Physical-Layer Reliability of Drones and Their Counter-Measures: Full vs. Half Duplex

Karel Pärlin, Taneli Riihonen, *Senior Member, IEEE*, Vincent Le Nir, and Marc Adrat

***Abstract*—In this article, we study the advantages and disadvantages that full-duplex (FD) radio technology brings to remote-controlled drone and counter-drone systems in comparison to classical half-duplex (HD) radio technology. We consider especially the physical-layer reliability perspective. For establishing a solid analytical background, we first derive original closed-form expressions to evaluate demodulation and detection performance of frequency-hopped and frequency-shift keyed drone remote control signals under external or self-inflicted interference. The developed analytical tools are verified by comparison to simulated results and then used to study the impact that the operation mode has on the flight range of drones and effective range of counter-drone systems in different scenarios, linking the physical layer performance to practical safety. Analysis of the scenarios shows that FD operation compared to HD can extend the effective range of a counter-drone system and that in FD mode a drone can detect the attacks from the counter-drone system from a greater distance than in HD mode. However, two-way communication between the remote controller and drone in FD mode compared to HD significantly reduces the controllable flight range when targeted by a smart counter-drone system.**

***Index Terms*—Reliability, drone, UAV, counter-drone, half-duplex, full-duplex, jamming, energy detection.**

I. Introduction

RELIABILITY is a critical issue in wireless communications, since malicious users may, due to the broadcast nature of wireless transmissions, rather easily interfere with the reception of the transmitted signals at the intended receiver. There are some reliability-enhancing methods that can be used on the upper layers of a two-point wireless communications link to mitigate the effect of interference. For example, channel coding can help overcome interference at the cost of redundancy in the communication. However, the physical-layer implementation (i.e., the modulation technique and rate along with the use of spread spectrum techniques) of a wireless system lays the foundation for the communication's overall reliability, similarly to how the physical-layer implementation of an electronic counter-measure system determines its respective performance.

One recent development that has the potential to enhance both wireless communication systems and electronic counter-measure systems is full-duplex (FD) radio technology. Advances in the self-interference (SI) cancellation research are facilitating FD operation [1], allowing at the same time to combine different aspects of wireless communications and electronic warfare. Such as, e.g., simultaneous signals reception and jamming, to prevent eavesdropping and increase the security of wireless systems, or simultaneous surveillance and jamming, to increase the efficiency of electronic counter-measure systems [2]. As such, FD radio technology is a promising candidate for improving the reliability and also security of wireless systems. Several practical works demonstrating the feasibility of applying FD technology for such combinations have already been published [3]–[5] in addition to the purely information theoretic physical-layer secrecy studies [6], [7]. However, practical gains of such combinations have not yet been comprehensively studied.

Reliability is essential in any wireless application and it is becoming increasingly relevant, as the number of connected devices grows. However, in order to relate this work to the safety of practical and timely systems, we focus here on drone and counter-drone systems only. We consider drones as the central theme of this work because the proliferation of consumer drones poses a significant challenge in protecting various airspaces [8] and, as the application of drones in all aspects of life increases, their reliability and security is becoming more and more important for the safety of the applications in which they are used. There is also significant overlap in FD and drone research as FD-enhanced drones have been shown to outperform their terrestrial and strictly half-duplex (HD) counterparts as base stations [9] and relaying systems [10].

Countering malicious drones and improving the reliability and security of remote-controlled drones in general has received significant interest as the availability of drones has increased. The existing counter-measures have been thoroughly studied and various aspects of counter-drone operations are progressively enhanced [11]–[13]. Likewise, robustness and privacy of the the wireless communications links of legitimate drone applications have been carefully considered against various threats and improvements are being suggested [14]–[16]. Furthermore, it has been recognized that the management of intentional interference in satellite navigation on board of drones is of significant importance [17]. However, all of these works emphasize that, in order to promote safe, secure, and privacy-respecting drone operations, there is a need for innovative technologies to neutralize malicious drones and improve resilience of legitimate drone applications.

Manuscript received November 18, 2022; date of current version November 18, 2022. The associate editor coordinating the review of this paper and approving it for publication was N. Name.

K. Pärlin and T. Riihonen are with Tampere University, Faculty of Information Technology and Communication Sciences, Korkeakoulunkatu 1, 33720 Tampere, Finland (e-mail: karel.parlin@tuni.fi; taneli.riihonen@tuni.fi).

V. Le Nir is with Royal Military Academy, Signal and Image Center, Avenue de la Renaissance 30, B-1000 Brussels, Belgium (e-mail: vincent.lenir@rma.ac.be).

M. Adrat is with Fraunhofer Institute for Communication, Information Processing and Ergonomics (FKIE), Fraunhofer Straße 20, 53343 Wachtberg, Germany (e-mail: marc.adrat@fkie.fraunhofer.de).

This research work was supported by the Academy of Finland and the Finnish Scientific Advisory Board for Defence.

Digital Object Identifier 10.1109/TWC.202X.XXXXXXX

In the context of wireless networks, it has been proposed that jointly optimizing the trajectory and output power [18], [19] or using 3D beamforming [20] can be used to improve the physical-layer security of drones. However, these methods rely on the channel state information being available to drones and this is difficult to acquire in practice, especially when dealing with non-cooperative nodes. Another solution, which has been studied under the term covert communications, is hiding wireless transmissions [21]. Interference-generating FD receivers have great potential of hiding wireless transmissions from eavesdroppers [22], but this assumes that the interference-generating node is ever-present at the eavesdroppers location [22] or that the eavesdropper is uncertain about the noise parameters at its receiver [23]. In practice it is difficult to justify these assumptions within the context of practical drone and counter-drone scenarios.

In this work, we examine how using FD over HD in remote-controlled drone and counter-drone systems affects their reliability. To make the analysis comprehensive and practically relevant, we consider counter-drone systems with varying levels of sophistication. The goal of this study is to characterize the performance of the remote-controlled drone and counter-drone system for all of the relevant configurations of HD and FD capabilities on either side, giving detailed insight into the achievable physical-layer reliability, which translates into safety of practical environments where drones are used, for good or bad. Similar reliability analysis has not been carried out before.

This work complements the existing research from a new, practical perspective. Unlike the drone physical-layer security works [18]–[20], this work does not assume known channel states nor optimizes the output power and trajectory, but rather studies if FD provides a benefit over HD at maximum practical output powers and operation-imposed trajectories. Compared to FD physical-layer security works [6], [7], this work does not analyse when the communication becomes theoretically insecure, but when the remote control link breaks down and renders the drone inoperable. Compared to FD drone wireless network studies [9], [10], this work studies the physical safety, which stems from the remote control link reliability, rather than spectrum efficiency. Unlike existing counter-drone [11]–[13] and counter counter-drone works [14]–[16] that consider principles such as machine learning, e.g., this work studies the benefit of FD operation compared to HD.

In order to facilitate the analysis, we first derive analytical methods for evaluating the detection and demodulation probabilities of frequency-hopped binary frequency-shift keying (BFSK) signals under interference. We then use that functionality within three scenarios. The scenarios illustrate the duplexing mode trade-offs in improving the reliability and security of remotely controlled drones as following. Firstly, the analysis shows that in FD mode a counter-drone system can expect to protect a somewhat larger area than in HD mode. Secondly, compared to HD mode, a FD remote control link is an easier target to smart counter-drone systems and significantly reduces the operational area. Thirdly, compared to HD mode, FD operation significantly improves drones' ability to detect malicious interference from a counter-drone system. Within all three scenarios, we also see the performance difference of counter-drone systems with different complexities. Finally, we show the energy efficiencies of the studies jamming strategies and demonstrate the hard truth that elevating the counter-drone system can be a more significant improvement than any of the strategies or operation modes.

The rest of this article is organized as follows. To begin with, Section II introduces in detail the system model considered in this work. Then, Section III develops the techniques necessary for analysing all the possible configurations of the presented system model. In Section IV, firstly, the developed analysis techniques are verified by comparison to simulation results. Secondly, three practical scenarios are presented, showcasing the importance of reliability in drone and counter-drone systems, and the performance of HD and FD operation is studied within those scenarios. Finally, conclusions of the study are given in Section V.

II. System Model

In this work we consider a system of three nodes — a remote controller, a remote-controlled drone, and a counter-drone system, as illustrated in Fig. 1. We assume that the remote controller and the drone use a two-way slow frequency-hopped BFSK radio-frequency (RF) remote control link, such as is used in many practical remote-controlled drone systems [8]. The counter-drone system aims to detect that RF link and neutralize the remote-controlled drone by interfering with its reception of the remote control signals or with the remote controller's reception of the feedback signals. Each of the three nodes operates in either classical HD mode or in enhanced FD mode, with the FD mode enabling simultaneous transmission and reception on the same frequency to combine a selection of wireless communications, signals reconnaissance, and signals interference functions. We assume that the channels h_{RD}, h_{RJ}, and h_{DJ} are affected only by path loss, which itself depends on the elevation of the nodes. The device-specific capabilities and objectives of the three nodes are as follows.

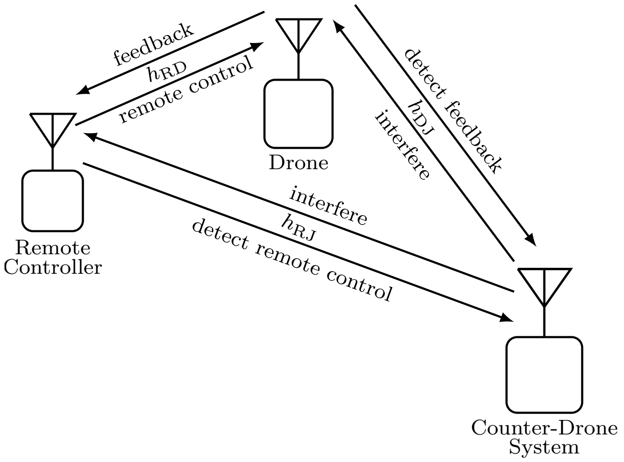


Fig. 1. Three-node system model, consisting of a remote controller, a remote-controlled drone, and a counter-drone system. The three-node model is simple, yet realistic representation of counter-drone scenarios.

A. Remote Controller

The main task of the remote controller is to transmit control signals to the drone for directing its movements. The basic elements of the transmitter at the remote controller are shown in Fig. 2. The input binary data has a rate R_b [bits/s] and it is error-correction encoded at a code rate r, so that the encoded data has a rate $R_\mathrm{c} = R_\mathrm{b}/r$ [bits/s]. The encoded data is converted to BFSK symbols, and, since binary modulation is considered, the symbol rate is equal to the encoded data rate $R_\mathrm{s} = R_\mathrm{c}$. Finally, the symbols are mixed with a frequency hopping tone of frequency ω_m that changes with hop rate R_h. As a result, the drone's remote controller transmits a sequence of slow frequency-hopped BFSK signal

$$x_{m,l}(t) = \sqrt{P_\mathrm{x}} \exp\left(i\left(\omega_m + l\omega_\Delta\right)t + i\theta_\mathrm{x}\right) \tag{1}$$

with fixed signal power P_x, frequency-hopped channel center frequency ω_m, channel number m, symbol l either 1 or -1 depending on the encoded data, frequency deviation ω_Δ, and random initial phase θ_x. The usual definition of slow frequency hopping is that $R_\mathrm{s} > R_\mathrm{h}$, so that several symbols are transmitted during a single hop, which is also the case here. The total bandwidth W is divided into M consecutive frequency hopping channels with bandwidths $W/M = W_m$, as is typical for commercial drones in order to provide a robust control link in noisy radio environments [8].

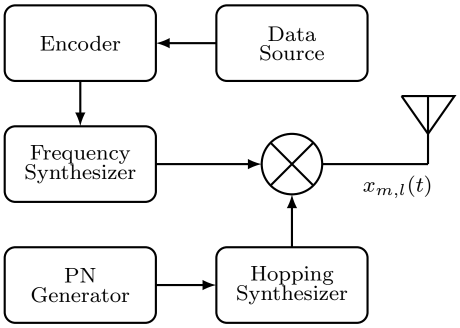


Fig. 2. Block diagram of a slow frequency-hopped binary frequency-shift keying transmitter.

Additionally, in HD mode the remote controller is capable of receiving signals on any of the channels that it is not simultaneously transmitting on, while in FD mode the remote controller is capable of receiving signals on any of the channels at any time, subject to disturbance from residual SI on the channel that it is simultaneously transmitting on. Residual SI refers to the interference that the transmitting node causes to itself, which due to insufficient cancellation interferes with the desired signal being received by that node [1]. The received signals can be either feedback from the drone, interference from the counter-drone system, or both feedback and interference superposed. The remote controller is assumed to be fitted with a feedback receiver, which corresponds to the noncoherent demodulator described in the next subsection.

B. Remote-Controlled Drone

For the purpose of this system model, the main task of the drone is to receive the remote control signals without errors from the operator. The structure of the receiver at the drone is illustrated in Fig. 3. It is assumed that the remote controller and drone have in advance agreed on a frequency hopping pattern and that the dehopping synthesizer is perfectly aligned with the hopping synthesizer. Furthermore, we consider a frequency-flat wideband channel, where each separate subchannel is modeled by the same single complex coefficient. After dehopping, the received complex baseband signal for channel m is

$$y_{m,l}(t) = h_\mathrm{RD}\sqrt{P_\mathrm{x}} \exp\left(il\omega_\Delta t + i\theta_\mathrm{x}\right) + h_\mathrm{JD} j_m(t) + n(t), \tag{2}$$

where h_RD and h_JD are complex coefficients for the channels between the remote controller and the drone and the counter-drone system and the drone respectively, $j_m(t)$ is the interference transmitted by the counter-drone system signal on frequency channel m, and $n(t)$ denotes complex lowpass additive white Gaussian noise with variance $\mathcal{E}\{n^2(t)\} \triangleq \sigma_\mathrm{n}^2$. In order to demodulate the dehopped signal, the task of the noncoherent demodulator is to decide between the two hypotheses

$$H_0 : r_m(t) = y_{m,-1}(t), \tag{3}$$
$$H_1 : r_m(t) = y_{m,+1}(t), \tag{4}$$

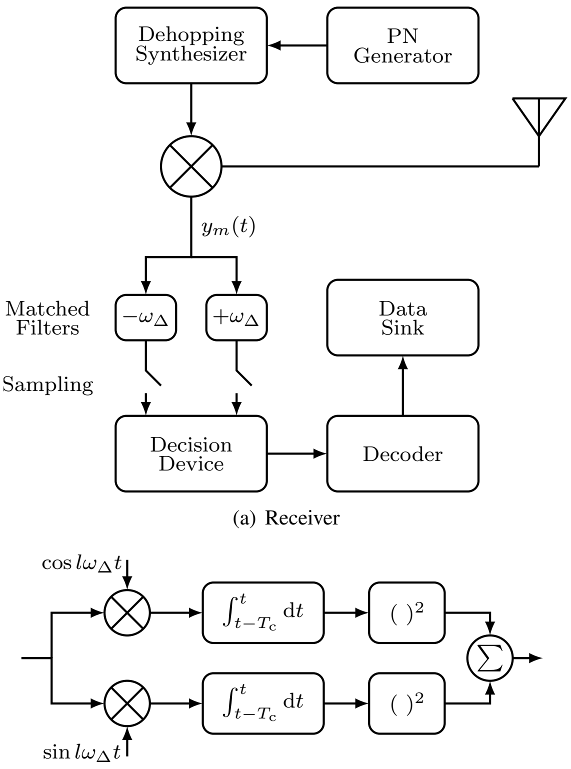
where the signal of interest $y_{m,l}$ has either $l = -1$ or $l = +1$ deviation. The noncoherent demodulator passes the dehopped signal through two matched filters, see Fig. 3(b), the output of which are sampled every $1/R_\mathrm{c}$ and which result in two test statistics $Y_l = \int_0^{T_\mathrm{c}} v_l(t) r_m(t) dt$, where $v_l = \exp\left(i\omega_l t\right)$ is the complex basis function and T_c the coded bit time duration. To decide, which symbol was sent, the two values, Y_{-1} and Y_1, are compared and the largest is chosen.

Finally, decoding is performed to correct the errors. In this work, we assume that block coding is used, which allows us to approximate the information-bit error rate depending on the channel-bit error rate using

$$P_\mathrm{ib} \approx \frac{d}{n} \sum_{i=t+1}^{d} \binom{n}{i} P_\mathrm{cb}^i \left(1 - P_\mathrm{cb}\right)^{n-i} + \frac{1}{n} \sum_{i=d+1}^{n} i \binom{n}{i} P_\mathrm{cb}^i \left(1 - P_\mathrm{cb}\right)^{n-i}, \tag{5}$$

where P_cb is the channel-bit error rate, d is the minimum distance between codewords, $t = \lfloor (d-1)/2 \rfloor$, and n is the length of the codewords [24].

Furthermore, in HD mode the drone is capable of transmitting signals on any of the channels that its not simultaneously receiving on, while in FD mode the drone is capable of transmitting signals on any of the channels at any time, although impacting the receiving performance due to residual SI. The transmitted signals can be either feedback to the remote controller or interference targeting the counter-drone system, if the drone chooses to apply some electronic counter-countermeasures. For transmitting feedback signals, the drone is assumed to be fitted with the same transmitter as described in the previous subsection.



(a) Receiver

(b) Matched filter

Fig. 3. Block diagram of a slow frequency-hopped binary noncoherent frequency-shift keying receiver.

C. Counter-Drone System

The counter-drone system is composed of detection and jamming subsystems and we analyze the counter-drone system with various levels of sophistication that are typical for electronic counter-measure systems [25]. For detecting the remote control signal, the counter-drone system relies on a channelized energy detector as illustrated in Fig. 4, which gives a single binary detection result together with a channel index. It is assumed that the detector uses an energy detector with M channels, and that the detector has an RF front-end that is perfectly matched with the channel frequencies and bandwidths used by the remote controller (for analytical purposes). The task of each of the individual energy detector channels is to decide between the two hypotheses

$$H_0 : r_m(t) = j_m(t) + n(t), \tag{6}$$

$$H_1 : r_m(t) = x_m(t) + j_m(t) + n(t), \tag{7}$$

where the signal of interest x_m is either absent or present. In order to do that, the basic energy detector filters, squares, and integrates the received signal over a period T_d, which results in a test statistic $z_m = 1/T_\mathrm{d} \int_0^{T_\mathrm{d}} |r_m(t)|^2 \, dt$ that is compared to an energy threshold V_T to select between the two hypotheses [26]. The counter-drone system chooses numerically the detection threshold V_T based on the detection time T_d and noise variance σ_n^2 to produce some acceptable constant false alarm rate (CFAR) relying on the propositions in Section III.

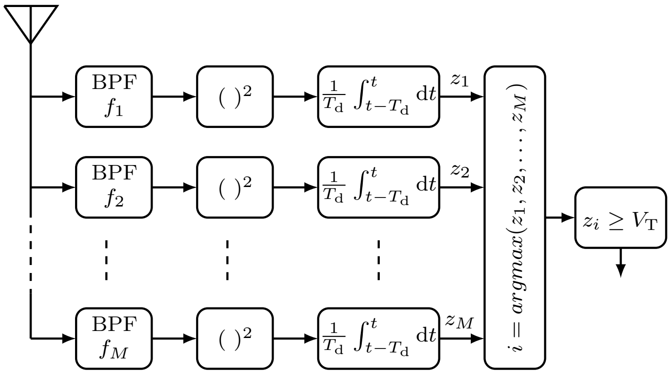

BPF f_1
$(\ )^2$
$\frac{1}{T_\mathrm{d}} \int_{t-T_\mathrm{d}}^{t} \mathrm{d}t$
z_1
BPF f_2
$(\ )^2$
$\frac{1}{T_\mathrm{d}} \int_{t-T_\mathrm{d}}^{t} \mathrm{d}t$
z_2
BPF f_M
$(\ )^2$
$\frac{1}{T_\mathrm{d}} \int_{t-T_\mathrm{d}}^{t} \mathrm{d}t$
z_M
$i = argmax(z_1, z_2, \ldots, z_M)$
$z_i \geq V_\mathrm{T}$

Fig. 4. Block diagram of a channelized energy detector.

We consider that the counter-drone system has the described channelized radiometer based signal detection capability and then it applies either constant, reactive, or follower jamming principles, which are illustrated in Fig. 5 and altogether cover the bulk of the modern jamming strategies.

1) Constant: In the simplest case, the counter-drone system completely avoids the chance of it not detecting the remote control signals, the system does not try to conserve energy, nor does it try to hide the jamming signals. As such, it continuously jams the total bandwidth W using either noise with fixed signal power P_j or linearly frequency-swept interference

$$j_\mathrm{s}(t) = \sqrt{P_\mathrm{j}} \exp\left(i\left(ct/2 + \omega_\mathrm{j}\right)t + i\theta_\mathrm{j}\right) \tag{8}$$

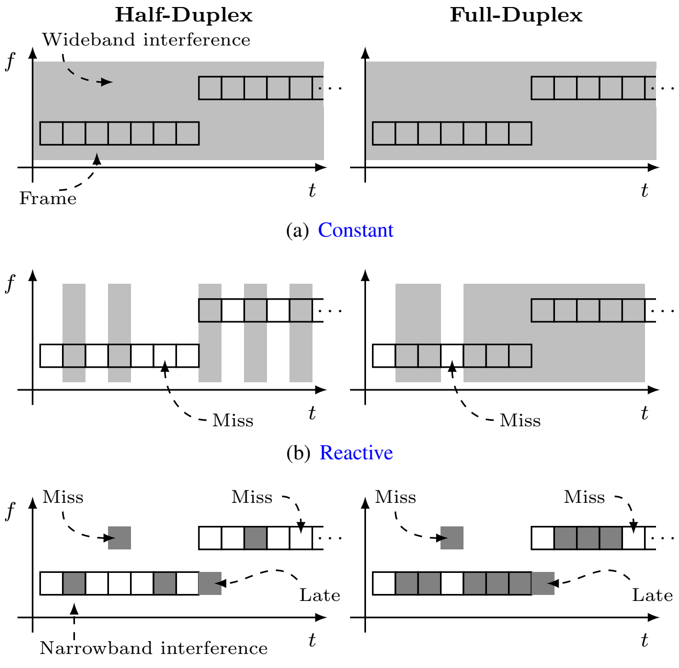
with sweep rate c, arbitrary phase offset θ_j, and fixed signal power P_j. As such, the counter-drone system is strictly limited to jamming if it operates in HD mode. However, in FD mode, the counter-drone system still has the possibility to detect the remote control signals, as long as the signal-to-interference-plus-noise ratio (SINR) allows, even though constant jamming itself does not have any use for this kind of signals intelligence. Still, the information can be useful in a broader perspective within an operational scenario. For example, to notify the counter-drone system operator of an advancing threat, try to estimate the direction of the threat, or perhaps to change the jamming strategy.

2) Reactive: In the more complicated case, the counter-drone system does rely on the channelized radiometer to detect the targeted signal, but does not take into account the detected channel, instead considering the detection result for the whole band using logical-OR combining, i.e., selecting the individual energy detector with highest test statistic $z_i \geq z_k \ \forall \ k$ and comparing that test statistic to the threshold, resulting in

$$\text{detection} = \begin{cases} \text{true}, & \text{if } z_i \geq V_\mathrm{T} \\ \text{false}, & \text{otherwise.} \end{cases} \tag{9}$$

This may be desirable if the counter-drone system is interested in interfering with fast frequency-hopped communications where the reaction time might be insufficient, the propagation delays cause problems, or if in reality the counter-drone system does not have the channel information or capability to process the full bandwidth in a channelized manner [27]. Then, to neutralize the connection between the remote controller and drone, the jamming subsystem of the counter-drone system transmits either noise with total bandwidth W and signal power P_j or linearly frequency-swept interference as in (8) but for time duration T_j. In HD mode, after T_j, the counter-drone system stops jamming and returns to detection mode, while in FD mode, the counter-drone system then continues jamming throughout the next detection stage.

3) Follower: In the most sophisticated and potentially most efficient case, the counter-drone system relies on the complete information produced by the channelized radiometer to follow the targeted signal in the frequency domain [28]. As such, the follower jammer transmits noise with bandwidth W_m and signal power P_j. For the follower jammer, we discard the frequency-swept interference, since the idea behind frequency sweeping is to spread the interference impact across many channels, when the exact channel is unknown. In HD mode, the counter-drone system applying follower jamming is limited to detecting the remote control signals when it is not simultaneously jamming, while in FD mode, the counter-drone system is able to simultaneously jam and detect on all of the channels, subject to SI on the jammed channel. This is a reasonable presumption as we will rely on powerful jammer output powers, for which receiving even on adjacent channels simultaneously to transmitting is challenging in HD mode.



(a) Constant

(b) Reactive

(c) Follower

Fig. 5. Conceptual diagram of frequency-hopped communications and different jamming techniques. The wideband interference can be either wideband noise or frequency-swept narrowband signal. For reactive and follower jamming strategies, the FD operation mode allows to affect a larger portion of the targeted signal frame than HD operation mode.

III. Analysis Techniques

In this section, we present analytical methods for evaluating the detection and demodulation probabilities of frequency-hopped BFSK signal under interference, self-inflicted or otherwise. The methods are presented in terms of

N_d — number of samples per channel,
P_x — received signal power,
P_si — received self-interference power,
P_i — received interference power,
σ_n^2 — noise variance per channel,
c — sweep rate,
V_T — detection threshold, and
M — number of channels.

In Section IV, the methods will be used for studying the remote-controllable flight range of drones and the effective range of counter-drone systems in FD and HD modes.

A. Detection

Since we consider a counter-drone system that operates in HD or FD mode and provides varying levels of details about the spectrum depending on the specific strategy, we present novel expressions for signal detection probabilities for the following separate cases that altogether cover the counter-drone system detection capabilities described in the system model.

Proposition 1. *The steady-state probability of a half-duplex counter-drone system missing a jamming opportunity is*

$$P_\mathrm{MD,F}^\mathrm{HD}\left(N_\mathrm{d}, P_\mathrm{x}, \sigma_n^2, V_\mathrm{T}, M\right) = \\ 1/\left(2 - P_\mathrm{MD,F}\left(N_\mathrm{d}, P_\mathrm{x}, \sigma_n^2, V_\mathrm{T}, M\right)\right) \quad (10)$$

where the probability of missed detection for a channelized energy detector without self-interference is

$$P_\mathrm{MD,F}\left(N_\mathrm{d}, P_\mathrm{x}, \sigma_n^2, V_\mathrm{T}, M\right) = \\ 1 - \frac{1}{2}\int_{V_\mathrm{T}}^{\infty}\left(\frac{x}{\lambda}\right)^{\frac{N_\mathrm{d}-1}{2}}\left(\frac{\gamma\left(N_\mathrm{d}, \frac{x}{2}\right)}{\Gamma\left(N_d\right)}\right)^{M-1} \\ \cdot \exp\left(\frac{-\lambda - x}{2}\right) I_{N_d-1}\left(\sqrt{\lambda x}\right)\mathrm{d}x, \quad (11)$$

where $\lambda = 2N_\mathrm{d}P_\mathrm{x}/\sigma_\mathrm{n}^2$ is the noncentrality parameter, $\gamma(a, x)$ is the lower incomplete gamma function [29, eq. 6.5.2], $\Gamma(z)$ denotes the gamma function [29, eq. 6.1.1], and $I_v(z)$ is the modified Bessel function of the first kind [29, eq. 9.6.3].

Proof. Given V_j, the test statistic for the channel that contains the signals of interest, and that V_i are statistically independent for all i, the probability of the test statistic V_j being larger than any of the other test statistics is

$$\Pr\left(V_i < V_j, \text{ all } i \neq j \mid V_j\right) = \\ \prod_{i=1, i\neq j}^{M} \Pr\left(V_i < V_j \mid V_j\right), \quad (12)$$

where the probability on the right-hand side can be expressed through the cumulative distribution function of a chi-squared distributed random variable so that

$$\Pr\left(V_i < V_j \mid V_j\right) = \frac{\gamma\left(N_\mathrm{d}, \frac{V_j}{2}\right)}{\Gamma\left(N_\mathrm{d}\right)}. \quad (13)$$

Since V_j contains the signal of interest, it has a noncentral chi-squared probability density function (PDF) given by

$$p_{\chi^2}\left(x;N_{\mathrm{d}},\lambda\right)=\frac{1}{2}\left(\frac{x}{\lambda}\right)^{\frac{N_{\mathrm{d}}-1}{2}}\exp\left(\frac{-\lambda-x}{2}\right)I_{N_{\mathrm{d}}-1}\left(\sqrt{\lambda x}\right)\quad(14)$$

and the probability of correct detection is (13) averaged over V_j from V_{T} to ∞, where V_j has the PDF given in (14). Therefore, the single-shot probability of missed detection for a channelized energy detector without self-interference results in the integral given in (11). Considering that the HD counter-drone system is always required to go into detection state after jamming or after a missed detection, the steady-state probability of a HD counter-drone system missing a jamming opportunity is given by (10). □

Proposition 2. *The steady-state probability of a half-duplex counter-drone system with logical-OR energy detector missing a jamming opportunity is*

$$P_{\mathrm{MD,R}}^{\mathrm{HD}}\left(N_{\mathrm{d}},P_{\mathrm{x}},\sigma_n^2,V_{\mathrm{T}},M\right)=1/\left(2-P_{\mathrm{MD,R}}\left(N_{\mathrm{d}},P_{\mathrm{x}},\sigma_n^2,V_{\mathrm{T}},M\right)\right)\quad(15)$$

where the probability of missed detection for a channelized energy detector using logical-OR without self-interference is

$$P_{\mathrm{MD,R}}\left(N_{\mathrm{d}},P_{\mathrm{x}},\sigma_{\mathrm{n}}^2,V_{\mathrm{T}},M\right)=P_{\mathrm{MD}}(N_{\mathrm{d}},P_{\mathrm{x}},\sigma_{\mathrm{n}}^2,V_{\mathrm{T}})\cdot(1-P_{\mathrm{FA}}(N_{\mathrm{d}},\sigma_{\mathrm{n}}^2,V_{\mathrm{T}}))^{M-1},\quad(16)$$

where

$$P_{\mathrm{FA}}(N_{\mathrm{d}},\sigma_{\mathrm{n}}^2,V_{\mathrm{T}})=\frac{\Gamma(N_{\mathrm{d}},\frac{V_{\mathrm{T}}}{\sigma_{\mathrm{n}}^2})}{\Gamma(N_{\mathrm{d}})}\quad(17)$$

and

$$P_{\mathrm{MD}}(N_{\mathrm{d}},P_{\mathrm{x}},\sigma_{\mathrm{n}}^2,V_{\mathrm{T}})=1-Q_{N_{\mathrm{d}}}\left(\sqrt{2N_{\mathrm{d}}P_{\mathrm{x}}/\sigma_{\mathrm{n}}^2},\sqrt{2V_{\mathrm{T}}/\sigma_{\mathrm{n}}^2}\right),\quad(18)$$

with $Q_v(\alpha,\beta)$ being the generalized Marcum Q-function [30, eq. A.16].

Proof. When relying on logical-OR combining at the output of the channelized energy detector, the overall probability of missed detection can be expressed in terms of the probabilities of false alarm $P_{\mathrm{FA}}(N_{\mathrm{d}},\sigma_{\mathrm{n}}^2,V_{\mathrm{T}})$ and missed detection $P_{\mathrm{MD}}(N_{\mathrm{d}},P_{\mathrm{x}},\sigma_{\mathrm{n}}^2,V_{\mathrm{T}})$ for an individual energy detector channel. The probabilities of false alarm and missed detection for an individual energy detector channel without interference are characterized by the noncentral χ^2 distribution as given in (17) and (18) respectively [31]. The probability of missed detection for a channelized energy detector using logical-OR combining is the probability that the detection is missed for the channel that actually contains the signal and that the other channels, which do not contain the signal of interest, do not cause a false alarm. The probability of those independent events occurring together can be estimated using the result in (16). And again, the steady-state probability of a HD counter-drone system missing a jamming opportunity is given by (15). □

Propositions 1 and 2 provide the main tools for analyzing the remote control signal detection performance without SI. With SI, the estimation is further complicated due to the non-uniform noise floor in case of follower jamming and frequency-swept interference in case of reactive jamming.

Proposition 3. *The steady-state probability of a full-duplex counter-drone system missing a jamming opportunity is*

$$\begin{aligned}P_{\mathrm{MD,F}}^{\mathrm{FD}}\left(N_{\mathrm{d}},P_{\mathrm{x}},P_{\mathrm{si}},\sigma_{\mathrm{n}}^2,V_{\mathrm{T}},M\right)=&\\ P_{\mathrm{MD,F}}\left(N_{\mathrm{d}},P_{\mathrm{x}}\sigma_{\mathrm{n}}^2/\left(P_{\mathrm{si}}+\sigma_{\mathrm{n}}^2\right),\sigma_{\mathrm{n}}^2,V_{\mathrm{T}},M\right)&\\ /\big(P_{\mathrm{MD,F}}\left(N_{\mathrm{d}},P_{\mathrm{x}}\sigma_{\mathrm{n}}^2/\left(P_{\mathrm{si}}+\sigma_{\mathrm{n}}^2\right),\sigma_{\mathrm{n}}^2,V_{\mathrm{T}},M\right)&\\ +1-P_{\mathrm{MD,F}}\left(N_{\mathrm{d}},P_{\mathrm{x}},\sigma_{\mathrm{n}}^2,V_{\mathrm{T}},M\right)\big).&\quad(19)\end{aligned}$$

Proof. We assume that the energy detector knows the residual SI power and normalizes the integrated energy in the affected channel to have the same distribution as the channels without the SI. This is equivalent to defining separate detection thresholds for the channels with and without SI based on a desired CFAR. In either case, the detector-jammer then has two states — firstly, the SI is occupying a different channel as the signal of interest or there being no SI at all due to previous missed detection and, secondly, the SI is occupying the same channel as the signal of interest. In the first case, the probability of missed detection is simply given by (11) as

$$P_{\mathrm{MD,F}}\left(N_{\mathrm{d}},P_{\mathrm{x}},\sigma_{\mathrm{n}}^2,V_{\mathrm{T}},M\right),$$

whereas in the second case the probability of missed detection due to the normalization of the integrated energy is given by (11) as

$$P_{\mathrm{MD,F}}\left(N_{\mathrm{d}},P_{\mathrm{x}}\sigma_{\mathrm{n}}^2/\left(P_{\mathrm{si}}+\sigma_{\mathrm{n}}^2\right),\sigma_{\mathrm{n}}^2,V_{\mathrm{T}},M\right).$$

These probabilities give us the transition probabilities of a two-state Markov chain [32]. The steady-state distribution, or the overall missed detection probability, becomes (19). □

Proposition 4. *The steady-state probability of a full-duplex counter-drone system with logical-OR energy detector missing a jamming opportunity under wideband noise-like self-interference is*

$$\begin{aligned}P_{\mathrm{MD,R}}^{\mathrm{FD}}\left(N_{\mathrm{d}},P_{\mathrm{x}},P_{\mathrm{si}},\sigma_{\mathrm{n}}^2,V_{\mathrm{T}},M\right)=&\\ P_{\mathrm{MD,R}}\left(N_{\mathrm{d}},P_{\mathrm{x}}\sigma_{\mathrm{n}}^2/\left(P_{\mathrm{si}}+\sigma_{\mathrm{n}}^2\right),\sigma_{\mathrm{n}}^2,V_{\mathrm{T}},M\right)&\\ /\big(P_{\mathrm{MD,R}}\left(N_{\mathrm{d}},P_{\mathrm{x}}\sigma_{\mathrm{n}}^2/\left(P_{\mathrm{si}}+\sigma_{\mathrm{n}}^2\right),\sigma_{\mathrm{n}}^2,V_{\mathrm{T}},M\right)&\\ +1-P_{\mathrm{MD,R}}\left(N_{\mathrm{d}},P_{\mathrm{x}},\sigma_{\mathrm{n}}^2,V_{\mathrm{T}},M\right)\big).&\quad(20)\end{aligned}$$

Proof. Similarly to the proof of Proposition 3, we assume that the energy detector knows the residual SI power and normalizes the integrated energy in all of the channels to have the same distribution as the channels would without the SI. This is equivalent to defining a separate detection thresholds for detection with and without SI based on a desired CFAR. In either case, the detector-jammer then has two states — firstly, there is no SI due to previous missed detection or, secondly, the SI is hampering the detection of the signal of interest. In the first case, the probability of missed detection is simply given by (16) as

$$P_{\mathrm{MD,R}}\left(N_{\mathrm{d}},P_{\mathrm{x}},\sigma_{\mathrm{n}}^2,V_{\mathrm{T}},M\right),$$

whereas in the second case the probability of missed detection due to the normalization of the integrated energy is given by (16) as

$$P_{\mathrm{MD,R}}\left(N_{\mathrm{d}}, P_{\mathrm{x}}\sigma_{\mathrm{n}}^2/\left(P_{\mathrm{si}}+\sigma_{\mathrm{n}}^2\right), \sigma_{\mathrm{n}}^2, V_{\mathrm{T}}, M\right).$$

These probabilities give us the transition probabilities of a two-state Markov chain. The steady-state distribution, or the overall missed detection probability, becomes (20). □

From (18), it directly follows that the false alarm probability under unknown deterministic interference for an individual energy detector is

$$P_{\mathrm{FA}}^{\mathrm{SI}}(N_{\mathrm{d}}, P_{\mathrm{si}}, \sigma_{\mathrm{n}}^2, V_{\mathrm{T}}) = Q_{N_{\mathrm{d}}}\left(\sqrt{2N_{\mathrm{d}}P_{\mathrm{si}}/\sigma_{\mathrm{n}}^2}, \sqrt{2V_{\mathrm{T}}/\sigma_{\mathrm{n}}^2}\right). \quad (21)$$

In order to calculate the probability of missed detection under unknown deterministic interference for an individual energy detector, the signal-and-interference to noise ratio must be considered instead of the signal-to-noise ratio (SNR). So that (18) becomes

$$P_{\mathrm{MD}}^{\mathrm{SI}}(N_{\mathrm{d}}, P_{\mathrm{x}}, P_{\mathrm{si}}, \sigma_{\mathrm{n}}^2, V_{\mathrm{T}}, \rho_{k,l}) = 1 - Q_{N_{\mathrm{d}}}\left(\sqrt{2\gamma}, \sqrt{2V_{\mathrm{T}}/\sigma_{\mathrm{n}}^2}\right), \quad (22)$$

and where γ is the signal-and-interference to noise ratio of the superposed signal-of-interest and interference signals as

$$\gamma = \frac{P_{\mathrm{x}} + P_{\mathrm{si}} + \sqrt{P_{\mathrm{x}}P_{\mathrm{si}}}\Re\{\rho_l\}}{\sigma_{\mathrm{n}}^2}, \quad (23)$$

where $\Re\{z\}$ denotes the real part of a complex-valued variable and ρ_l is the correlation coefficient between the signal of interest $x_{k,l}$ and interference j_k that for frequency-swept interference can be estimated using Proposition 6.

The probability of missed detection using logical-OR without interference is given by the probability of independent events that the signal of interest is missed in the channel where it exists and a false alarm does not occur in any other channels as [33]

$$P_{\mathrm{MD,R}}(N_{\mathrm{d}}, P_{\mathrm{x}}, \sigma_{\mathrm{n}}^2, V_{\mathrm{T}}, M) = P_{\mathrm{MD}}(N_{\mathrm{d}}, P_{\mathrm{x}}, \sigma_{\mathrm{n}}^2, V_{\mathrm{T}}) \cdot (1 - P_{\mathrm{FA}}(N_{\mathrm{d}}, \sigma_{\mathrm{n}}^2, V_{\mathrm{T}}))^{M-1}. \quad (24)$$

When interference and signal of interest are in the same channel this becomes

$$P_{\mathrm{MD,R}}^{\mathrm{SI,1}}(N_{\mathrm{d}}, P_{\mathrm{x}}, \sigma_{\mathrm{n}}^2, V_{\mathrm{T}}, M) = P_{\mathrm{MD}}^{\mathrm{SI}}(N_{\mathrm{d}}, P_{\mathrm{x}}, P_{\mathrm{si}}, \sigma_{\mathrm{n}}^2, V_{\mathrm{T}}, \rho_{k,l}) \cdot (1 - P_{\mathrm{FA}}(N_{\mathrm{d}}, \sigma_{\mathrm{n}}^2, V_{\mathrm{T}}))^{M-1}. \quad (25)$$

If both occupy different channels, the probability becomes

$$P_{\mathrm{MD,R}}^{\mathrm{SI,2}}(N_{\mathrm{d}}, P_{\mathrm{x}}, \sigma_{\mathrm{n}}^2, V_{\mathrm{T}}, M) = P_{\mathrm{MD}}(N_{\mathrm{d}}, P_{\mathrm{x}}, \sigma_{\mathrm{n}}^2, V_{\mathrm{T}}) \cdot (1 - P_{\mathrm{FA}}^{\mathrm{SI}}(N_{\mathrm{d}}, P_{\mathrm{si}}, \sigma_{\mathrm{n}}^2, V_{\mathrm{T}})) \cdot (1 - P_{\mathrm{FA}}(N_{\mathrm{d}}, \sigma_{\mathrm{n}}^2, V_{\mathrm{T}}))^{M-2}. \quad (26)$$

With uniform frequency hopping, the probability that interference and remote control (RC) signal are in the same channel is $1/M$ and the overall probability of missed detection is the sum of the probabilities of the two mutually exclusive events.

Proposition 5. *The probability of false alarm under frequency-swept interference for a channelized radiometer using logical-OR is*

$$P_{\mathrm{FA,R}}^{\mathrm{SI}}\left(N_{\mathrm{d}}, P_{\mathrm{si}}, \sigma_{\mathrm{n}}^2, V_{\mathrm{T}}, M\right) = 1 - (1 - P_{\mathrm{FA}}^{\mathrm{SI}}(N_{\mathrm{d}}, P_{\mathrm{si}}, \sigma_{\mathrm{n}}^2, V_{\mathrm{T}})) \cdot (1 - P_{\mathrm{FA}}(N_{\mathrm{d}}, \sigma_{\mathrm{n}}^2, V_{\mathrm{T}}))^{M-1}. \quad (27)$$

Proof. The probability of false alarm when using logical-OR without interference is given by the probabilities that in none of the channels a false alarm occurs [33]

$$P_{\mathrm{FA,R}}\left(N_{\mathrm{d}}, \sigma_{\mathrm{n}}^2, V_{\mathrm{T}}, M\right) = 1 - (1 - P_{\mathrm{FA}}(N_{\mathrm{d}}, \sigma_{\mathrm{n}}^2, V_{\mathrm{T}}))^M. \quad (28)$$

With interference, which for the integration time stays within a single channel, the probability of false alarm for that channel is given by (21) and the logical-OR result becomes (27). □

Proposition 6. *Correlation coefficient between a BFSK signal and frequency-swept interference can be estimated from*

$$\rho_l\left(\omega_{\mathrm{j}}, \omega_\Delta, \theta, c, T\right) = \exp\left(i\theta - i\frac{\left(\omega_{\mathrm{j}} + l\omega_\Delta\right)^2}{2c}\right) \left(\frac{1+i}{2}\right)\sqrt{\frac{\pi}{c}}\left(\operatorname{erf}\left(\frac{(1-i)\left(\omega_{\mathrm{j}} + l\omega_\Delta\right)}{2\sqrt{c}}\right) - \operatorname{erf}\left(\frac{(1-i)\left(cT + \omega_{\mathrm{j}} + l\omega_\Delta\right)}{2\sqrt{c}}\right)\right), \quad (29)$$

where erf *is the complex error function [29, eq. 7.1.1].*

Proof. Correlation of a tone and frequency-swept signal is

$$\rho_l = \int_0^T \exp\left(i\left(ct^2/2 + \omega_{\mathrm{j}}t + \theta\right)\right)\exp\left(-il\omega_\Delta t\right)\mathrm{d}t \quad (30)$$

$$= \int_0^T \exp\left(i\left(ct^2/2 + \left(\omega_{\mathrm{j}} - l\omega_\Delta\right)t + \theta\right)\right)\mathrm{d}t. \quad (31)$$

Using rule [34, eq. (5.A2)], this simplifies to

$$\rho_l = \exp\left(i\theta - i\frac{\left(\omega_{\mathrm{j}} + l\omega_\Delta\right)^2}{2c}\right)\left(\frac{1+i}{2}\right)\sqrt{\frac{\pi}{c}} \operatorname{erf}\left(\frac{(1-i)\left(ct + \omega_{\mathrm{j}} + l\omega_\Delta\right)}{2\sqrt{c}}\right)\Bigg|_0^T \quad (32)$$

that evaluated from 0 to T results in (29). □

Since frequency-swept interference can have any frequency and phase offsets at the beginning of the integration period, the overall missed detection probability for an individual radiometer is obtained by averaging the phase θ over interval $(0, 2\pi)$ and frequency ω_{j} over the relevant interval.

B. Demodulation

In order to evaluate the demodulation bit error rate under interference, the challenge becomes to determine the probability by which one Rician random variable fluctuates above another. It has been previously shown that for uncorrelated Rician random variables, i.e., orthogonal BFSK, this probability can be calculated using

$$P_{\mathrm{e}}(N_{\mathrm{d}}, P_{\mathrm{x}}, \sigma_{\mathrm{n}}^2, \rho) = \frac{1}{2}\left[1 + Q_1\left(\sqrt{b}, \sqrt{a}\right) - Q_1\left(\sqrt{a}, \sqrt{b}\right)\right], \tag{33}$$

where variables a and b denote the ratios between the deterministic and nondeterministic signal components in either of the BFSK branches such as $a = N_{\mathrm{d}} P_{\mathrm{x}} / \sigma_{\mathrm{n}}^2$ and $b = 0$ for $x_{k,-1}$ transmitted. In case of correlated Rician variables, i.e. nonorthogonal BFSK, the variables must first be decorrelated [35], resulting in

$$a = \frac{N_{\mathrm{d}} P_{\mathrm{x}}}{2\sigma_{\mathrm{n}}^2}\left(1 + \sqrt{1 - |\rho|^2}\right) \qquad b = \frac{N_{\mathrm{d}} P_{\mathrm{x}}}{2\sigma_{\mathrm{n}}^2}\left(1 - \sqrt{1 - |\rho|^2}\right)$$

where $\rho = |\rho| e^{i\alpha}$ is the correlation coefficient between $x_{k,-1}$ and $x_{k,+1}$.

Proposition 7. *The probability of bit error for noncoherent BFSK demodulator under deterministic interference is*

$$P^{\mathrm{I}}{}_{\mathrm{e}}\left(N_{\mathrm{d}}, P_{\mathrm{x}}, P_{\mathrm{i}}, \sigma_{\mathrm{n}}^2, \rho, \rho_l\right) = \frac{1}{2}\left[1 + Q_1\left(\sqrt{b_l}, \sqrt{a_l}\right) - Q_1\left(\sqrt{a_l}, \sqrt{b_l}\right)\right], \tag{34}$$

where

$$a_l = \frac{P_{\mathrm{i}} N_{\mathrm{d}}}{4\sigma_{\mathrm{n}}^2\left(|\rho| + 1\right)}\Big(\left(C + \rho_l\right)\left(\beta + 1\right) e^{i\alpha} - \left(\beta - 1\right)\left(C\rho + \rho_{-l}\right)\Big)^2 e^{-2i\alpha}, \tag{35}$$

$$b_l = \frac{P_{\mathrm{i}} N_{\mathrm{d}}}{4\sigma_{\mathrm{n}}^2\left(|\rho| + 1\right)}\Big(-\left(C + \rho_l\right)\left(\beta - 1\right) e^{i\alpha} + \left(\beta + 1\right)\left(C\rho + \rho_{-l}\right)\Big)^2 e^{-2i\alpha}, \tag{36}$$

$C = \sqrt{P_{\mathrm{x}}/P_{\mathrm{i}}}$ *and* $\beta = \sqrt{\left(1 + |\rho|\right) / \left(1 - |\rho|\right)}$.

Proof. The underlying correlated Rician random variables of the test statistics are $y_1 = v_{-1}^* r_k / \sigma_{\mathrm{n}}^2$ and $y_2 = v_{+1}^* r_k / \sigma_{\mathrm{n}}^2$. The means of those correlated variables are $\langle y_1 \rangle = \sqrt{P_{\mathrm{x}}}\sigma_{\mathrm{n}}(1 + \frac{\rho_l}{C})$ and $\langle y_2 \rangle = \sqrt{P_{\mathrm{x}}}\sigma_{\mathrm{n}}(\rho + \frac{\rho_{-l}}{C})$. In [35] the decorrelation transformation is given by

$$\langle x_1 \rangle = \langle y_1 \rangle \left(1 + \beta\right) b + \langle y_2 \rangle (1 - \beta) b e^{-i\alpha}, \tag{37}$$

$$\langle x_2 \rangle = \langle y_1 \rangle \left(1 - \beta\right) b + \langle y_2 \rangle (1 + \beta) b e^{-i\alpha}, \tag{38}$$

where $b = \frac{1}{\sqrt{4\beta}}$. Applying the transformation, we get

$$\langle x_1 \rangle = \frac{\sqrt{P_{\mathrm{x}}}\sigma_{\mathrm{n}}}{2C\sqrt{\beta}}\Big(\left(C + \rho_l\right)\left(\beta + 1\right) e^{i\alpha} - \left(\beta - 1\right)\left(C\rho + \rho_{-l}\right)\Big) e^{-i\alpha}, \tag{39}$$

$$\langle x_2 \rangle = \frac{\sqrt{P_{\mathrm{x}}}\sigma_{\mathrm{n}}}{2C\sqrt{\beta}}\Big(-\left(C + \rho_l\right)\left(\beta - 1\right) e^{i\alpha} + \left(\beta + 1\right)\left(C\rho + \rho_{-l}\right)\Big) e^{-i\alpha}. \tag{40}$$

As a result of this transformation, variance of the newly created uncorrelated complex Gaussian variables is $\sigma_{x_1}^2 = \sigma_{x_2}^2 = 4b^2(1 + \rho)$ [36, pp. 226–231] and therefore arguments of the Q-function in (33) are given by $\frac{\langle x_1 \rangle^2}{4b^2(1+\rho)}$ and $\frac{\langle x_2 \rangle^2}{4b^2(1+\rho)}$ that result in (35) and (36). Thus, the probability of selecting the erroneous bit is given by (34). □

Again, ρ_l can be calculated using (29). The overall probability of bit error is obtained by averaging the phase θ over region $(0, 2\pi)$ and frequency ω_j over the relevant interval.

IV. Results and Analysis

We compare the advantages and disadvantages of FD and HD in three different counter-drone scenarios. In the first scenario, we evaluate the counter-drone system's ability to minimize the area into which a remote-controlled drone can intrude (i.e., minimizing the intrusion area). In the second scenario, we consider the drone's ability to maximize the area in which it can operate in the presence of a malicious counter-drone system (i.e., maximizing the operable area). In the third scenario, we study the drone's ability to detect malicious interference at ineffective levels to prevent entering areas in which the interference would become effective. Table I summarizes operation configurations of the three devices (remote controller (RC), drone (UAV), and counter-drone system (CDS)) in the considered scenarios. The highlighted background in the table indicates the comparison in question for any given scenario. Finally, we also analyse the energy efficiency of different counter-drone system strategies and the effect of elevation to a counter-drone scenario.

TABLE I
Summary of Scenarios

Operation / Scenario	Transmit	Receive	Interfere	Detect	Device
1	HD	HD			RC
	HD	HD			UAV
			HD/FD	HD/FD	CDS
2	HD/FD	HD/FD			RC
	HD/FD	HD/FD			UAV
			HD/FD	HD/FD	CDS
3	HD	HD			RC
	HD/FD	HD		HD/FD	UAV
			HD/FD	HD/FD	CDS

The following parameters are used in the system model to represent realistic situations in terms of the capabilities of the devices and their surrounding environment. The parameter values do not strictly correspond to specific systems, but are close to what can be found in many remote-controlled drone and counter-drone systems [37], [38]. The total bandwidth used by the remote control link is taken to be 80 MHz and it is divided into 160 equally spaced channels with bandwidths of 0.5 MHz. The remote controller and drone transmit BFSK signal with frequency deviation of 200 kHz, encoded data rate 25 kbps, and frequency hopping rate of 40 hops per second.

The remote controller and drone both have transmit output powers of 20 dBm in HD mode, while the counter-drone system has an output power of 40 dBm regardless of the operation mode. The drone system halves its output power in FD mode to retain the same energy-per-bit ratio as in HD mode, while the counter-drone system uses always the highest possible output power to maximise its impact. For frequency sweep jamming, 2.5 kHz sweep rate is used, meaning that the interference covers 16 channels during a single bit transmission, giving a good chance of high bit error rate (BER) even at low jammer-to-signal ratios (JSRs). The noise floor in a 0.5 MHz channel is taken to be -90 dBm. Both the signal detection and jamming times are taken to be 1.6 ms, hence the HD counter-drone system uses a 50% duty cycle.

We consider the radio link between the remote controller and drone to be functional as long as the channel-bit error rate in both ways is less than 1%. With a moderate coding rate, this would allow to reach an information-bit error rate that suffices for the repetitive nature of drone remote control. For example, using Golay (23, 12) code and relying on (5), we can approximate that channel-bit error rate of 1% allows to reach information-bit error rate of about 10^{-5} after decoding.

We assume that the drone is always operated at an elevation of 100 m above ground level, while the other nodes are at ground level unless stated otherwise. The ground-to-air channel between the remote controller and the drone is in practice clearly distinguishable from the conventional ground-to-ground channel between the remote controller and the counter-drone system [39]. Furthermore, a third, air-to-air, channel model is required if any two of the three nodes are in the air. Therefore, in order take these differences into account, we rely on empirical studies that have characterized the air-to-air, ground-to-air, and ground-to-ground channels in wireless drone communications, and take the path loss exponents in those channels to be 2.0, 2.2, and 3.3 respectively [40], [41].

A. Verification of Analytical Expressions

Before using the analysis techniques developed in Section III for studying the three scenarios, we first compare the analytical results to simulated ones, in order to verify that the proposed techniques are accurate. We begin by checking the probabilities of correct detection and false alarm by the counter-drone system in FD and HD mode (i.e., with and without SI). Using Propositions 3 through 5, which build on Propositions 1 and 2, we have evaluated the receiver operating characteristic (ROC) curves and plotted them together with the simulated results in Fig. 6. The reactive jammer with noise ($\mathrm{RJ_n}$) or frequency-swept interference ($\mathrm{RJ_s}$) is guaranteed to correctly detect the presence of the signal of interest with low enough threshold, while the follower jammer ($\mathrm{FJ_n}$) is not guaranteed to choose the correct channel. And, as expected, we observe flattening of the ROC curves as the residual SI level increases when using noise as interference, but not when using a deterministic signal. Overall, the results indicate that the analytical estimations are closely matched with the simulated results.

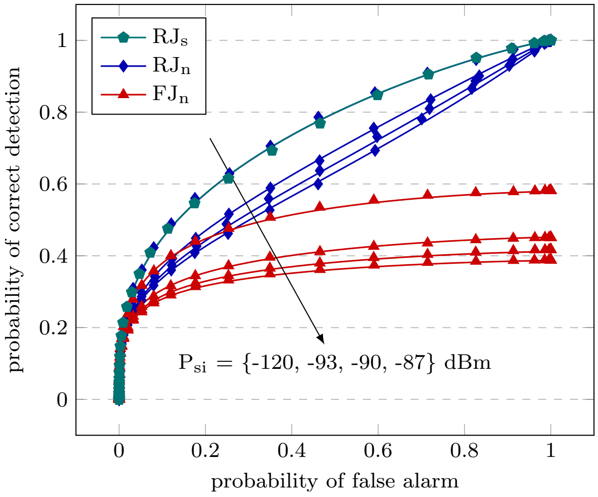


Fig. 6. Receiver operating characteristic curves of the counter-drone system with different detection strategies and at varying levels of self-interference. Solid lines represent the analytical and marks the simulated results.

Since we can now be confident in our detection estimation accuracy, we present the demodulation results by building on the detection analysis. That is, we compare the estimated and simulated channel-bit error rates at the drone, whereas the counter-drone system is first required to detect the signal transmitted by the remote controller. Using additionally Propositions 6 and 7, we estimate the bit error rate at the drone receiver depending on the strategy and mode of the counter-drone system. The simulated and analytical results are presented in Fig. 7. As expected, follower jamming becomes effective at lower JSRs than reactive jamming because it is able to overcome the processing gain of frequency hopping. Also, reactive frequency-swept interference has the potential to become effective at lower JSRs than reactive noise jamming, since the interference is concentrated to just 10% of the total bandwidth during a single symbol transmission. Similarly, FD operation mode becomes effective at lower JSRs than HD because it is able to spend more time in jamming mode.

It is interesting to note that, as the SNR at the counter-drone system worsens, the performance difference between FD and HD counter-drone system diminishes. That is because the FD system stops taking advantage of its ability to jam continuously due to the missed detections. Together the results in Fig. 6 and Fig. 7 cover the analysis techniques presented in Section III and indicate a good match between estimated and simulated results. This allows us to confidently present the following scenarios relying purely on the analytical functions. Using the analytical functions is is significantly less computing intensive than running simulations, especially considering the vast amount of data points that will be considered next to cover the scenarios.

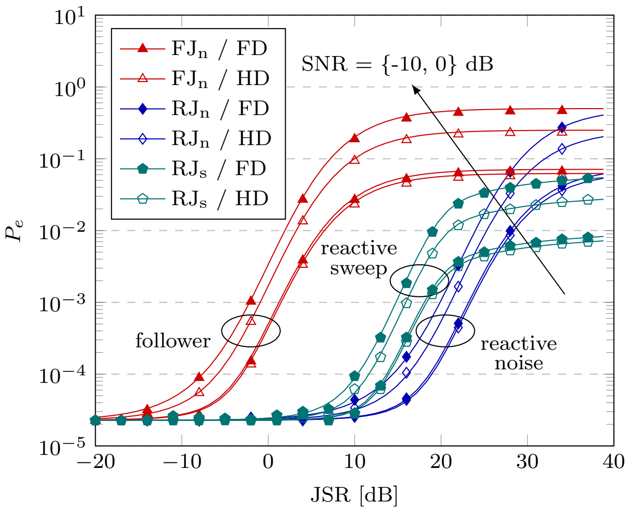


Fig. 7. Bit error rate at a frequency-hopped BFSK receiver under reactive or follower jamming at different SNRs at the counter-drone system. The detection threshold at the counter-drone system is chosen so that the false alarm rate is 1%. Solid lines represent the analytical and marks the simulated results.

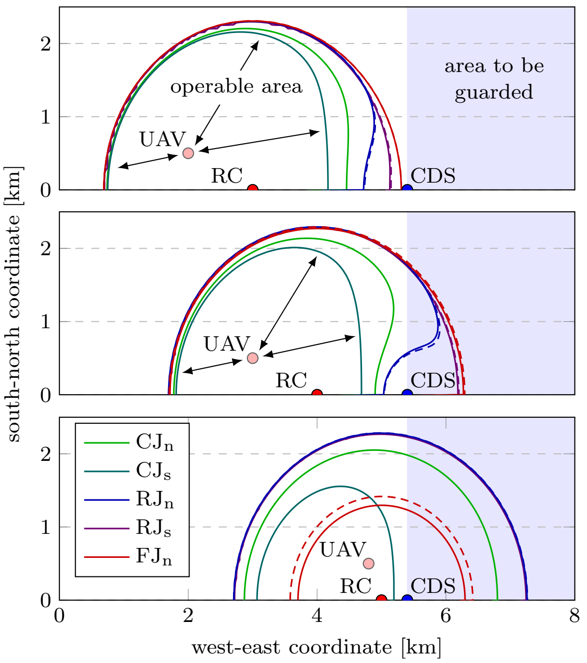


Fig. 8. Operable area of a remote-controlled drone against a counter-drone system. Results for counter-drone system in FD operation mode are plotted in solid lines and HD in dashed lines.

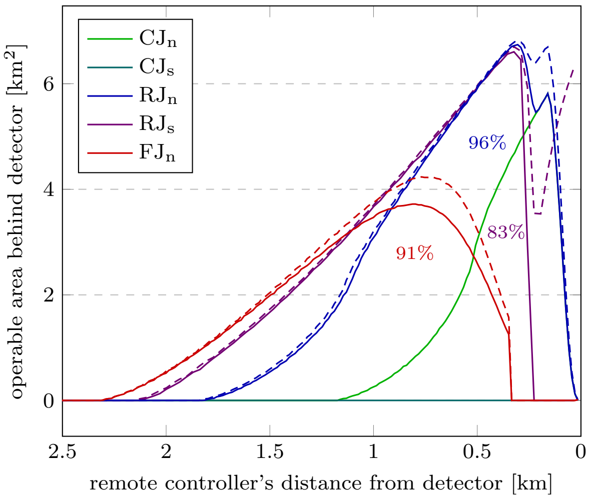


Fig. 9. Area behind the counter-drone system in which a malicious drone can be controlled. The reactive and follower jammers are operated with a constant false alarm rate of 10%. Results for FD counter-drone system are plotted in solid lines and HD in dashed lines.

B. Scenario 1 (Minimizing Intrusion Area)

In the first scenario, we consider the defensive counter-drone system perspective as illustrated in Fig. 8. The counter-drone system is positioned in front of an area that is to be restricted to drones. This could be, e.g., national border, prison or airport perimeter, or around some critical infrastructure. The drone operator aims to control the drone to enter the area behind the counter-drone system and the counter-drone system aims to minimize the area behind itself in which the drone can be remote-controlled. Using all of the derived analytical functions, we study which counter-drone system strategies and operation modes are most efficient in reducing the intrusion area. The operational area depends on the position of the remote controller relative to the counter-drone system and Fig. 8 illustrates how the different strategies and operation modes limit the operational area of the remote-controlled drone at different remote controller positions. The illustration shows that FD operation outperforms HD to some extent in any case due to more time spent jamming, but the efficiency of the different strategies is a more significant factor than the operation mode.

In Fig. 9, the area that can be covered by a malicious drone behind a counter-drone system is plotted for different jamming strategies and modes depending on the remote controller's distance from the counter-drone system. From those results, several conclusions can be drawn. Due to the differences in the ground-to-air and ground-to-ground channels, the counter-drone system is at a significant disadvantage compared to the drone when detecting the remote control signals. As such, when the remote controller is far away from the counter-drone system, i.e., the remote control signal received by the counter-drone system is weak, constant jamming outperforms other strategies. Of course this increases the detectability of the counter-drone system. If detectability is not a concern, then using constant jamming and switching to follower jamming after confidently detecting the remote control signals would be the optimal strategy for reducing the operable area. It is also evident that, compared to HD reactive and follower jammers, their FD counterparts reduce the operable area somewhat. Depending on the strategy, the operable area is reduced by 4% to 17%. This is due to the FD counter-drone system being able to spend more time in jamming mode than its HD counterpart.

C. Scenario 2 (Maximizing Operable Area)

In the second scenario, we consider the defensive drone point of view. Specifically, we analyze the situation where a remote-controlled drone is flying over an area that it surveys as illustrated in Fig. 10. Similarly to the first scenario, this could be, e.g., a national border or the perimeter of any restricted area. The malicious counter-drone system aims to neutralize the drone in order to carry out some activity in the surveyed area unseen and the drone aims to maximize the area in which it can be remote-controlled and send feedback to the operator. Given that the counter-drone system is either HD or FD and uses some neutralization strategy, the question then is which operation mode between the remote controller and drone is most beneficial from the drone's perspective. We consider that the remote controller and drone use the same energy per bit ratio in both FD and HD operation modes. That is, in FD mode the symbol transmission time is doubled but the transmission power is halved compared to the HD mode.

Fig. 10 gives results for some node placements. The actual area in which the drone can be remote-controlled decreases as the counter-drone system approaches the remote controller. Due to the different channel models, if the drone is transmitting and receiving at the same time (i.e., FD mode), it becomes a much easier target than in the HD time division mode when the counter-drone system needs to detect the signals from the remote controller. Therefore, using FD for two-way communications between the remote controller and drone make the drone system highly vulnerable to jamming attacks. Fig. 11 gives the operable areas as depending on the counter-drone system's distance from the remote controller. The operable area in FD mode can be reduced to as little as couple percent of that in HD mode. The results highlight the relative vulnerability of FD two-way communications between a drone and its remote controller compared to HD operation. This is a considerable issue that affects many potential FD drone applications.

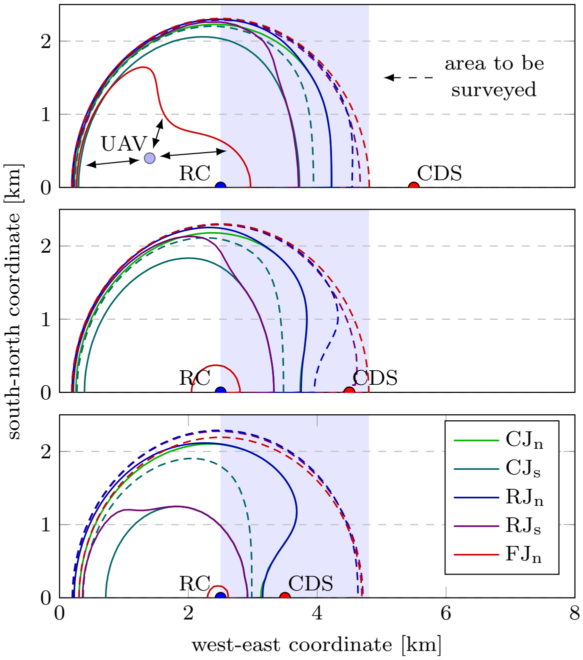


Fig. 10. Area in which a drone can be controlled. The reactive and follower jammers are operated in FD mode with a constant false alarm rate of 10%. Solid lines represent operable area in FD remote control mode and dashed lines in HD mode.

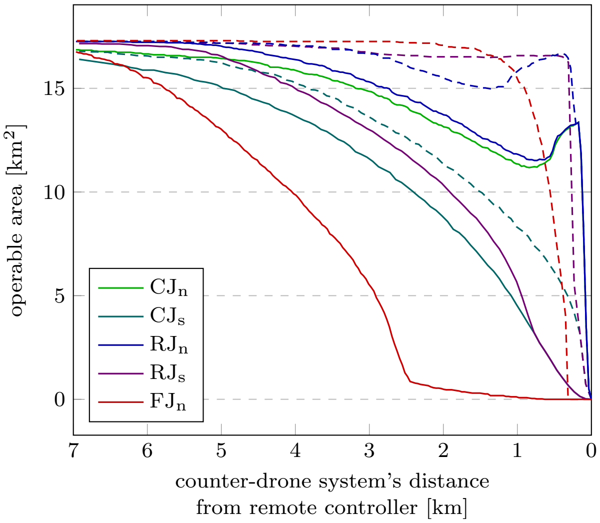


Fig. 11. Illustration of the area in which a drone can be controlled. The reactive and follower jammers are operated in FD mode with a constant false alarm rate of 10%. Solid lines represent operable area in FD remote control mode and dashed lines in HD mode.

D. Scenario 3 (Detecting Counter-Measures)

In the third scenario, we continue with the defensive drone point of view, but we analyze the drone's ability to detect intentional interference from the counter-drone system to make sure that the drone does not enter the area in which it would be immobilized or that the drone can back off from an approaching counter-drone system. This could again be applicable in a situation where the remote-controlled drone is flying over an area that it surveys. The counter-drone system aims to disable the drone in order to reduce the situational awareness about the area and the drone aims to avoid becoming disabled by detecting the counter-measures applied by the adversarial counter-drone system. In this scenario we only consider the follower jammer, which can be the most difficult to detect.

Fig. 12 illustrates the scenario — the drone is positioned at some distance from the remote controller, leaving it to be vulnerable to jamming attacks. The effective jamming area, in which the counter-drone system needs to be positioned to be effective, is shown in red. The counter-drone system detection area, in which the counter-drone system needs to be position to be detected by the drone system, is shown in blue. The results show that jamming detection in FD mode can lead to up to 60% increase of the detection area compared to HD mode. The FD-enhanced remote controller and drone have a considerable advantage over their HD-limited counterparts because simultaneous transmission and detection capability allows to detect the jamming attacks more consistently. Without that capability, HD drone is limited to detecting the counter-drone system's attacks only when the counter-drone system targets a wrong channel or is too late with its attack against a recently vacated channel. As such, jamming detection in FD mode is more certain to be able to detect the malicious interference before becoming immobilized by it. Depending on the direction from which the counter-drone system approaches, HD detection might miss the adversary altogether before becoming paralyzed.

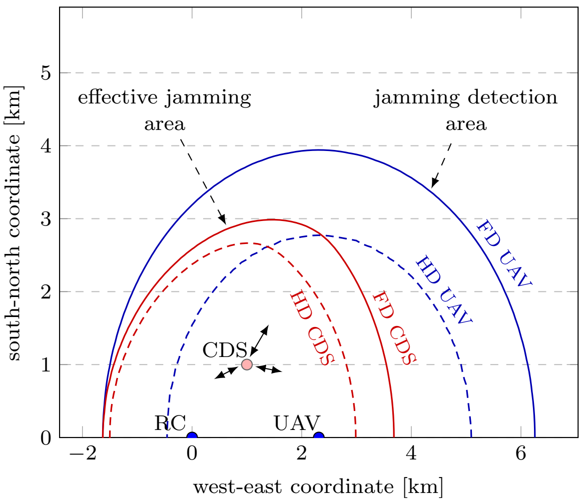


Fig. 12. Comparison on jamming detection by drone systems with HD and FD capabilities. For illustration, the effective jamming area is also plotted, which allows to get some sense about the drone's capability to detect ineffective interference and avoid entering an area where interference becomes effective.

In Fig. 13, counter-drone system detectability is plotted depending on the false alarm rate used by the counter-drone system. Furthermore, P_d is the target detection rate at the drone, i.e., the percentage of jamming attempts that are required to be detected. As the detection threshold at the counter-drone system is lowered, i.e., the false alarm rate is increased, the counter drone system is less discerning about the channels that it attacks, consequently becoming detectable from a greater distance.

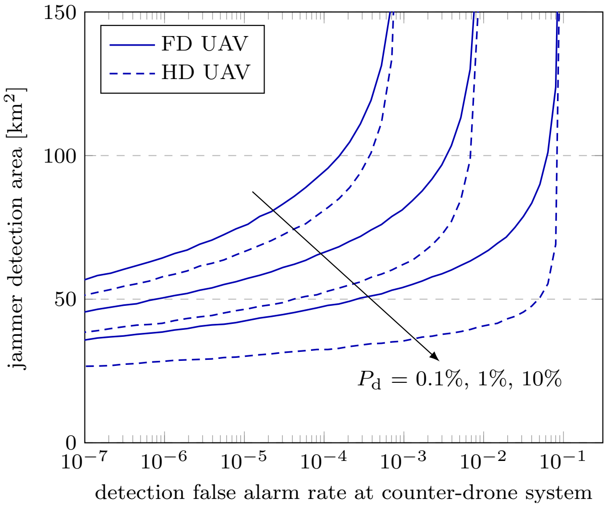


Fig. 13. Comparison of areas in which HD and FD drone system can detect a counter-drone system that is using the follower jamming strategy. The area depends on the detection thresholds at either node and the operation mode.

E. *Energy Efficiency and Elevation*

Since high-power jamming takes a lot of energy, it could be beneficial to take into account the energy efficiency of different counter-drone strategies. For example, constant jamming strategy is clearly the most wasteful when there are no malicious drones. In this work we simplify the analysis somewhat and look only at the time when the threat has realised (i.e., there is a malicious drone in the vicinity). Fig. 14 shows the drone's operable area reduction divided by the counter-drone system's average output power (i.e., the energy efficiency). Several effects can be noticed. Firstly, FD operation essentially allows to double the jamming energy consumption over HD operation. However, this does not lead to equivalent gains in the operable area reduction. As such, when looking strictly at the area that the counter-drone system is able to protect at given energy consumption, the HD operation mode utilises the energy more efficiently. This is understandable, since once the 1% bit error rate threshold is crossed, there is no benefit to increasing the bit error rate by using more energy. Furthermore, follower jamming can be the most energy efficient strategy, but that requires the nodes to be positioned so that the follower jammer is able to target the correct channels.

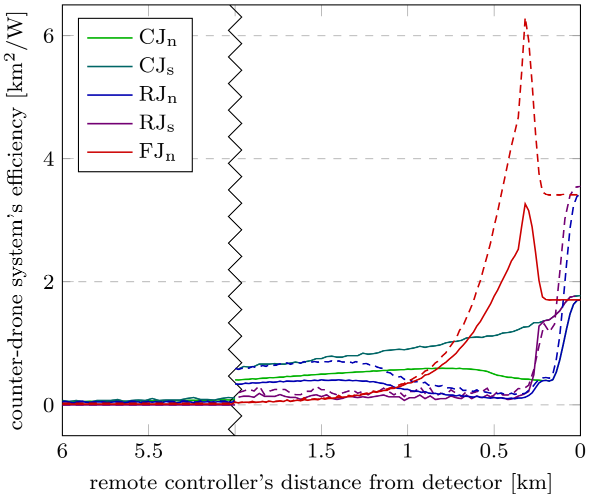


Fig. 14. Energy efficiency of counter-drone systems with different strategies and operation modes.

One of the main characteristics that separates drone and general physical-layer reliability studies is the difference in the air-to-air, ground-to-air, and ground-to-ground channels. Specifically, the ground-to-air channel between a drone and its remote controller is much less prone to degradation than the ground-to-ground channel between a typical counter-drone system and a remote controller. So far, in all of the results we have assumed that the counter-drone system is on the ground, which is a fair assumption considering most practical systems. However, it is plausible that the counter-drone system be elevated (using, e.g., a tethered drone or antenna tower) to an altitude similar as the malicious drone. This would level the playing field from the counter-drone system perspective. In Fig. 15, we analyse the performance of different counter-drone systems when they are positioned on the ground and elevated to the same altitude as the drone. The plot shows how much is the drone's operable area reduced by the counter-drone system. The results are quite clear, a counter-drone system that has been lifted up in the air outperforms a terrestrial counter-drone system regardless of the operation mode and strategy.

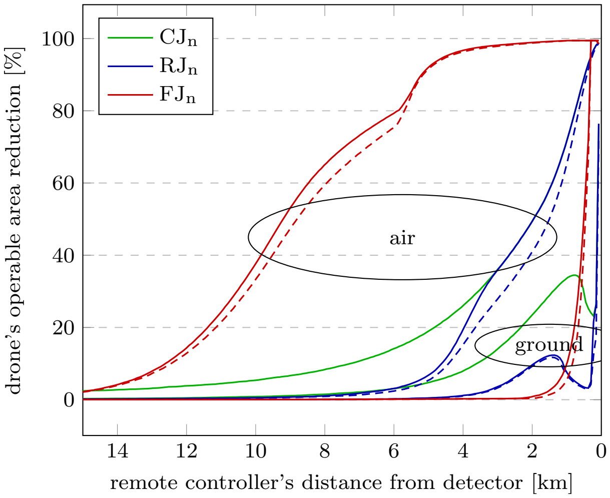


Fig. 15. Performance of the counter-drone system from ground and air.

V. Conclusions

In this article, we have presented a systematic approach for the reliability analysis of FD and HD operation modes in remote-controlled drone and counter-drone systems. We developed analytical tools to evaluate the detection and demodulation probabilities of frequency-hopped BFSK with channelized energy detectors and noncoherent demodulators under adversarial or self-induced interference. We verified the analytical methods through comparison to simulated results and then used the methods to study three different scenarios, showing what can be expected to be the actual impact of either operation mode in terms of the coverage or operation area. Analysis of the three scenarios showed that FD radio technology has clear benefits in remote-controlled drone and counter-drone systems. Specifically, FD operation mode can extend the effective range of counter-drone systems and allows drone systems to detect interference from the counter-drone system at a greater distance. However, there are also potential drawbacks to using FD over HD operation mode, especially in two-way communications. That is because FD operation between a remote controller and drone simplifies targeting that link for the counter-drone system, resulting in significantly reduced remote-controllable flight range for the drone, although achieving better spectral efficiency.

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 J. Sel. Areas Commun.*, vol. 32, no. 9, pp. 1637–1652, Sep. 2014.

[2] K. Pärlin, T. Riihonen, V. Le Nir, M. Bowyer, T. Ranstrom, E. Axell, B. Asp, R. Ulman, M. Tschauner, and M. Adrat, "Full-duplex tactical information and electronic warfare systems," *IEEE Commun. Mag.*, vol. 59, no. 8, pp. 73–79, Aug. 2021.

[3] 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.

[4] K. Pärlin, T. Riihonen, G. Karm, and M. Turunen, "Jamming and classification of drones using full-duplex radios and deep learning," in *Proc. International Symposium on Personal, Indoor and Mobile Radio Communications*, Sep. 2020.

[5] N. Ebrahimi, H.-S. Kim, and D. Blaauw, "Physical layer secret key generation using joint interference and phase shift keying modulation," *IEEE Trans. Microw. Theory Tech.*, vol. 69, no. 5, pp. 2673–2685, May 2021.

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

[7] F. Zhu, F. Gao, T. Zhang, K. Sun, and M. Yao, "Physical-layer security for full duplex communications with self-interference mitigation," *IEEE Trans. Wireless Commun.*, vol. 15, no. 1, pp. 329–340, Jan. 2016.

[8] I. Guvenc, F. Koohifar, S. Singh, M. L. Sichitiu, and D. Matolak, "Detection, tracking, and interdiction for amateur drones," *IEEE Commun. Mag.*, vol. 56, no. 4, pp. 75–81, Apr. 2018.

[9] L. Zhang and N. Ansari, "A framework for 5G networks with in-band full-duplex enabled drone-mounted base-stations," *IEEE Wireless Commun. Mag.*, vol. 26, no. 5, pp. 121–127, Oct. 2019.

[10] H. Wang, J. Wang, G. Ding, J. Chen, Y. Li, and Z. Han, "Spectrum sharing planning for full-duplex UAV relaying systems with underlaid D2D communications," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 9, pp. 1986–1999, Sep. 2018.

[11] V. Chamola, P. Kotesh, A. Agarwal, N. Gupta, M. Guizani *et al.*, "A comprehensive review of unmanned aerial vehicle attacks and neutralization techniques," *Ad hoc networks*, vol. 111, Feb. 2021.

[12] J. Wang, Y. Liu, and H. Song, "Counter-unmanned aircraft system(s) (C-UAS): State of the art, challenges, and future trends," *IEEE Aerosp. Electron. Syst. Mag.*, vol. 36, no. 3, pp. 4–29, Mar. 2021.

[13] S. Park, H. T. Kim, S. Lee, H. Joo, and H. Kim, "Survey on anti-drone systems: Components, designs, and challenges," *IEEE Access*, vol. 9, pp. 42 635–42 659, Mar. 2021.

[14] C. Lin, D. He, N. Kumar, K.-K. R. Choo, A. Vinel, and X. Huang, "Security and privacy for the internet of drones: Challenges and solutions," *IEEE Commun. Mag.*, vol. 56, no. 1, pp. 64–69, Jan. 2018.

[15] G. Secinti, P. B. Darian, B. Canberk, and K. R. Chowdhury, "SDNs in the sky: Robust end-to-end connectivity for aerial vehicular networks," *IEEE Commun. Mag.*, vol. 56, no. 1, pp. 16–21, Jan. 2018.

[16] X. Lu, L. Xiao, C. Dai, and H. Dai, "UAV-aided cellular communications with deep reinforcement learning against jamming," *IEEE Wireless Commun. Mag.*, vol. 27, no. 4, pp. 48–53, Aug. 2020.

[17] R. Morales-Ferre, P. Richter, E. Falletti, A. de la Fuente, and E. S. Lohan, "A survey on coping with intentional interference in satellite navigation for manned and unmanned aircraft," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 249–291, Oct. 2019.

[18] H.-M. Wang, X. Zhang, and J.-C. Jiang, "UAV-involved wireless physical-layer secure communications: Overview and research directions," *IEEE Wireless Commun. Mag.*, vol. 26, no. 5, pp. 32–39, Oct. 2019.

[19] X. Sun, D. W. K. Ng, Z. Ding, Y. Xu, and Z. Zhong, "Physical layer security in UAV systems: Challenges and opportunities," *IEEE Wireless Commun. Mag.*, vol. 26, no. 5, pp. 40–47, Oct. 2019.

[20] Q. Wu, W. Mei, and R. Zhang, "Safeguarding wireless network with UAVs: A physical layer security perspective," *IEEE Wireless Commun. Mag.*, vol. 26, no. 5, pp. 12–18, Oct. 2019.

[21] T. V. Sobers, B. A. Bash, S. Guha, D. Towsley, and D. Goeckel, "Covert communication in the presence of an uninformed jammer," *IEEE Trans. Wireless Commun.*, vol. 16, no. 9, pp. 6193–6206, Sep. 2017.

[22] K. Shahzad, X. Zhou, S. Yan, J. Hu, F. Shu, and J. Li, "Achieving covert wireless communications using a full-duplex receiver," *IEEE Trans. Wireless Commun.*, vol. 17, no. 12, pp. 8517–8530, Dec. 2018.

[23] S. Lee, R. J. Baxley, M. A. Weitnauer, and B. Walkenhorst, "Achieving undetectable communication," *IEEE J. Sel. Topics Signal Process.*, vol. 9, no. 7, pp. 1195–1205, Oct. 2015.

[24] D. Torrieri, "The information-bit error rate for block codes," *IEEE Trans. Commun.*, vol. 32, no. 4, pp. 474–476, Apr. 1984.

[25] 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, Feb. 2016.

[26] H. Urkowitz, "Energy detection of unknown deterministic signals," *Proceedings of the IEEE*, vol. 55, no. 4, pp. 523–531, Apr. 1967.

[27] J. Bird and E. Felstead, "Antijam performance of fast frequency-hopped M-ary NCFSK–an overview," *IEEE J. Sel. Areas Commun.*, vol. 4, no. 2, pp. 216–233, Mar. 1986.

[28] E. B. Felstead, "Follower jammer considerations for frequency hopped spread spectrum," in *Proc. Military Communications Conference*, vol. 2, Oct. 1998, pp. 474–478.

[29] M. Abramowitz and I. A. Stegun, *Handbook of mathematical functions with formulas, graphs, and mathematical tables*. United States Department of Commerce, National Bureau of Standards, 1964, vol. 55.

[30] J. Marcum, “A statistical theory of target detection by pulsed radar,” *IEEE Trans. Inf. Theory*, vol. 6, no. 2, pp. 59–267, Apr. 1960.

[31] S. Atapattu, C. Tellambura, and H. Jiang, *Energy detection for spectrum sensing in cognitive radio*. Springer, Feb. 2014.

[32] A. Mizera, J. Pang, and Q. Yuan, “Reviving the two-state Markov chain approach,” *IEEE/ACM Trans. Comput. Biol. Bioinformatics*, vol. 15, no. 5, pp. 1525–1537, Sep. 2018.

[33] L. Miller, J. Lee, and D. Torrieri, “Frequency-hopping signal detection using partial band coverage,” *IEEE Trans. Aerosp. Electron. Syst.*, vol. 29, no. 2, pp. 540–553, Apr. 1993.

[34] E. W. Ng and M. Geller, “A table of integrals of the error functions,” *Journal of Research of the National Bureau of Standards*, vol. 73, no. 1, Mar. 1969.

[35] S. Stein, “Unified analysis of certain coherent and noncoherent binary communications systems,” *IEEE Trans. Inf. Theory*, vol. 10, no. 1, pp. 43–51, Jan. 1964.

[36] D. W. Bliss and S. Govindasamy, *Adaptive wireless communications: MIMO channels and networks*. Cambridge University Press, May 2013.

[37] K. Pärlin, M. M. Alam, and Y. Le Moullec, “Jamming of UAV remote control systems using software defined radio,” in *Int. Conference on Military Communications and Information Systems*, May 2018.

[38] M. Ezuma, F. Erden, C. K. Anjinappa, O. Ozdemir, and I. Guvenc, “Detection and classification of UAVs using RF fingerprints in the presence of Wi-Fi and Bluetooth interference,” *IEEE Open Journal of the Commun. Soc.*, vol. 1, pp. 60–76, Nov. 2019.

[39] A. A. Khuwaja, Y. Chen, N. Zhao, M.-S. Alouini, and P. Dobbins, “A survey of channel modeling for UAV communications,” *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 2804–2821, Jul. 2018.

[40] J. Allred, A. B. Hasan, S. Panichsakul, W. Pisano, P. Gray, J. Huang, R. Han, D. Lawrence, and K. Mohseni, “Sensorflock: an airborne wireless sensor network of micro-air vehicles,” in *Proc. Int. Conf. on Embedded Networked Sensor Systems*, Nov. 2007, pp. 117–129.

[41] N. Ahmed, S. S. Kanhere, and S. Jha, “On the importance of link characterization for aerial wireless sensor networks,” *IEEE Commun. Mag.*, vol. 54, no. 5, pp. 52–57, May 2016.

Karel Pärlin received his M.Sc. degree in electrical engineering from Tallinn University of Technology, Estonia, in 2017. He is currently pursuing his D.Sc. degree in communication engineering at Tampere University, Finland. His research interests include adaptive signal processing, signal processing for communications, and physical layer security.

Taneli Riihonen [S’06, M’14, SM’22] received his D.Sc. degree in electrical engineering from Aalto University, Finland, in 2014. He is currently a tenure-track Associate Professor with the Faculty of Information Technology and Communication Sciences, Tampere University, Finland. His research interests include physical-layer OFDM(A), multi-antenna, multihop, and full-duplex wireless techniques with current research interest includes the evolution of beyond 5G systems.

Vincent Le Nir received his Ph.D. degree in electronics from the National Institute of Applied Sciences, France, in 2004. He is currently a senior researcher at the Royal Military Academy in Brussels, Belgium. His research interests are related to digital communications and signal processing in the wireless and wireline domains, MIMO communications, space–time coding, OFDM and multicarrier-code-division multiple-access, turbo-equalization, software defined and cognitive radio.

Marc Adrat received his Diploma and Dr.-Ing. degrees in electrical engineering from RWTH Aachen University, Germany, in 1997 and 2003, respectively. He is currently the head of the Software Defined Radio (SDR) research group at Fraunhofer FKIE in Wachtberg, Germany. His research interests include digital signal processing for mobile tactical radio communications as well as emerging technologies like in-band full-duplex communications. Since over 10 years, he is a guest lecturer at RWTH Aachen University for a course on channel coding.