Sweep Jamming Mitigation Using Adaptive Filtering for Detecting Frequency Agile Systems

Karel Pärlin*, Taneli Riihonen†, and Matias Turunen†

*Rantelon, Tallinn, Estonia

†Faculty of Information Technology and Communication Sciences, Tampere University, Finland

e-mail: karel.parlin@rantelon.ee, taneli.riihonen@tuni.fi, matias.turunen@tuni.fi

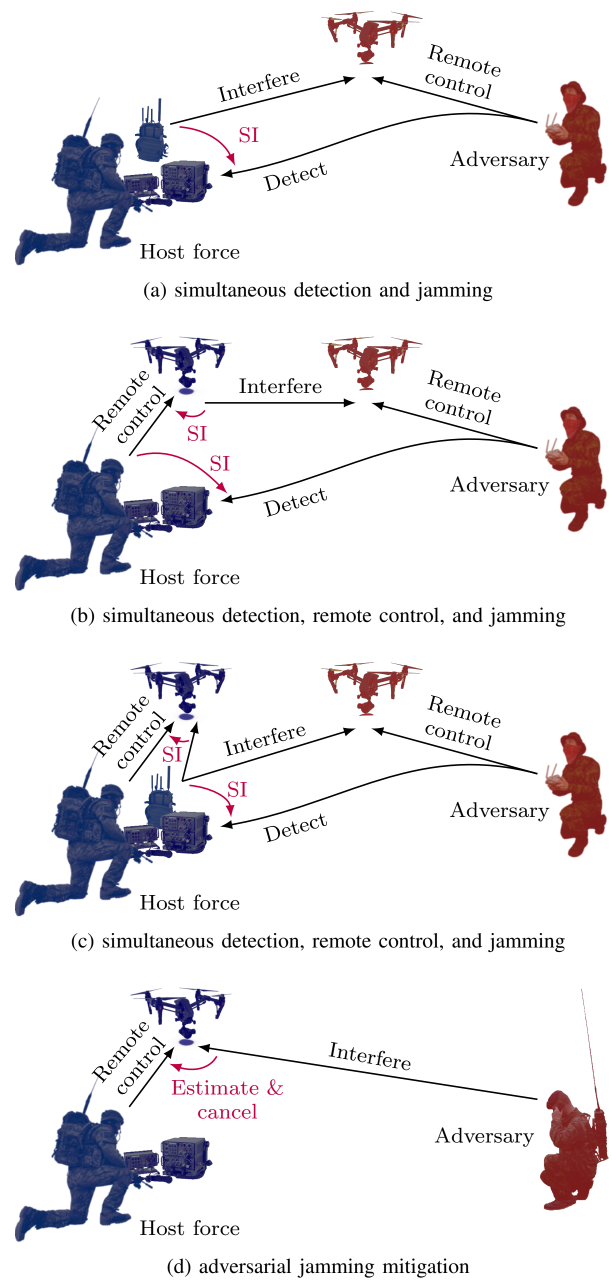
***Abstract*—The military applications of interference mitigation are numerous, with the most obvious application being suppressing the effects of adversarial jamming. However, jamming mitigation also becomes essential in scenarios where the host force's jammer and signal intelligence receiver are in close proximity to each other and the jammer inadvertently introduces interference in the receiver. In this paper, through experiments carried out in a laboratory environment, we demonstrate the feasibility of digitally mitigating non-stationary narrowband interference caused by a sweep jammer, while simultaneously retaining the ability to receive and detect signals from unmanned aerial vehicle (UAV) remote control systems that use frequency hopping in the jammed frequency band.**

I. Introduction

Interference mitigation in the military domain has an important application in the form of adversarial jamming suppression. Equally vital, however, is the mitigation of self-jamming produced by operating jammers in close proximity to receivers when carrying out electronic attack (EA) and electronic support (ES) actions in the same frequency band simultaneously [1]. Such use of EA and ES could be especially beneficial, e.g., in preventing unauthorized unmanned aerial vehicles (UAVs) from operating in restricted airspaces through simultaneous jamming and signals intelligence.

When countering rogue UAVs, jamming suppression could be used in several ways as illustrated in Fig. 1. In the simplest case, jammer suppression enables simultaneously preventing unauthorized UAV remote control through jamming while also retaining the ability to receive and detect the remote control signals (Fig. 1a). The received remote control signals could be used to find the direction of the adversary or classify the used remote control system, both of which can be highly valuable information in a tactical situation. Furthermore, such capability could be used to optimize the jamming waveform against the UAV remote control system on the fly by learning the parameters of the targeted frequency agile communications while already jamming and also taking into account how the targeted system reacts to jamming.

Additionally, jamming mitigation techniques could enable the remote control of authorized UAVs all the while preventing rogue UAVs from using the same spectral resources.



(a) simultaneous detection and jamming

(b) simultaneous detection, remote control, and jamming

(c) simultaneous detection, remote control, and jamming

(d) adversarial jamming mitigation

Fig. 1. Jammer interference, or self-interference (SI), suppression to simultaneously jam and receive adversarial unmanned aerial vehicle (UAV) remote control systems or mitigate adversarial jamming in the host forces' systems.

This research work was funded partially by the Academy of Finland under the grant 315858 "Radio Shield Against Malign Wireless Communication."

This could be achieved by equipping the authorized UAVs with a multifunction radio capable of simultaneously receiving remote control signals and transmitting jamming signals (Fig. 1b). In that case, the jamming power would be limited by the achievable passive isolation between the jammer and the receiver, unless some form of analog self-interference (SI) cancellation is also used. On the other hand, when a ground-based jammer uses jamming signals that are known to the authorized UAV, the jamming signals could be estimated and cancelled on-board (Fig. 1c). Similarly, in case of the adversary using jamming signals that can be estimated, the cancellation techniques could be repurposed to mitigate adversarial jamming (Fig. 1d).

In the case of co-located jammer and receiver where the jamming signal is known to the receiver, the challenge of jamming suppression becomes similar to the problem of SI cancellation in military full-duplex radios (MFDRs) [2], [3]. In fact, practical studies have been already published that demonstrate the feasibility of simultaneous signals detection or interception while jamming [4], [5] and also protecting one's own tactical communications from adversarial interception using MFDRs [6]. However, SI cancellation requires a replica of the jamming signal alone to be available at the receiver in both digital and analog domain to cancel the SI. That is unless it can be estimated. The objective of this work is to study the practical feasibility of operating separate jamming and receive devices in close proximity by estimating and cancelling the jamming signal digitally in the receiver in the presence of frequency hopping UAV remote control signals.

We focus on mitigating sweep jamming because of its widespread use against frequency agile wireless communications [7]. Whereas the mitigation of narrowband interference, such as the sweep jamming, for direct-sequence spread spectrum (DSSS) communications has been extensively studied [8], mitigation in frequency-hopping spread spectrum (FHSS) systems has not been covered to such extent. In the case of combined FHSS and DSSS systems, the sweep interference mitigation comes down to interference mitigation in DSSS systems with a changing center frequency (when each channel is considered separately), whereas the interference swiftly enters and leaves the channel [9]. However, for detection and analysis purposes, we instantaneously focus on the full bandwidth that the UAV remote controllers use, thus resulting in a somewhat different challenge.

The remainder of this paper is organized as follows. In Section II, the digital sweep jamming estimation and mitigation techniques used herein are introduced. The experimental setup that was used assess those methods is discussed in Section III and the results are presented in Section IV. Finally, the paper is concluded in Section V

II. Sweep Jamming Estimation & Cancellation

In this work, we combine a jammer and a wideband digital receiver. The jammer is intended for jamming UAV remote control systems and generates a linear frequency sweep, also referred to as a chirp, jamming signal with configurable sweep rate, covering the full 2.4 GHz industrial, scientific, and medical (ISM) frequency band. The accumulative wideband nature of the sweep jamming signal means that it has an impact on the remote control systems comparable to the increase in the noise floor. However, the fact that sweep jamming itself is instantaneously a narrowband signal, can be exploited to mitigate it in the received signal.

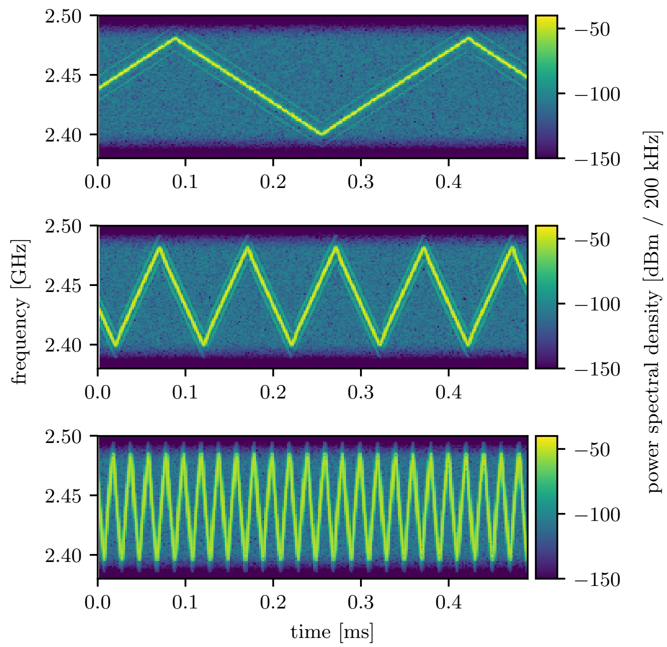


Fig. 2. Time-frequency evolution of the sweep jamming signals with different sweep rates (3, 10, and 50 kHz) as generated by the jammer.

We suppress the jamming signal by first estimating the instantaneous frequencies (IFs) of the chirp over its entire bandwidth and reconstructing the jamming signal in the digital domain based on the estimations. Then, through adaptive filtering, the jamming signal can be subtracted from the received signal. The method can be extended to suppress broadband jamming if the IF estimation step can be replaced with a method that is able to estimate the broadband jamming signal. Furthermore, given a known jamming signal, this method could possibly be applied to also cancel the interference in the analog domain through an auxiliary transmission chain much like in some of the full-duplex (FD) radio prototypes [10].

A. Instantaneous Frequency Estimation

In our experiments that we describe in the following sections, we have used sweep jamming with three different sweep rates. Each sweep rate is optimal for jamming frequency agile systems with different characteristics and as such we aim to demonstrate the usability of the jamming suppression technique in different scenarios. The used sweep rates are 3, 10, and 50 kHz. The time–frequency evolution of the jamming signals with different sweep rates as transmitted by the jammer are plotted in Fig. 2. As can be seen from those plots, the IF of the jamming signal evolves linearly over the

2.4 GHz ISM radio band while following a periodic pattern. The continuous-time single-component unidirectional signal, $x(t)$, can therefore be approximately modeled as

$$x(t) = A(t) \exp[j(\omega_0 t + \frac{t^2}{2}\psi + \phi_0)] \quad (1)$$

where $A(t)$ is the instantaneous amplitude of the jamming signal, ω_0 is related to the center frequency, ϕ_0 is the initial phase, and ψ is the sweep rate. The model in (1) neglects several properties of the actual jamming signal, e.g., its phase noise. However, it captures the most important feature of $x(t)$, which is the fact that it is instantaneously a narrowband signal.

Because of the instantaneously narrow bandwidth of the jamming signal, its successive phase differences can be used for IF estimation. For a single-component signal, the IF is defined as the derivative of its phase [11] as

$$f_i(t) = \frac{1}{2\pi}\frac{d\phi(t)}{dt} \quad (2)$$

where $\phi(t)$ is the phase of the signal. The discrete-time IF estimation for a complex valued signal, based on the single phase differencing operation [12], is

$$\begin{aligned} \hat{f}_x(n) &= \frac{1}{2\pi}(\phi(n) - \phi(n-1)) \\ &= \frac{1}{2\pi}\angle[x(n)x^*(n-1)]. \end{aligned} \quad (3)$$

The estimator given in (3) is computationally efficient, but it has high variance for noisy signals. In order to reduce the variance, knowing that the interference and the signals of interest are constrained to a certain bandwidth, the input can be filtered outside this bandwidth. Furthermore, smoothing and time averaging can be used to lower the variance [13]. Weighted phase difference estimator [13], that for stationary signals with sufficient signal-to-noise ratio (SNR) reaches the Cramér–Rao bound, is given by

$$\hat{f}_x = \frac{1}{2\pi}\sum_{n=0}^{N-2} h_n \cdot \angle[x(n)x^*(n-1)], \quad (4)$$

where h_n, i.e., the smoothing window, is given by

$$h_n = \frac{1.5N}{N^2-1}\left(1 - \left[\frac{n-((N/2)-1)}{N/2}\right]^2\right). \quad (5)$$

B. Jamming Mitigation

The weighted phase difference estimator in (4) and (5) suffices to estimate and track the IF of a single-component signal applied as a sliding window function, but in order to suppress that signal, exact amplitude and phase need to be estimated as well. Therefore, based on the estimated IFs, $\hat{f}_x(n)$, of the jamming signal, we construct a digital representation, $\hat{x}(n)$, of the jamming signal such that it exactly follows the estimated IFs. We then use adaptive filtering as illustrated in Fig. 3 to suppress the reconstructed jamming signal in the received signal similarly to the adaptive noise cancelling concept [14].

The signal of interest $s(n)$, i.e., the UAV remote controller signal, is corrupted by the interference resulting from jamming

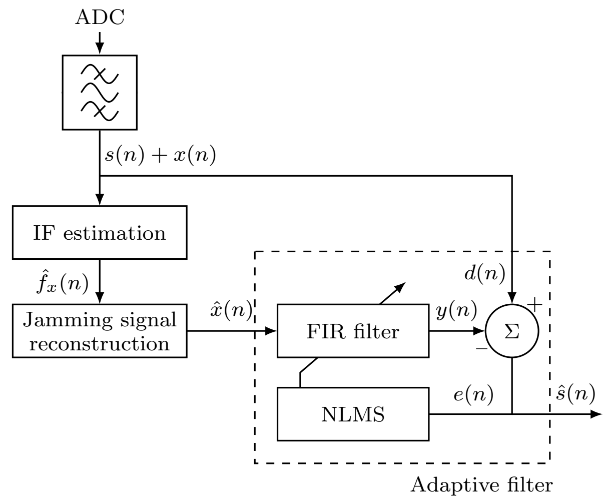


Fig. 3. Suppressing the jamming signal through adaptive filtering after estimating the instantaneous frequencies (IFs) of the jamming signal. The error signal, $e(n)$, approximates the desired signal component, $s(n)$, if $x(n)$ and $\hat{x}(n)$ are strongly correlated.

$x(n)$ and noise. In order to obtain an interference-free version of $s(n)$, we employ the noisy input signal, $s(n)+x(n)$, as the reference signal, $d(n)$, for the adaptive filter, whose input is the estimated jamming signal, $\hat{x}(n)$, that is strongly correlated to the actual jamming signal, $x(n)$. The adaptive mechanism adjusts the filter coefficients in such a manner that the filter output, $y(n)$, approximates the jamming signal, $x(n)$, with proper amplitude and phase, thus forcing the error signal, $e(n)$, to resemble the signal of interest, $s(n)$. A single-frequency reference based adaptive canceller has the properties of a notch filter at the reference frequency and the level of interference is reduced at the expense of introducing some distortion on the desired signal [8], [14].

Several algorithms have been proposed for adapting the filter weights, previous comparisons of least mean squares (LMS) and recursive least squares (RLS) for tracking chirped signals in noise have found the LMS to be superior in low SNR scenarios and especially for very narrowband signals [15]. In the presented configuration, the LMS-based filter updating has similarly shown better performance in terms of the minimizing the mean square error when compared to the RLS-based updating. Thus, we have used the normalized LMS method for updating the filter taps. In this case, for large SNRs, a single complex filter tap is sufficient [16]. The learning rate was chosen empirically for each of the three sweep rates.

III. Experimental Setup

In order to verify the feasibility of simultaneous jamming and detection, we carried out experiments in a laboratory environment. The laboratory setup simulates a scenario, where an unauthorized UAV is being remotely controlled by an adversary and the jamming suppression is used to simultaneously jam and receive the remote control link from a co-located site. As already mentioned in Section II, the transceiver prototype

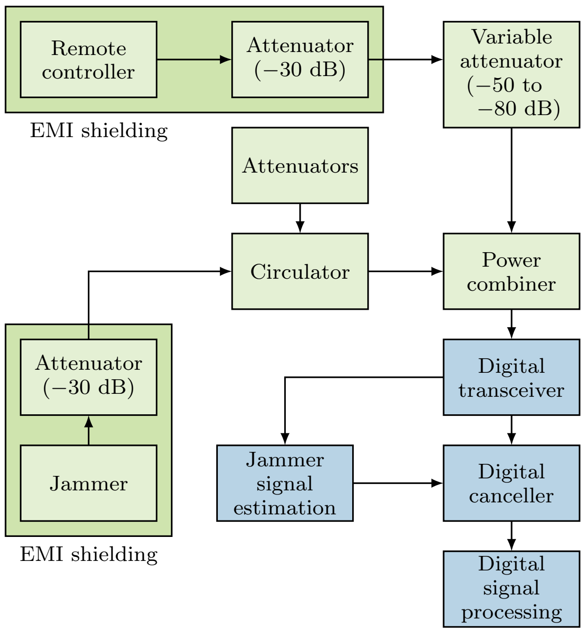


Fig. 4. Diagram of the setup used for the measurements. Both transmitters were enclosed in electromagnetic interference (EMI) shielding boxes to prevent wireless leakage from reaching the receiving front-end.

used in this work consisted of a separate jammer and a vector signal transceiver, with their transmit and receive front-ends separated by passive isolation. Three different UAV remote control systems were used as the signals of interest. We have focused solely on the ability to simultaneously jam and receive the UAV remote control signals. Thus, we have not considered the efficiency of the jamming on the UAV remote control systems, while this has already been studied to some extent previously [17].

The measurements were carried out in a closed laboratory environment as illustrated in Fig. 4, i.e., all the devices involved in the measurements were connected through coaxial cables instead of using antennas. This provided a controlled environment in which all sources of interference, besides the devices under test, were eliminated. Also, this ensured precise control and measurement of the power levels during the measurements. Furthermore, effects in the radio channel, such as multipath propagation and fading, are not skewing the measurement results. By performing the tests in the described closed environment, it was ensured that the jammer did not have adverse effects on any of the receivers in the vicinity.

A. Experimental Transceiver

The transceiver prototype used in these measurements was built on top of National Instruments high-quality vector signal transceiver (PXIe-1073) that received and recorded measurements using $120\,\mathrm{MHz}$ sampling rate ($100\,\mathrm{MHz}$ bandwidth) with duration of $50\,\mathrm{ms}$. A separate jammer with output power of $43\,\mathrm{dBm}$ was used to generate and transmit a $80\,\mathrm{MHz}$ wide linear sweep jamming signal with center frequency of $2.44\,\mathrm{GHz}$ that acts as SI for the signal surveillance at the receiver. In order to suppress the jamming signal, a circulator is used together with $30\,\mathrm{dB}$ of attenuation immediately after the jammer to imitate transmit and receive antenna separation of approximately $70\,\mathrm{dB}$. Typically UAV jammers, and in fact the jammer used in our measurements, use highly directional antennas. Therefore, it is plausible that such isolation could be achieved for co-located jammer and receiver antennas [18]. The residual interference is suppressed digitally by first estimating the IFs of the linear chirp signal and then subtracting it from the received signal as described in Section II.

B. Remote Control Systems

Three different UAV remote controllers were used separately to provide the signals of interest in the measurements. The remote controllers were: Taranis X9D Plus, DJI Phantom 2, and DJI Phantom 3 Advanced. Each of those remote control systems makes full use of the $2.4\,\mathrm{GHz}$ ISM band through frequency hopping, which provides robustness against other spectrum usage in the same band, e.g., interference from other UAV remote control systems or wireless local area networks (WLANs). Output powers of the remote controllers adhere to the $20\,\mathrm{dBm}$ limit of the ISM band. In order to simulate different UAV remote controller signal strengths, a variable attenuator was used between the remote controller and the receiving front-end. During the measurements, the UAV remote controller signal was attenuated in the range of -80 to $-110\,\mathrm{dB}$ with $5\,\mathrm{dB}$ steps. The attenuation range was chosen such that the remote control signal powers would eventually drop below the receiver noise floor.

The remote control systems during our experiments exhibited the following characteristics. The Taranis X9D Plus remote controller frequency-hops among 47 channels with $1.5\,\mathrm{MHz}$ spacing between the center frequencies of adjacent channels and has a dwell time of $9\,\mathrm{ms}$, which is the time interval between each hop or, in other words, the time between each transmitted packet. The packet transmission time itself is actually $4.75\,\mathrm{ms}$. The DJI Phantom 2 remote control system frequency-hops among 36 channels with a dwell time of $7\,\mathrm{ms}$, packet transmission duration of $1.6\,\mathrm{ms}$, and has a spacing of $2.048\,\mathrm{MHz}$ between adjacent channels' center frequencies. In a similar manner, the DJI Phantom 3 uses 34 different channels with channel spacing of approximately $2\,\mathrm{MHz}$, dwell time of $14\,\mathrm{ms}$, and transmission duration of $2.15\,\mathrm{ms}$.

IV. Sweep Jamming Mitigation Results

Since the jamming signal that reaches the digital transceiver is rather powerful in our measurements, the computationally efficient phase difference-based estimator is capable of estimating the IF of the linear chirp signals with high accuracy as illustrated in Fig. 5. The main limitation of this method is when the power of the jamming signal becomes comparable to the power of the signal of interest as the phase difference-based estimation will not be able to accurately estimate the IFs. In such case, however, depending on the signal processing method, the SNR of the signal of interest might be sufficient to not require any jamming mitigation.

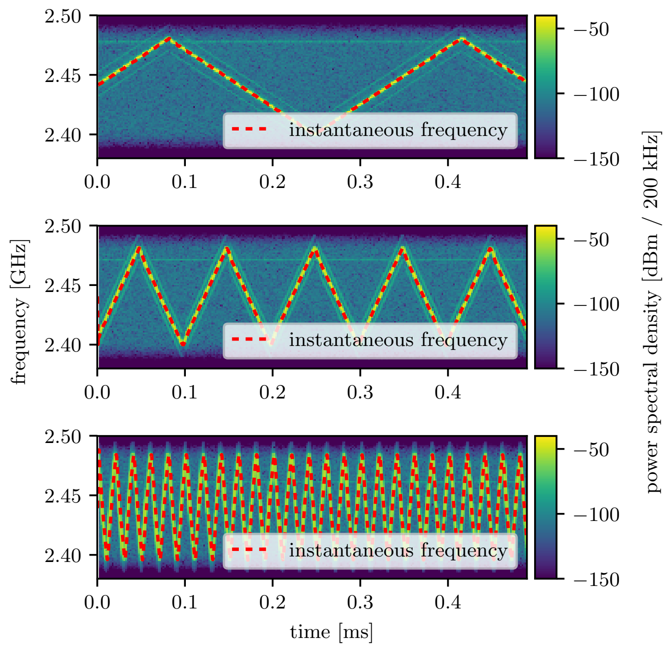


Fig. 5. Illustration of the linear sweep signals (3, 10, and 50 kHz) with superposed instantaneous frequency estimates. A remote control signal is faintly visible as a horizontal line in the background of each sweeping signal.

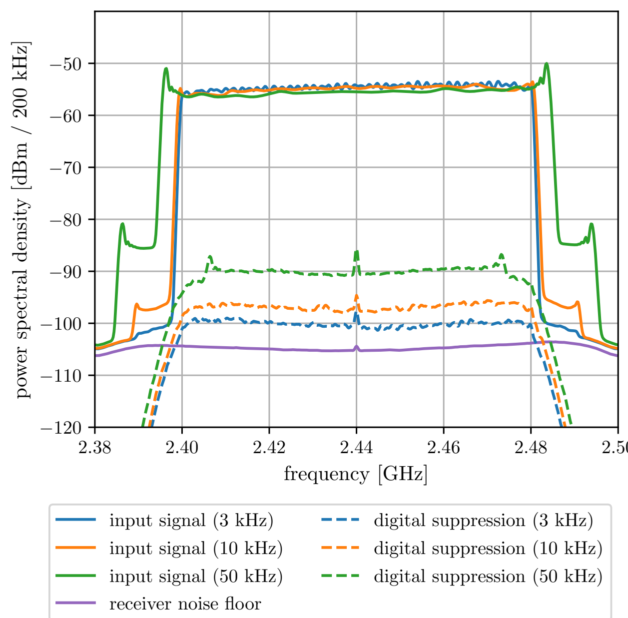


Fig. 6. Performance of the digital jamming mitigation technique in suppressing the interference caused by sweep jamming at different sweep rates.

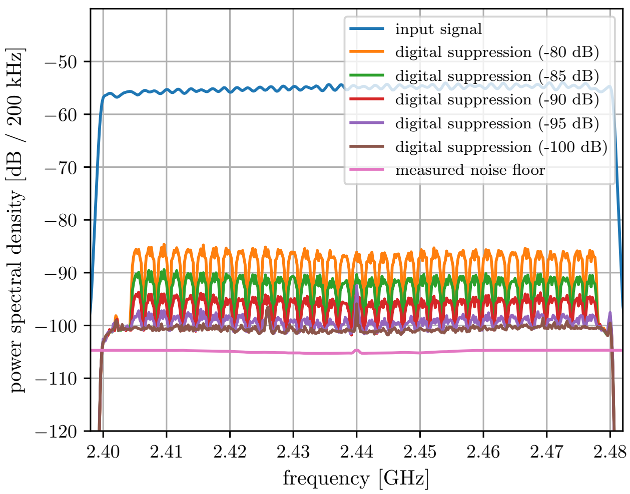
The sweep jamming suppression results obtained without the UAV remote controllers are presented in Fig. 6. The power of phase noise and spurs introduced by the jammer increases with the increase of the sweep rate, thus interference mitigation at higher sweep rates is not as efficient. Nevertheless, for the 3 kHz sweep, approximately 45 dB of digital mitigation was achieved. For the 10 kHz and 50 kHz sweeps, 41 dB and 34 dB of suppression was achieved.

The sweep jamming mitigation results for the 3 kHz sweep together with the UAV remote control signals are illustrated in Fig. 7. It might seem like the remote controller is not using all of the channels. However, this is simply the result of our limited recording time since not all of the channels happened to be used during the measurement windows. The presence of the remote controller signals at the measured power levels has not affected jammer mitigation results. However, any purely digital interference mitigation method is limited by the analog-to-digital converter (ADC) range and quantization noise in order to prevent saturation and this, together with the non-linearities of the jamming signal, limits the sensitivity here as well. Still, Fig. 7 demonstrates that the remote control signals are distinguishable at attenuation levels down to -90 dB to -100 dB depending on the remote controller and can be detected using, e.g., energy based methods.

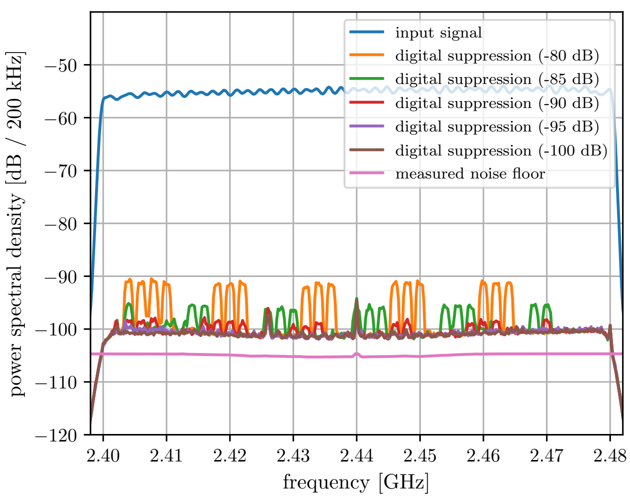
Any efforts to analyze the extent of distortion caused in the received UAV remote control signals by the interference mitigation are out of the scope of the present work. Nonetheless, the immediate results of the digital jamming suppression method examined here can already be used, e.g., in time–frequency analysis of the remote controller protocol to improve the jamming efficiency through altering the sweep rate [19], to classify the remote control protocol through time–frequency analysis [20], or even to estimate the direction of the remote controller based on signal amplitude [21]. Such metadata, i.e., direction, transmitter type, and its activity, is already highly valuable information in tactical situations. Although, the applicability of the described method for adversarial interference mitigation does depend on the tolerance of the underlying communication protocol to the possible distortions.

V. Conclusion

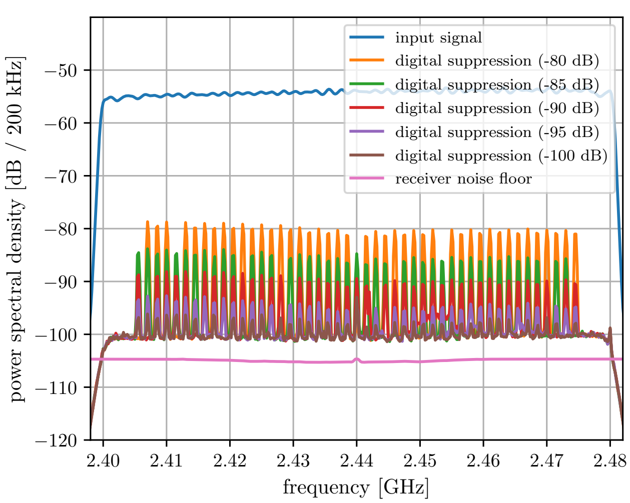
In this paper, we provided experimental results on suppressing sweep jamming in the presence of frequency hopping unmanned aerial vehicle (UAV) remote control systems. The accumulative wideband nature of the sweep jamming signal means that its impact on the remote control systems is comparable to the increase in noise floor. However, the fact that sweep jamming manifests itself instantaneously as a narrowband signal is a feature that can be exploited to estimate its instantaneous frequency (IF) and subsequently subtract it from the received signal in the digital domain through adaptive filtering. The experimental results indicate that, using a co-located jammer and a signals monitoring receiver with sufficient passive isolation, such a digital method can be used to simultaneously jam and detect wireless UAV remote control systems. Digital jamming suppression is, however, limited by the receiver's analog-to-digital converter (ADC) dynamic range. If the jamming signal can be coupled to or estimated in advance at the receiver, analog self-interference (SI) cancellation techniques could be used to further improve the total jamming suppression similarly to the concept of military full-duplex radios (MFDRs).



(a) jammer's interference and DJI Phantom 2 remote control signal



(b) jammer's interference and DJI Phantom 3 remote control signal



(c) jammer's interference and Taranis X9D Plus remote control signal

Fig. 7. Digital sweep jamming mitigation results at various remote control signal attenuation values. The attenuation values are given in the parentheses.

REFERENCES

[1] J. Laster and J. Reed, "Interference rejection in digital wireless communications," *IEEE Signal Processing Magazine*, vol. 14, no. 3, pp. 37–62, May 1997.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

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

[7] R. Poisel, *Modern Communications Jamming: Principles and Techniques*. Artech House, 2011, pp. 489–490.

[8] L. B. Milstein, "Interference rejection techniques in spread spectrum communications," *Proceedings of the IEEE*, vol. 76, no. 6, pp. 657–671, Jun. 1988.

[9] T. J. Kumpumäki, M. A. Isohookana, and J. K. Juntti, "Narrow-band interference rejection using transform domain signal processing in a hybrid DS/FH spread-spectrum system," in *Proc. IEEE Military Communications Conference*, vol. 1, Nov. 1997, pp. 89–93.

[10] M. Duarte and A. Sabharwal, "Full-duplex wireless communications using off-the-shelf radios: Feasibility and first results," in *Proc. 44th Asilomar Conference on Signals, Systems and Computers*, Nov. 2010, pp. 1558–1562.

[11] J. Ville, "Theorie et application dela notion de signal analytique," *Câbles et transmissions*, vol. 2, no. 1, pp. 61–74, 1948.

[12] B. Boashash, "Estimating and interpreting the instantaneous frequency of a signal. II. Algorithms and applications," *Proceedings of the IEEE*, vol. 80, no. 4, pp. 540–568, Apr. 1992.

[13] S. Kay, "Statistically/computationally efficient frequency estimation," in *Proc. International Conference on Acoustics, Speech, and Signal Processing*, Apr. 1988, pp. 2292–2295.

[14] B. Widrow, J. R. Glover, J. M. McCool, J. Kaunitz, C. S. Williams, R. H. Hearn, J. R. Zeidler, J. E. Dong, and R. C. Goodlin, "Adaptive noise cancelling: Principles and applications," *Proceedings of the IEEE*, vol. 63, no. 12, pp. 1692–1716, Dec. 1975.

[15] P. C. Wei, J. Han, J. R. Zeidler, and W. H. Ku, "Comparative tracking performance of the LMS and RLS algorithms for chirped narrowband signal recovery," *IEEE Transactions on Signal Processing*, vol. 50, no. 7, pp. 1602–1609, Jul. 2002.

[16] N. Bershad and O. Macchi, "Comparison of RLS and LMS algorithms for tracking a chirped signal," in *Proc. International Conference on Acoustics, Speech, and Signal Processing*, May 1989, pp. 896–899.

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

[18] E. Everett, A. Sahai, and A. Sabharwal, "Passive self-interference suppression for full-duplex infrastructure nodes," *IEEE Transactions on Wireless Communications*, vol. 13, no. 2, pp. 680–694, Feb. 2014.

[19] H. Saarnisaari, "Sweep jamming hit rate analysis for frequency agile communications," in *Proc. International Conference on Military Communications and Information Systems*, May 2016.

[20] M. Gandetto, M. Guainazzo, and C. S. Regazzoni, "Use of time-frequency analysis and neural networks for mode identification in a wireless software-defined radio approach," *EURASIP Journal on Applied Signal Processing*, vol. 2004, pp. 1778–1790, Dec. 2004.

[21] R. Pöhlmann, S. Zhang, T. Jost, and A. Dammann, "Power-based direction-of-arrival estimation using a single multi-mode antenna," in *Proc. 14th Workshop on Positioning, Navigation and Communications*, Oct. 2017.