data flow, imperfect SI cancellation, and increased inter-node interference, the improvement in throughput may not always be remarkable. Nevertheless, as discussed next, the FD radio technology also has the potential to improve several other aspects of tactical networks which in turn can enhance situational awareness and network security.

9.2.3.1 Hidden Node

One of the most prominent challenges in tactical and also commercial ad hoc networks is the hidden node issue since it is a major source of collisions. The hidden node, or sometimes referred to as the hidden terminal, issue arises when a node is not aware that the recipient, to whom it is about to start transmitting, is already receiving signals because those signals are not reaching the node which intends to transmit. In this case, the two nodes that have information to transmit to a common node are hidden from each other. If the second node were to also start transmitting then the recipient would receive mixed signals and not be able to make sense of either of those transmissions, which in turn would result in decreased network throughput and increased latency as information has to be retransmitted.

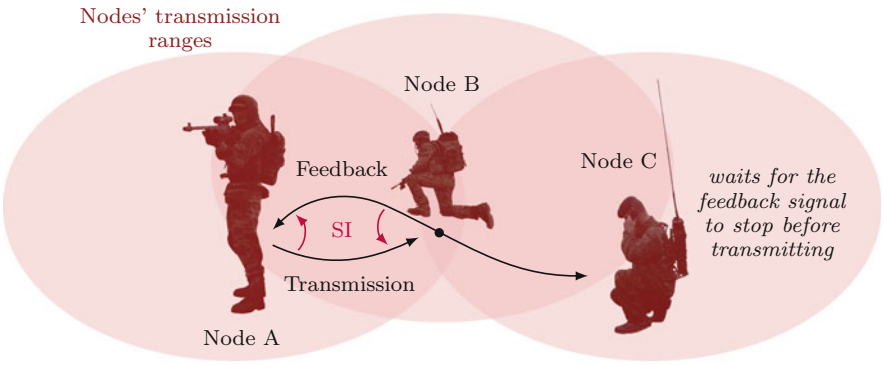

Fig. 9.3 Application of military full-duplex radios to prevent the hidden node problem from occurring in tactical ad hoc networks. Self-interference is abbreviated as SI

To solve this problem, a busy-tone scheme which uses a separate wireless channel to acknowledge the ongoing transmission was initially proposed [23, 24]. This scheme is able to eliminate collisions, but the requirement of allocating a separate wireless channel for collision avoidance only makes it impractical in real ad hoc networks. A pragmatic and widely accepted solution is the use of request to send/clear to send (RTS/CTS) mechanism before data transmission [25]. This way, both parties, the transmitter and the receiver, acknowledge to all nodes in their transmission range that they are about to start communicating. This results in performance increase by reducing the number of collisions and required retransmissions, while on the other hand, this method also introduces considerable overhead in the form of the RTS/CTS exchange. In case the network does not have any hidden nodes, such prior exchange is redundant and prevents the network from achieving the otherwise highest possible throughput.

Similarly to the busy-tone scheme which uses a second frequency to acknowledge the reception with a feedback signal, the FD radio technology enables the recipient to acknowledge the reception with simultaneous transmission but on the exact same frequency. As illustrated in Fig. 9.3, the recipient can consequently inform any nodes in its range about ongoing communications and therefore prevent the hidden node issue from occurring [26, 27]. Furthermore, since simultaneous listening and sensing is being performed on a frequency band while the signals are being transmitted, each node can decide whether or not the other nodes have simultaneously started transmitting and thus prevent multiple access collisions [28].

9.2.3.2 Adaptive Power Control

By facilitating simultaneous two-way information exchange, the FD radio technology significantly reduces latency and end-to-end delays in wireless networks [27]. Lower latency enables tactical networks to employ faster adaptive power control

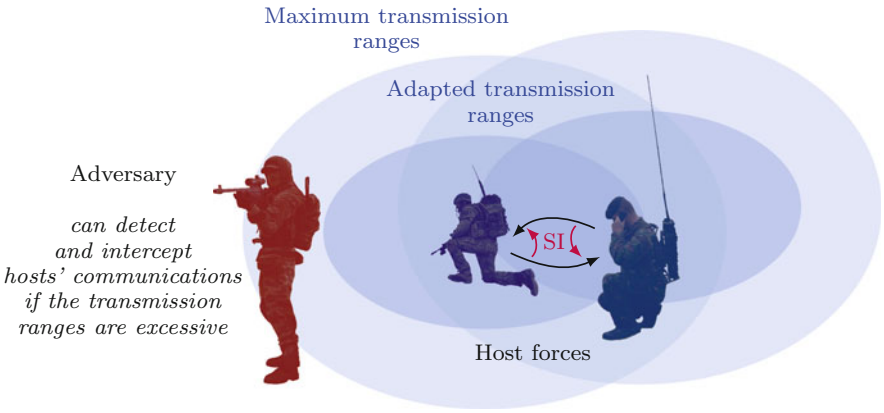

Fig. 9.4 Application of low latency military full-duplex radios with adaptive power control towards low probability of detection and interception. Self-interference is abbreviated as SI

so that the radio links do not use excessive output powers for extended periods of time. This could possibly improve battery life and reduce inter-node interference in multi-hop networks [29, 30]. More importantly in the context of military wireless communications, however, fast adaptive power control can help keep the transmission range as small as possible and therefore lower the probabilities of detection and interception as illustrated in Fig. 9.4. Adapting the transmit power can also reduce the SI in FD radios and therefore improve the reception quality in some cases [31].

9.2.3.3 Secure Key Exchange

As was stressed when discussing requirements for military radios, a prerequisite for securely encrypted communications in wireless networks is secure key exchange. However, due to the broadcast nature of the wireless medium it is not trivial to achieve wirelessly. If an adversary intercepts a wireless key exchange, then it can decrypt the following communications encrypted with that key. Works on secret key extraction from radio channel measurements have demonstrated that two devices can generate shared keys based on the channel variations between the devices [32, 33]. The key generation rate with such methods, however, depends on the rate of channel variations and can be low in static environments. Furthermore, methods which rely on channel variations are susceptible to disagreements about the generated keys between the two devices. An alternative method relies on sending the key twice, each time jamming different parts of the key by the receiver and assuming that the eavesdropper cannot discern which parts have been jammed during either transmission [34].

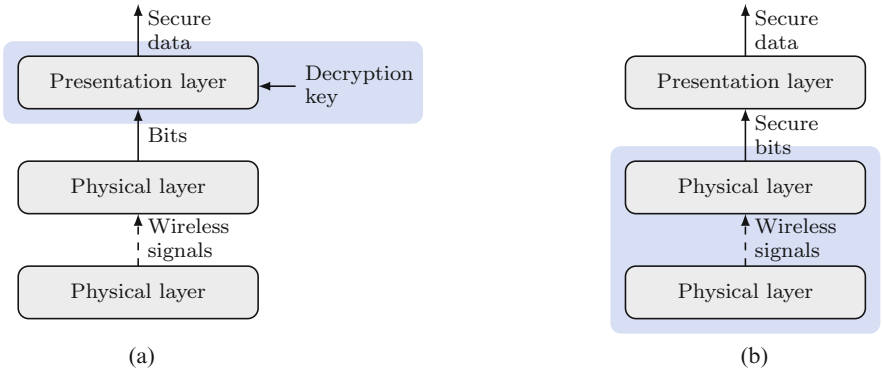

Fig. 9.5 Cryptographic and physical layer security approaches to securing wireless communications. (**a**) Encryption based security. (**b**) Physical layer security

Simultaneous reception and jamming that is facilitated by the FD technology simplifies such key exchange methods to require the key to be transmitted only once [35]. Adversary then receives superposed signals that are difficult to separate and consequently is prevented from intercepting the key. Incorporation of such key exchange schemes in military networks could enable secure wireless key exchange with reduced risk of enemy's signals intelligence decrypting the host's communications should they successfully intercept any. Figure 9.5 illustrates how the FD radio technology enables exchanging secure messages by shifting the security focus from the upper communication layers to the physical layer. A significant benefit of physical layer security compared to cryptographic methods is that physical layer security does not rely on the opponent's limited computational capabilities and therefore the applications for such methods go beyond secure key exchange [36].

9.2.3.4 Directional Medium Access Control

To increase jamming resistance and lower the detection and interception probability in tactical networks, directional medium access control (MAC) protocols have been proposed [37]. This approach aims to concentrate the transmission power towards the intended recipient through beamforming [38]. A significant challenge in applying directional protocols in dynamic topologies is to keep a good estimate of the direction of the intended receiver. To that end, several solutions have been proposed, mostly using a variation of the RTS/CTS exchange to let both the source and destination nodes determine each other's directions [39–41]. However, the performance of such schemes can be expected to degrade as the node mobility increases [41].

It is reasonable to envision that SF-STAR is used so that the transmitter processes the feedback signal from the intended receiver to update the estimated direction

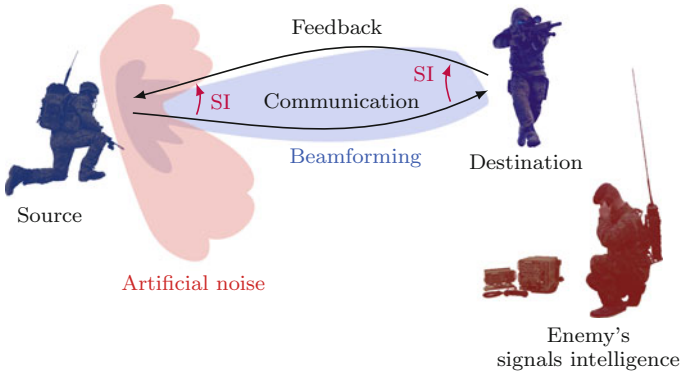

Fig. 9.6 Applying the military full-duplex radio technology to improve direction estimation in directional medium access control protocols for improved throughput and security. Self-interference is abbreviated as SI

of the recipient simultaneously to transmitting as illustrated in Fig. 9.6. Similar concept has been evaluated based on a retrodirective array system that enables FD communication and high-speed beam tracking [42]. Therefore, the node mobility issue that has been of a concern in directional MAC protocols so far can possibly be solved by enabling SF-STAR operation. Additionally, artificial noise can be transmitted in the surrounding directions to further ensure LPI [38, 43]. In static environments and network topologies, the combination of directional antennas with the FD technology has been analytically shown to increase network throughput [44], while beamforming improves the secrecy rate of FD point-to-point links [45].

9.2.4 Continuous-Wave Radars

Radars use high-power radio frequency (RF) transmissions ranging from HF to millimeter-waves (mmWaves) in order to illuminate targets by collecting the reflected echoes in either pulsed or CW modes. The received echoes are used to determine each target's location and velocity, which can be used in both offensive and defensive weapon systems to control and direct the weapon at the target [7]. In pulsed radars, the RF front-end is switched from transmission to reception mode to transmit and then receive the pulse without interfering with itself. In CW radars, echoes from the targets are received simultaneously to transmitting, which causes direct leakage from the radar's transmitter to its receiver that needs to be suppressed by some form of SI cancellation [46]. In that sense, CW radars are quite similar to FD radios.

9.2.4.1 Self-Interference Cancellation

Even though military radars typically operate with much higher frequencies [7] than the currently reported academic FD radio prototypes, many of the SI cancellation solutions could be potentially applied also in low-power CW military radars [1]. More so because typically radar systems require less isolation than FD data transfer applications. However, efficient SI cancellation is not the only challenge in military radars. Radar and data communications are often opposing one another and compete for the same spectral resources, which can result in degradation of sensitivity in the radar or communication systems.

Recent results suggest that by co-designing the radar and communication systems from the ground up, the scarce RF resources could be shared by those seemingly conflicting applications [47]. Based on the advances in SI cancellation, a method for cancelling the radar-induced interference to enable spectrum sensing has been presented in [48]. Classically such coexistent systems could only operate in a time-multiplexed manner, preventing either system from continuously carrying out its task. However, by using the cancellation methods, the known radar signal can be sufficiently suppressed in adjacent receivers. It is reasonable to envision that not only spectrum sensing can be achieved simultaneously to the radar operation but also receiving wireless communications as illustrated in Fig. 9.7.

Besides suppressing the interference caused by radars in co-located receivers, there is significant interest in using the radar waveforms for both object detection and information transmission [49–51]. Such joint radar and communication systems typically study the use of waveforms, such as direct-sequence spread spectrum (DSSS) and orthogonal frequency-division multiplexing (OFDM), which are similar to those used in experiments with research prototype FD transceivers. Such joint radar and communication platforms could therefore take advantage of the SI cancellation techniques to improve near-end local leakage suppression in the radar to improve the radar performance but also to suppress the reflected radar signals

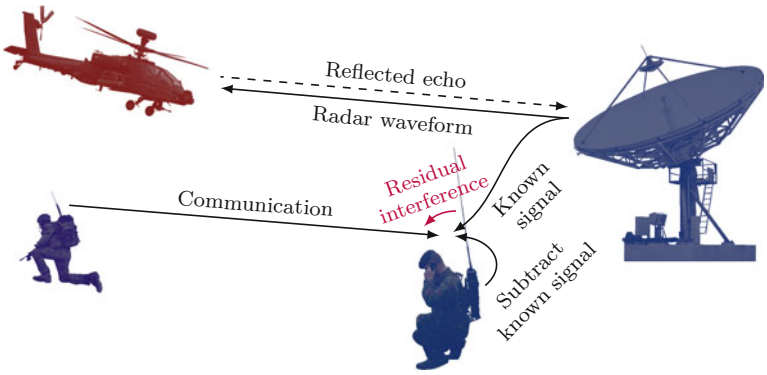

Fig. 9.7 Concurrent radar and communication operation by using the same-frequency simultaneous transmit and receive methods to suppress known radar signals

in order to receive communication signals in the same frequency band. The latter combination is essentially the same as the FD technology used in wireless communications to improve the spectral efficiency.

9.2.4.2 Electronic Countermeasures

In order to evade an opponent's radars, electronic countermeasures (ECMs) such as suppression jamming and deception jamming are often used. Suppression jamming is exercised to impair the opponent's ability to detect objects in the operational environment [52], while deception jamming, which is arguably more difficult to perform, is used to mislead the enemy about the operational environment [53]. For example, through false target generation or delayed radar signal replaying, by use of the digital radio frequency memory (DRFM), the target could be shown to be at a different distance altogether [54]. Through velocity or angle deception, the target could be shown to be moving with a different speed than it actually is or prevent the correct angle from being detected.

To circumvent and detect ECMs in radars, electronic counter-countermeasures (ECCMs) such as frequency agility, frequency diversity, and jamming cancellation through various signal processing techniques are employed [53, 55]. These methods rely to some extent on the jammer's incapability to quickly respond to changes in the radar signal. By integrating the SF-STAR capabilities into radar ECM systems, those systems could simultaneously receive the radar signal and transmit a spoofed echo back. Given adequate signal processing abilities, SF-STAR therefore enables the ECM systems to adapt to the radar signal in real time and possibly evade the aforementioned ECCMs as illustrated in Fig. 9.8.

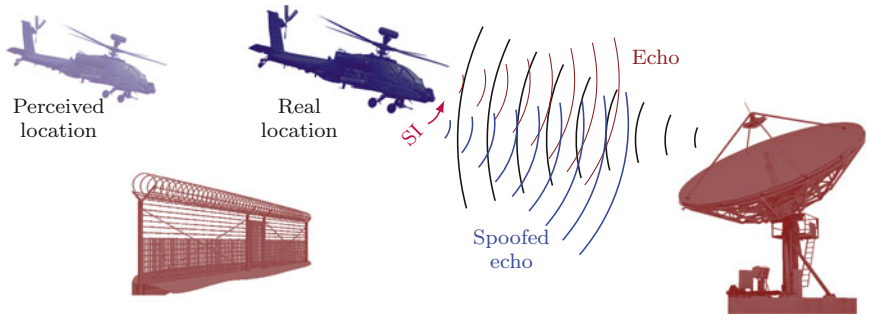

Fig. 9.8 Use of same-frequency simultaneous transmit and receive in electronic countermeasures against radars Self-interference is abbreviated as SI

9.2.5 *Multifunction Radios*

The military domain is characterized by long-term acquisitions, while missions and technical requirements change at quicker rates, therefore the ability to upgrade and reconfigure radio systems through software rather than hardware is highly sought after [56]. Concepts like the joint tactical radio system (JTRS) have focused on replacing aging legacy radios with a single, versatile system based on software defined radio (SDR) [57, 58]. Thus, enabling the radio to be upgraded or modified to operate with other communications systems by the addition or reconfiguration of software as opposed to redesigning or changing hardware. Depending on the mission requirements, each JTRS is envisioned to be capable of executing different waveforms or communication standards, therefore enabling collaboration between otherwise incompatible systems [59].

Furthermore, integrating multiple communication and non-communication tasks simultaneously in the form of advanced multifuncion radio frequency concept (AMRFC) and subsequently integrated topside (INTOP) have been proposed [60–62]. Those concepts encompass the integration of RF functions, such as radar, EW operations, and communications, into a single system utilizing a common set of hardware (as illustrated in Fig. 9.9) for which the functionality is programmed as necessary. The potential benefits of such multifunction systems include reduced number of antennas, increased potential for future growth without adding new aperture therefore resulting in significantly lower upgrade costs, and better control over EM interference through agile and intelligent frequency management. However, the ultimate power of multifunction military radios lies in the ability to adapt the functionality together with key parameters of the equipment to the current tactical operations [61].

Conventional HD single-function systems are able to operate at peak performance by applying various isolation techniques that are tailored to each individual system. However, most of those techniques cannot be directly applied when a single aperture performs multiple functions [63]. So far, multifunction military RF

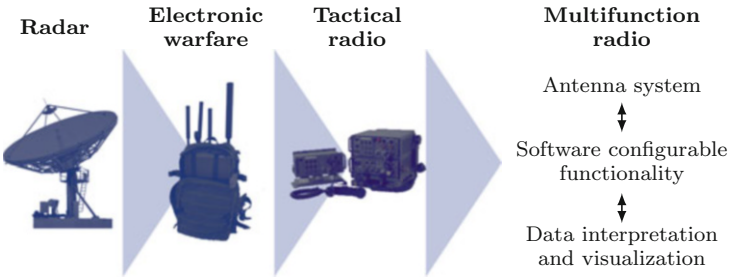

Fig. 9.9 Integration of multiple functions, including radar, electronic warfare, and communications, into a shared set of antennas and signal processing hardware to provide radio functionality depending on the operational needs

systems have mostly relied on separation of transmit and receive antennas to provide moderate isolation between those paths and consequently a key topic for further refinement of multifunction RF systems is to employ improved transmit-to-receive isolation techniques [61]. Therefore FD radio technology can become an elemental part of the multifunction radio vision because it potentially allows transmit and receive functions, whatever they are, to operate simultaneously.

9.3 Applications for Full-Duplex Radios in Civilian Security

When considering the civilian security domain instead of the electronic battlefield, defensive applications rather than offensive ones are paramount. Another significant difference is the fact that many military communication systems operate in the HF and VHF bands while their commercial counterparts work in the UHF band. In that sense, the existing FD prototypes can be more readily applied in the civilian security domain rather than in the military. The malicious wireless communications to be considered in the civilian security domain are, e.g., unauthorized use of remotely controlled UAVs near restricted areas and eavesdropping on or tampering with private wireless communications.

9.3.1 Radio Shield

In order to counter the aforementioned threats, the FD radio technology can be exploited through jamming to propagate a protective electromagnetic field, i.e., a "radio shield," around the transceiver. The jamming prevents any third party within the shield from successfully receiving wireless transmissions while the transceiver's own reception of any other transmissions is unaffected. Moreover, if using a known pseudo-random jamming signal, any other authorized device can also cancel the jamming signal and thereby be capable of transmission and reception inside the radio shield. A conventional HD jammer on the other hand cannot receive at the same frequencies while transmitting and this leads to potentially dangerous situations, e.g., when the malicious wireless communications use the same frequencies as the law enforcement. Using conventional jammers, law enforcement then has to decide whether to block or allow all communications, including their own.

The radio shield could be useful for any common wireless device, including mobile terminals and network infrastructure. For example, the radio shield could be useful in a corporate environment to prevent unintentional information leakage, decreasing the risk of improper or lacking use of encryption. Such wireless physical layer firewalls have been previously proposed on the basis of reactive jammers, which rely on first analyzing the wireless communications and begin to jam when the communication is deemed obtrusive [64]. In case of FD jamming transceivers, it is also possible to carry out simultaneous spectrum surveillance. The transceiver

would therefore be able to detect and identify malicious users who attempt to communicate within the radio shield despite being prohibited from doing so.

However, the predominant challenge in implementing a radio shield is maintaining backwards compatibility with the existing communication systems. This means that the radio shield blocks unwarranted communications while at the same time allowing authorized users to continue using legacy communication standards as if there was no SI. Furthermore, colluding eavesdroppers present a security risk [65] as the radio shield requires the number of antennas transmitting artificial noise or jamming signal to exceed the number of eavesdropper antennas [43].

Several works have already been published regarding the radio shield and they mainly divide into two separate categories: the information-theoretical works, where the secrecy rate under jamming is formally investigated and signal processing works which provide results with high practical value. The latter is mainly focused on the following topics that exemplify the potential value of a FD radio shield in civilian wireless security.

9.3.1.1 Drones

Due to the increased availability of consumer-grade UAVs, it has become necessary to restrict their unauthorized use in areas where they might cause accidents or be used for malicious purposes. Disabling UAV remote control links by wideband jamming while simultaneously retaining the ability to receive communications [66] or detect such links [67, 68] has been shown feasible with the FD radio technology. Consequently, the FD transceiver is also able to detect and identify malicious users who attempt to remotely control UAVs within the radio shield despite being prohibited from doing so. Ideally such restrictions should not prevent authorized UAVs from operating in the same space and if the radio shield used pseudo-random jamming signals, then authorized UAVs could cancel its effect using co-located interference cancellation methods [69] as envisioned in Fig. 9.10. From a non-security perspective, the FD radio technology enables UAVs to form efficient ad hoc networks [70].

9.3.1.2 Wireless Energy Transfer

The fundamental challenge in enabling the ever-growing number of wireless devices part of the Internet of Things (IoT) to communicate is in developing protocols that enable energy-efficient communications between devices without interfering with one another. Acquiring energy from RF signals has opened the way for unified wireless power transmission and communication since those signals carry energy and information simultaneously. Combining such energy harvesting with the FD radio technology potentially enables nodes to power simultaneous reception and transmission from the received signal [71], while at the same time reducing multiple access collisions and improving transmission throughput [72, 73]. The nodes could

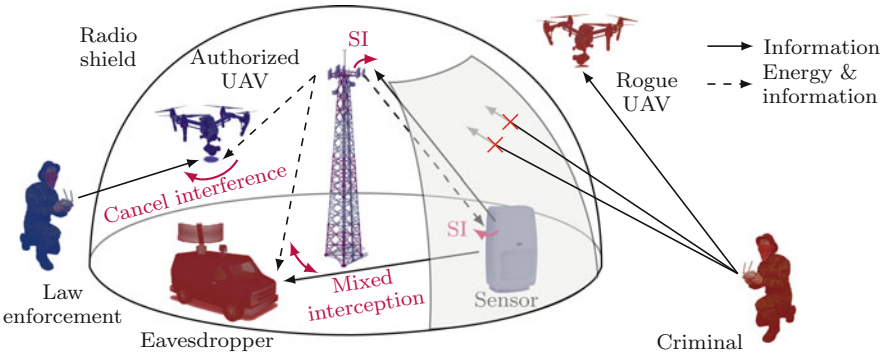

Fig. 9.10 Conceptual use of full-duplex radio shield for wireless power transfer and restricting unauthorized use of the radio frequency spectrum. Self-interference is abbreviated as SI. © [2018] IEEE. Reprinted, with permission, from [2]

be powered from base stations or even from UAVs that could act as FD relays [74]. Therefore, the radio shield can conceivably prevent unauthorized spectrum usage or eavesdropping inside the protective dome, while authorized devices can harvest energy and communicate as illustrated in Fig. 9.10. By adopting beamforming instead of omnidirectional methods, both energy harvesting and SI cancellation capabilities can be increased at FD transceivers [75].

9.3.1.3 Medical Devices

Wearable medical sensors and implanted medical devices (IMDs) are also going through rapid development as they promise to revolutionize healthcare in the form of wireless body area networks (WBANs). However, among other challenges, such as power consumption and aesthetic issues, WBANs face the need to secure the wireless communications from eavesdropping and tampering. Typically, encryption is being considered as a solution [76], yet, concerned by the lack of encryption in existing devices, methods based on FD and reactive jamming have been presented [77, 78]. In such methods, the IMD user wears an additional device—the radio shield generator, which acts as a secure gateway for external devices that want to communicate with the IMD. The radio shield, as an external device, can establish secure connection to a legitimate reader more conveniently than the IMD. The shield jams unauthorized transmission to the IMD or transmissions from the IMD, preventing perpetrators from gaining access to the IMD as illustrated in Fig. 9.11. However, such radio shield does lend itself to attacks from adversaries with multiple reception antennas, as the single-antenna radio shield cannot provide strong confidentiality guarantees in all settings where the attacker can be freely positioned [79].

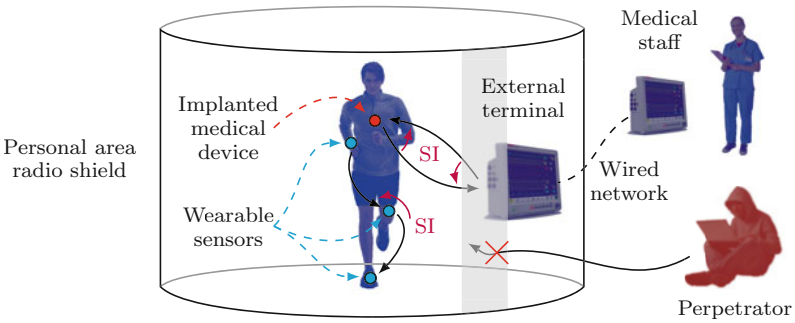

Fig. 9.11 Conceptual use of full-duplex radio shield to provide physical layer security in wireless body area networks and for medical implanted devices. Self-interference is abbreviated as SI. © [2018] IEEE. Reprinted, with permission, from [2]

9.3.1.4 Automotive Radars and Vehicle-to-Vehicle Communications

The automotive industry is also seeking to take advantage of the RF spectrum as the industry is edging towards self-driving cars. To that end, two technologies in particular are essential: automotive radars and vehicle-to-vehicle communications. Radars have been already deployed on consumer vehicles to avoid collisions and provide some self-driving features [47], while vehicular ad hoc network (VANET) protocols are being developed by the automotive industry to provide vehicle operators a better overview of the environment [80, 81]. For example, such communication methods could be used to warn the driver of an accident ahead.

Compared to the previous topics, confidentiality of wireless communications in VANETs is not as important as the authenticity of the information and therefore the physical layer security is typically not considered [82]. However, spectrum congestion and multiple access collisions are as significant issues as they are elsewhere. The proposed VANETs are based on the exchange of periodic cooperative awareness messages (CAMs) and transmitting such messages in highly dynamic network topologies can result in collisions which in turn makes the data transmission unreliable. The use of the FD radio technology can considerably improve the reliability of CAM delivery [83, 84] as simulated results indicate improvements compared to HD broadcasting techniques and cancellation of SI has been successfully demonstrated in a realistic multipath environment on a moving vehicle [85].

Spectrum congestion has motivated studies on the coexistence of automotive radar and communication technologies since they are so closely related. Consequently, radar waveforms can be coded with information without negative influences on the radar performance [50, 86]. Since the feasibility of such waveforms in FD radios has already been demonstrated with numerous prototypes, the combined radio in vehicles could be transmitting the CAMs and use the echoes for object detection or suppress the echoes and receive messages from other vehicles. In

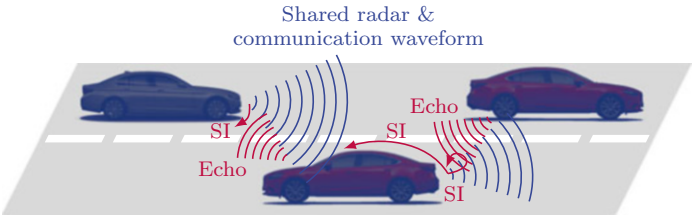

Fig. 9.12 Application of the full-duplex radio technology to enable simultaneous radar and communication capabilities for enhanced spectrum reuse and public safety in the automotive domain. Self-interference is abbreviated as SI

automotive applications, the radio shield could therefore consist of shared radar and communication waveforms that the vehicle uses to detect and track objects inside the shield, while at the same time communicating with other vehicles in the close vicinity as illustrated in Fig. 9.12.

9.3.2 Physical Layer Security

Practicality of the FD radio shield concept has already been demonstrated through experimental results as covered in the previous section. However, these studies have been complemented to a great extent by the physical layer security research incorporating the FD radio technology from an information-theoretic viewpoint. Information-theoretic studies on physical layer security in general have existed long before the emergence of FD radio technology. Most notably the introduction of the wiretap channel and subsequently the Gaussian wiretap channel sparked interest in this field [87, 88]. The fundamental principle behind physical layer security that resulted from these works is that the secrecy capacity of a wireless communications system is inherent in the difference between the channel capacities of the intended and wiretap channels. Non-zero secrecy capacity can only be achieved if the wiretap channel is of lower quality than the channel between the transmitter and the intended receiver. Furthermore, the emergence of multiple-input multiple-output (MIMO) systems led to the realization that the secrecy capabilities of wireless systems could be enhanced by taking advantage of the available spatial dimensions [89].

Assuming that the receiver operates in the HD mode, solutions against eavesdropping have been proposed, e.g., through the use of cooperating jammer nodes that confuse the eavesdropper [90]. Although cooperation has been shown to significantly improve the system security as compared to transmission without cooperation, then in order to effectively use cooperative jammers, challenges such as external node mobility, synchronization, and trustworthiness need to be addressed. By making use of the FD mode at the receiver, i.e., the possibility to transmit jamming noise simultaneously to receiving data as in case of the radio shield, the need for external cooperating nodes together with the respective

challenges is eliminated while still degrading the eavesdropper channel. Even more, simultaneous data reception and jamming possibly allows to hide the existence of the communication and thus provide physical layer privacy, something that is not typically considered in the information-theoretic physical layer security works but is emphasized in the signal processing-specific research.

Applications for which physical layer security through SF-STAR operation has been considered include increasing the security against eavesdroppers between point-to-point links [91], in relay networks [92], and in cellular base stations [93]. That being said, the use of the FD technology with regard to physical layer security has also been explored for offensive scenarios in the form of active eavesdroppers [94, 95]. The idea being that an active eavesdropper with FD capabilities can degrade the channel between the transmitter and receiver, therefore also reducing the secrecy rate of the system. Thus, active eavesdropping imposes a more significant challenge as compared to conventional passive eavesdropping from the wireless communications security perspective.

Herein we have given only a brief introduction to the physical layer security research problem and to how the information-theoretic research involving the FD technology in that sense relates to the signal processing research efforts. The information-theoretic research with regard to FD technology is considered in more detail in Chap. 10, which specifically focuses on resource allocation within multiuser FD communication systems in order to secure simultaneous downlink and uplink transmission.

9.4 Conclusion

The importance of electronic warfare (EW) is on the rise and it further establishes the electromagnetic (EM) spectrum as an operational environment, in which tasks must be coordinated and collaborated to enhance the capability to advance tactical and strategical aims. As the sophistication of EW increases so does the importance of the underlying technologies. Consequently, the radio frequency (RF) technology community is challenged with the task of delivering the technological base for EW systems to form a solid framework for conducting operations. Encouraged by the recent advances of the full-duplex (FD) radio technology in the wireless networking domain, we anticipate this technology not only to award spectrally efficient wireless communications but also to pave the way for combinations of non-communication and communication tasks in the military domain. Thus, this chapter surveyed the perspectives of military full-duplex radios (MFDRs) in electronic battlefields, combining tactical communications with EW operations. We have also reviewed possible related defensive applications in the civilian security field. Arguably the FD radio technology can provide a key technical advantage in either domain over an opponent or a perpetrator that is limited to employ the conventional half-duplex (HD) radio technology.

References

1. 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.
2. 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.
3. 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.
4. F. O'Hara and G. Moore, "A high performance CW receiver using feedthrough nulling," *Microwave Journal*, vol. 6, pp. 63–71, Sep. 1963.
5. M. Adrat, R. Keller, S. Wilden, V. L. Nir, T. Riihonen, M. Bowyer, and K. Pärlin, "Full duplex radio: Increasing the spectral efficiency for military applications," NATO, Tech. Rep., Jan. 2020.
6. M. Adrat, R. Keller, M. Tschauner, S. Wilden, V. L. Nir, T. Riihonen, M. Bowyer, and K. Pärlin, "Full-duplex radio technology – Increasing the spectral efficiency for military applications," in *Proc. International Conference on Military Communications and Information Systems*, May 2019.
7. A. E. Spezio, "Electronic warfare systems," *IEEE Transactions on Microwave Theory and Techniques*, vol. 50, no. 3, pp. 633–644, Mar. 2002.
8. 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.
9. S. M. Al-Shehri, P. Loskot, T. Numanoğlu, and M. Mert, "Comparing tactical and commercial MANETs design strategies and performance evaluations," in *Proc. IEEE Military Communications Conference*, Oct. 2017, pp. 599–604.
10. R. Poisel, *Modern Communications Jamming: Principles and Techniques*. Artech House, 2011, pp. 5–10.
11. A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1550–1573, Aug. 2014.
12. H. Saarnisaari and T. Bräysy, "Future military mobile radio communication systems from electronic warfare perspective," in *Proc. International Conference on Military Communications and Information Systems*, May 2017.
13. G. Karawas, K. Goverdhanam, and J. Koh, "Wideband active interference cancellation techniques for military applications," in *Proc. 5th European Conference on Antennas and Propagation*, Apr. 2011, pp. 390–392.
14. S. Enserink, M. P. Fitz, K. Goverdhanam, C. Gu, T. R. Halford, I. Hossain, G. Karawasy, and O. Y. Takeshita, "Joint analog and digital interference cancellation," in *Proc. IEEE MTT-S International Microwave Symposium*, Jun. 2014.
15. 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.
16. 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.
17. M. Lichtman, J. D. Poston, S. Amuru, C. Shahriar, T. C. Clancy, R. M. Buehrer, and J. H. Reed, "A communications jamming taxonomy," *IEEE Security & Privacy*, vol. 14, no. 1, pp. 47–54, Jan. 2016.

18. S. Corson and J. Macker, "Mobile ad hoc networking (MANET): Routing protocol performance issues and evaluation considerations," Jan. 1999.
19. J. L. Burbank, P. F. Chimento, B. K. Haberman, and W. T. Kasch, "Key challenges of military tactical networking and the elusive promise of MANET technology," *IEEE Communications Magazine*, vol. 44, no. 11, Nov. 2006.
20. R. J. Fontana, "Recent system applications of short-pulse ultra-wideband (UWB) technology," *IEEE Transactions on Microwave Theory and Techniques*, vol. 52, no. 9, pp. 2087–2104, Sep. 2004.
21. S. S. Kolenchery, J. K. Townsend, and J. A. Freebersyser, "A novel impulse radio network for tactical military wireless communications," in *Proc. IEEE Military Communications Conference*, vol. 1, Oct. 1998, pp. 59–65.
22. M. A. Alim, M. Kobayashi, S. Saruwatari, and T. Watanabe, "In-band full-duplex medium access control design for heterogeneous wireless LAN," *EURASIP Journal on Wireless Communications and Networking*, vol. 2017, no. 1, p. 83, May 2017.
23. F. Tobagi and L. Kleinrock, "Packet switching in radio channels: part II–the hidden terminal problem in carrier sense multiple-access and the busy-tone solution," *IEEE Transactions on Communications*, vol. 23, no. 12, pp. 1417–1433, Dec. 1975.
24. C.-s. Wu and V. Li, "Receiver-initiated busy-tone multiple access in packet radio networks," in *ACM SIGCOMM Computer Communication Review*, vol. 17, no. 5, Aug. 1987, pp. 336–342.
25. K. Xu, M. Gerla, and S. Bae, "How effective is the IEEE 802.11 RTS/CTS handshake in ad hoc networks," in *Proc. IEEE Global Telecommunications Conference*, vol. 1, Nov. 2002, pp. 72–76.
26. N. Singh, D. Gunawardena, A. Proutiere, B. Radunovi, H. V. Balan, and P. Key, "Efficient and fair MAC for wireless networks with self-interference cancellation," in *International Symposium on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks*, May 2011, pp. 94–101.
27. K. M. Thilina, H. Tabassum, E. Hossain, and D. I. Kim, "Medium access control design for full duplex wireless systems: challenges and approaches," *IEEE Communications Magazine*, vol. 53, no. 5, pp. 112–120, May 2015.
28. 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.
29. J. P. Monks, J.-P. Ebert, A. Wolisz, and W.-M. W. Hwu, "A study of the energy saving and capacity improvement potential of power control in multi-hop wireless networks," in *Proc. 26th Annual IEEE Conference on Local Computer Networks*, Nov. 2001, pp. 550–559.
30. W. Choi, H. Lim, and A. Sabharwal, "Power-controlled medium access control protocol for full-duplex WiFi networks," *IEEE Transactions on Wireless Communications*, vol. 14, no. 7, pp. 3601–3613, Jul. 2015.
31. T. Riihonen, S. Werner, and R. Wichman, "Hybrid full-duplex/half-duplex relaying with transmit power adaptation," *IEEE Transactions on Wireless Communications*, vol. 10, no. 9, pp. 3074–3085, Sep. 2011.
32. N. Patwari, J. Croft, S. Jana, and S. K. Kasera, "High-rate uncorrelated bit extraction for shared secret key generation from channel measurements," *IEEE Transactions on Mobile Computing*, vol. 9, no. 1, p. 17, Jan. 2010.
33. S. N. Premnath, S. Jana, J. Croft, P. L. Gowda, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "Secret key extraction from wireless signal strength in real environments," *IEEE Transactions on Mobile Computing*, vol. 12, no. 5, pp. 917–930, May 2013.
34. S. Gollakota and D. Katabi, "Physical layer wireless security made fast and channel independent," in *Proc. IEEE INFOCOM*, Apr. 2011.
35. R. Jin, X. Du, Z. Deng, K. Zeng, and J. Xu, "Practical secret key agreement for full-duplex near field communications," *IEEE Transactions on Mobile Computing*, vol. 15, no. 4, pp. 938–951, Apr. 2016.
36. R. Bassily, E. Ekrem, X. He, E. Tekin, J. Xie, M. R. Bloch, S. Ulukus, and A. Yener, "Cooperative security at the physical layer: A summary of recent advances," *IEEE Signal Processing Magazine*, vol. 30, no. 5, pp. 16–28, Sep. 2013.

37. S. L. Cotton, W. G. Scanlon, and B. K. Madahar, "Millimeter-wave soldier-to-soldier communications for covert battlefield operations," *IEEE Communications Magazine*, vol. 47, no. 10, pp. 72–81, Oct. 2009.
38. Y.-W. P. Hong, P.-C. Lan, and C.-C. J. Kuo, "Enhancing physical-layer secrecy in multiantenna wireless systems: An overview of signal processing approaches," *IEEE Signal Processing Magazine*, vol. 30, no. 5, pp. 29–40, Sep. 2013.
39. A. Nasipuri, S. Ye, J. You, and R. E. Hiromoto, "A MAC protocol for mobile ad hoc networks using directional antennas," in *IEEE Wireless Communications and Networking Conference*, vol. 3, Sep. 2000, pp. 1214–1219.
40. R. R. Choudhury, X. Yang, R. Ramanathan, and N. H. Vaidya, "On designing MAC protocols for wireless networks using directional antennas," *IEEE Transactions on Mobile Computing*, vol. 5, no. 5, pp. 477–491, May 2006.
41. T. Korakis, G. Jakllari, and L. Tassiulas, "CDR-MAC: A protocol for full exploitation of directional antennas in ad hoc wireless networks," *IEEE Transactions on Mobile Computing*, vol. 7, no. 2, pp. 145–155, Feb. 2008.
42. K. M. Leong, Y. Wang, and T. Itoh, "A full duplex capable retrodirective array system for high-speed beam tracking and pointing applications," *IEEE Transactions on Microwave Theory and Techniques*, vol. 52, no. 5, pp. 1479–1489, May 2004.
43. S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Transactions on Wireless Communications*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.
44. K. Miura and M. Bandai, "Node architecture and MAC protocol for full duplex wireless and directional antennas," in *Proc. 23rd International Symposium on Personal, Indoor and Mobile Radio Communications*, Sep. 2012, pp. 369–374.
45. F. Zhu, F. Gao, M. Yao, and H. Zou, "Joint information- and jamming-beamforming for physical layer security with full duplex base station," *IEEE Transactions on Signal Processing*, vol. 62, no. 24, pp. 6391–6401, Dec. 2014.
46. M. A. Richards, J. Scheer, W. A. Holm, and W. L. Melvin, *Principles of modern radar*. Institution of Engineering and Technology, 2010.
47. B. Paul, A. Chiriyath, and D. Bliss, "Survey of RF communications and sensing convergence research," *IEEE Access*, vol. 5, no. 99, pp. 252–270, Dec. 2016.
48. M. P. Fitz, T. R. Halford, I. Hossain, and S. W. Enserink, "Towards simultaneous radar and spectral sensing," in *Proc. IEEE International Symposium on Dynamic Spectrum Access Networks*, Apr. 2014, pp. 15–19.
49. M. Jamil, H.-J. Zepernick, and M. I. Pettersson, "On integrated radar and communication systems using Oppermann sequences," in *Proc. IEEE Military Communications Conference*, Oct. 2008.
50. C. Sturm and W. Wiesbeck, "Waveform design and signal processing aspects for fusion of wireless communications and radar sensing," *Proceedings of the IEEE*, vol. 99, no. 7, pp. 1236–1259, Jul. 2011.
51. L. Han and K. Wu, "Joint wireless communication and radar sensing systems–state of the art and future prospects," *IET Microwaves, Antennas & Propagation*, vol. 7, no. 11, pp. 876–885, Aug. 2013.
52. R. N. Lothes, M. B. Szymanski, and R. G. Wiley, *Radar vulnerability to jamming*. Artech House, 1990.
53. L. Neng-Jing and Z. Yi-Ting, "A survey of radar ECM and ECCM," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 31, no. 3, pp. 1110–1120, Jul. 1995.
54. S. Roome, "Digital radio frequency memory," *Electronics & Communication Engineering Journal*, vol. 2, no. 4, pp. 147–153, Aug. 1990.
55. M. Greco, F. Gini, and A. Farina, "Radar detection and classification of jamming signals belonging to a cone class," *IEEE Transactions on Signal Processing*, vol. 56, no. 5, pp. 1984–1993, May 2008.
56. T. Ulversoy, "Software defined radio: Challenges and opportunities," *IEEE Communications Surveys & Tutorials*, vol. 12, no. 4, pp. 531–550, Oct. 2010.

57. A. Feickert, "The joint tactical radio system (JTRS) and the army's future combat system (FCS): Issues for congress," Congressional Research Service, Tech. Rep. RL33161, 2005.
58. R. North, N. Browne, and L. Schiavone, "Joint tactical radio system – connecting the GIG to the tactical edge," in *Proc. IEEE Military Communications Conference*, Oct. 2006.
59. B. Perlman, J. Laskar, and K. Lim, "Fine-tuning commercial and military radio design," *IEEE Microwave Magazine*, vol. 9, no. 4, Aug. 2008.
60. P. K. Hughes and J. Y. Choe, "Overview of advanced multifunction RF system (AMRFS)," in *Proc. IEEE International Conference on Phased Array Systems and Technology*, May 2000, pp. 21–24.
61. G. C. Tavik, C. L. Hilterbrick, J. B. Evins, J. J. Alter, J. G. Crnkovich, J. W. de Graaf, W. Habicht, G. P. Hrin, S. A. Lessin, D. C. Wu *et al.*, "The advanced multifunction RF concept," *IEEE Transactions on Microwave Theory and Techniques*, vol. 53, no. 3, pp. 1009–1020, Mar. 2005.
62. J. A. Molnar, I. Corretjer, and G. Tavik, "Integrated topside-integration of narrowband and wideband array antennas for shipboard communications," in *Proc. IEEE Military Communications Conference*, Oct. 2011, pp. 1802–1807.
63. M. Parent, D. Taylor, G. Tavik, M. Kluskens, and J. Valenzi, "RF isolation of separate transmit and receive phased array antennas in a multifunction environment," in *Proc. Antenna Application Symposium*, vol. 2, Sep. 2001, pp. 413–442.
64. M. Wilhelm, I. Martinovic, J. B. Schmitt, and V. Lenders, "WiFire: a firewall for wireless networks," in *ACM SIGCOMM Computer Communication Review*, vol. 41, no. 4, Aug. 2011, pp. 456–457.
65. P. C. Pinto, J. Barros, and M. Z. Win, "Secure communication in stochastic wireless networks–part II: Maximum rate and collusion," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 1, pp. 139–147, Feb. 2012.
66. T. Riihonen, D. Korpi, M. Turunen, T. Peltola, J. Saikanmäki, M. Valkama, and R. Wichman, "Military full-duplex radio shield for protection against adversary receivers," in *Proc. International Conference on Military Communications and Information Systems*, May 2019.
67. 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.
68. 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.
69. K. Pärlin, T. Riihonen, and M. Turunen, "Sweep jamming mitigation using adaptive filtering for detecting frequency agile systems," in *Proc. International Conference on Military Communications and Information Systems*, May 2019.
70. Y. Cai, F. R. Yu, J. Li, Y. Zhou, and L. Lamont, "Medium access control for unmanned aerial vehicle (UAV) ad-hoc networks with full-duplex radios and multipacket reception capability," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 1, pp. 390–394, Jan. 2013.
71. I. Krikidis, S. Timotheou, S. Nikolaou, G. Zheng, D. W. K. Ng, and R. Schober, "Simultaneous wireless information and power transfer in modern communication systems," *IEEE Communications Magazine*, vol. 52, no. 11, pp. 104–110, Nov. 2014.
72. C. Zhong, H. A. Suraweera, G. Zheng, I. Krikidis, and Z. Zhang, "Wireless information and power transfer with full duplex relaying," *IEEE Transactions on Communications*, vol. 62, no. 10, pp. 3447–3461, Oct. 2014.
73. L. Zhao, X. Wang, and T. Riihonen, "Transmission rate optimization of full-duplex relay systems powered by wireless energy transfer," *IEEE Transactions on Wireless Communications*, vol. 16, no. 10, pp. 6438–6450, Oct. 2017.
74. Y. Ma, N. Selby, and F. Adib, "Drone relays for battery-free networks," in *Proc. Conference of the ACM Special Interest Group on Data Communication*, Aug. 2017, pp. 335–347.
75. M. Mohammadi, B. K. Chalise, H. A. Suraweera, C. Zhong, G. Zheng, and I. Krikidis, "Throughput analysis and optimization of wireless-powered multiple antenna full-duplex relay systems," *IEEE Transactions on Communications*, vol. 64, no. 4, pp. 1769–1785, Apr. 2016.

76. M. Li, W. Lou, and K. Ren, "Data security and privacy in wireless body area networks," *IEEE Wireless Communications*, vol. 17, no. 1, Feb. 2010.
77. S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, and K. Fu, "They can hear your heartbeats: Non-invasive security for implantable medical devices," in *ACM SIGCOMM Computer Communication Review*, vol. 41, no. 4, Aug. 2011, pp. 2–13.
78. F. Xu, Z. Qin, C. C. Tan, B. Wang, and Q. Li, "IMDGuard: Securing implantable medical devices with the external wearable guardian," in *Proc. IEEE INFOCOM*, Apr. 2011, pp. 1862–1870.
79. N. O. Tippenhauer, L. Malisa, A. Ranganathan, and S. Capkun, "On limitations of friendly jamming for confidentiality," in *IEEE Symposium on Security and Privacy*, May 2013, pp. 160–173.
80. J. B. Kenney, "Dedicated short-range communications (DSRC) standards in the United States," *Proceedings of the IEEE*, vol. 99, no. 7, pp. 1162–1182, Jul. 2011.
81. K. Sjöberg, P. Andres, T. Buburuzan, and A. Brakemeier, "Cooperative intelligent transport systems in Europe: current deployment status and outlook," *IEEE Vehicular Technology Magazine*, vol. 12, no. 2, pp. 89–97, Jun. 2017.
82. M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *Journal of computer security*, vol. 15, no. 1, pp. 39–68, Jan. 2007.
83. A. Bazzi, B. M. Masini, and A. Zanella, "Performance analysis of V2V beaconing using LTE in direct mode with full duplex radios," *IEEE Wireless Communications Letters*, vol. 4, no. 6, pp. 685–688, Dec. 2015.
84. C. Campolo, A. Molinaro, and A. O. Berthet, "Improving CAMs broadcasting in VANETs through full-duplex radios," in *IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications*, Sep. 2016, pp. 1–6.
85. K. E. Kolodziej, B. T. Perry, and J. S. Herd, "Simultaneous transmit and receive (STAR) system architecture using multiple analog cancellation layers," in *IEEE MTT-S International Microwave Symposium*, May 2015, pp. 1–4.
86. P. Kumari, J. Choi, N. González-Prelcic, and R. W. Heath, "IEEE 802.11 ad-based radar: An approach to joint vehicular communication-radar system," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 4, pp. 3012–3027, Apr. 2018.
87. A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.
88. S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.
89. A. O. Hero, "Secure space-time communication," *IEEE Transactions on Information Theory*, vol. 49, no. 12, pp. 3235–3249, Dec. 2003.
90. L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Transactions on Signal Processing*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.
91. 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.
92. G. Chen, Y. Gong, P. Xiao, and J. A. Chambers, "Physical layer network security in the full-duplex relay system," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 3, pp. 574–583, 2015.
93. F. Zhu, F. Gao, T. Zhang, K. Sun, and M. Yao, "Physical-layer security for full duplex communications with self-interference mitigation," *IEEE Transactions on Wireless Communications*, vol. 15, no. 1, pp. 329–340, Jan. 2016.
94. A. Mukherjee and A. L. Swindlehurst, "A full-duplex active eavesdropper in MIMO wiretap channels: Construction and countermeasures," in *Proc. 45th Asilomar Conference on Signals, Systems and Computers*, 2011, pp. 265–269.
95. X. Tang, P. Ren, Y. Wang, and Z. Han, "Combating full-duplex active eavesdropper: A hierarchical game perspective," *IEEE Transactions on Communications*, vol. 65, no. 3, pp. 1379–1395, Mar. 2016.