Perfecting Jamming Signals Against RC Systems: An Experimental Case Study on FHSS with GFSK

Jaakko Marin, Mikko Heino, Joni Saikanmäki, Miikka Mäenpää, Antti-Pekka Saarinen, and Taneli Riihonen

Faculty of Information Technology and Communication Sciences, Tampere University, Finland
e-mail: jaakko.marin@tuni.fi, mikko.heino@tuni.fi, taneli.riihonen@tuni.fi

***Abstract*—Cheap off-the-self drones and other radio control (RC) equipment are readily available for customers and are becoming increasingly popular, thus also increasing the adversary or illegal activities with the RC devices. Generic RC systems can be used, e.g., in multicopter drones or roadside bombs. This raises a demand for defense and security authorities to restrict the use of RC receivers by blocking their usage. This paper studies what is the most effective waveform for jamming a typical off-the-shelf RC receiver. As a case study, the targeted system is FlySky Automatic Frequency Hopping Digital System (AFHDS), which utilizes Gaussian frequency-shift keying (GFSK) control signal with frequency-hopping spread spectrum (FHSS). The frame error rate (FER) of the receiver is measured with varying jamming power levels. The successful identification of the most efficient waveform enables the jamming of the RC receiver with the least amount of power or at the longest distance possible.**

I. Introduction

During the last years, cheap radio-controlled devices have become an increasing means to commit adversary or illegal activities. The ever-decreasing price of unmanned aerial vehicles (UAVs), e.g., multirotor drones, make them accessible to everyone and disposable. For instance, illegal deliveries to a prison are a common use for cheap UAVs [1] and unauthorized drones have even shut down airports [2]. Another common use is the usage of cheap radio controller (RC) devices to trigger improvised explosive devices [3].

This raises a need for effective means to block the operation of RC systems. One of the most popular methods to counteract RC systems is radio-frequency (RF) jamming, especially jamming the control signal of the cheap RC components. Although the legal transmission power limit for RC systems is as low as 25 mW, many cheap off-the-shelf systems can have transmission powers of up to 1 W to enable long-range and non-line-of-sight radio control [4]. The high transmission power of RC systems requires the jamming system to be power-effective so the jamming distance can be as long as possible. Making the jamming system effective at lower power levels also decreases the collateral damage to other systems operating in the area, e.g., wireless local area network (WLAN) systems [4]. Also, high jamming powers might interfere with the flight control systems of airports [5].

This research work was funded by the Finnish Scientific Advisory Board for Defence (MATINE — Maanpuolustuksen tieteellinen neuvottelukunta) under the project 2500M-0117 "Electronic Interception of Unmanned Aerial Vehicles" and the Academy of Finland under the grant 315858 "Radio Shield Against Malign Wireless Communication."

Jamming performance of different waveforms against a WLAN signal has been previously studied in [6] and [7]. In addition, multi-tone and barrage jamming against frequency hopping (FH) communication was investigated in [8]. To the authors' knowledge, there is a lack of existing empirical scientific work on the effectiveness of various different waveforms to jam RC signals. By scientific herein, we particularly refer to the philosophical value of science's open and public nature while acknowledging that armed forces and defence industry have definitely created such information privately in the research and development of anti-drone technology.

In [9], several commercial noise-based low-cost jammers were tested and it was noted that the jamming of RC control signals of drones was not effective with the obtained jammers. In [10], tone, sweep and protocal-aware jamming signals were studied for Futaba Advanced Spread Spectrum Technology (FASST) and Advanced Continuous Channel Shifting Technology (ACCST) RC systems. Both of them use frequency-shift keying (FSK) modulation with frequency-hopping spread spectrum (FHSS). It was noted that protocol-aware jamming was effective above 2 dB jammer-to-signal ratio.

In this paper, a case study is presented targeting especially the FlySky Automatic Frequency Hopping Digital System (AFHDS) popular in the cheapest RC controllers. In AFHDS, Gaussian frequency-shift keying (GFSK) modulation is used together with FHSS. In this work, we perform a measurement-based evaluation of several jamming signals to study the effectiveness of the different methods. The effectiveness is obtained by measuring the actual frame error rate (FER) of the RC receiver with several RC transmit and jamming power levels. Compared to [10], this paper evaluates a wider variety of jamming signal waveforms, especially for the case when the jammer is aware of the used RC system protocol, but not of the actual sequence of the FH. The identification of the most effective waveform under this limitation enables practical jamming of RC systems at longest possible distances. It is shown that the optimal parameters of the jamming depend on the required FER and reliability level. Other RC systems such as ACCST and Futaba FASST and FHSS also use GFSK with frequency hopping, enabling wider applicability of the results presented in this paper.

II. Experimental Setup

A. Radio Control System

The target RC system uses an inexpensive AFHDS RC transmitter (viz. stock keeping unit, SKU: HK-T4A-M2) to control remotely a compatible RC receiver (viz. SKU: HK-T6A-V2). Both of them are based on AMICCOM A7105 wireless transceiver chips. The chip supports communication in the band from 2.4 to 2.4835 GHz at 1 dBm transmit power and receiver sensitivity ranging from -107 dBm to -95 dBm. The chip also supports cyclic-redundancy check (CRC) error detection and forward error correction (FEC).

In the AFHDS protocol, the 2.4-GHz industrial, scientific and medical (ISM) band is divided into 500-kHz subbands and each transmitter cycles frame-by-frame through a frequency-hopping pattern of 16 subbands. There are 160 options for the sequence which is determined by the serial number of the transmitting radio. Each frame is modulated by uncoded binary GFSK with about 200-kHz deviation. Frame length is 0.6 ms and the frame interval is 1.48 ms. The FH pattern of the transmitter can be seen in Fig. 4 of [11].

However, being an older model than the RC transmitter, the RC receiver does not listen to the subbands at 2419.5 MHz and 2429.5 MHz, due to which the RC link suffers from an inherent FER floor of 12.5%. In the following measurement results, this peculiarity is compensated by computing and reporting FERs based on only the 14 frames in each frequency-hopping cycle that may be received correctly in the first place and neglecting those two that are always lost.

The FER value is not directly readable from the RC receiver, as it only contains a receive signal strength indicator (RSSI) pin indicating the received power as a voltage signal. Due to this reason, a device based on Arduino Mega 2560 R3 microcontroller was built to sample the voltage signal at the rate of 19.231 kHz. When the receiver is off, the RSSI pin gives a voltage of 2.2 V and a lower voltage corresponding to the RSSI when the receiver is turned on during a frame. The receiver turns on approximately 400 µs before the beginning of a frame and turns off after each frame in order to change the reception band to the center frequency of the next frame. If the frame was not successfully received, the receiver will remain on for a longer period than if the frame was successfully received. Based on this information, a computer program fetches the voltage data from the microcontroller and determines the successfully received frames and calculates the FER value of the RC receiver.

Furthermore, both the RC transmitter and the RC receiver have been modified to have SMA (SubMiniature version A) connectors in the place of their default antennas, which allows us to perform controlled experiments on coaxial cables.

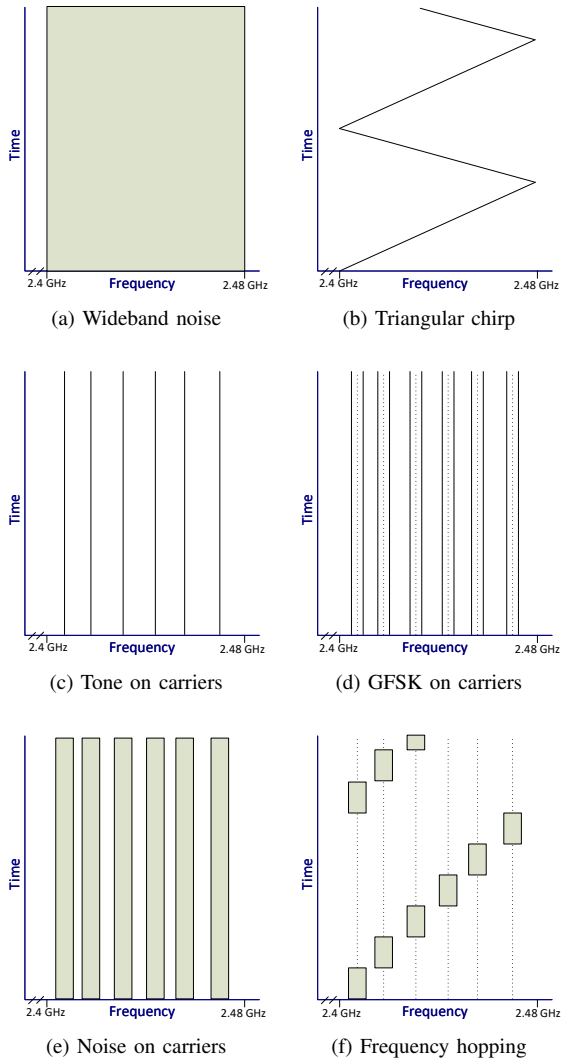
B. Jamming Signals

The jamming waveforms chosen were similar to the ones identified in [12]. In the experiments, two groups of jamming signals were used. First group of signals was designed so that the jammer is aware that the RC system is operating in the ISM band but the exact protocol is not known. In the second group, it is assumed that the jammer knows the used protocol (AFHDS) and the subbands in use but the sequence of the frequency-hopping is not known. For the first case, the following jamming signals were measured:

- An 80-MHz-wide noise signal across the ISM band (2.4 to 2.48 MHz) (Fig. 1a).
- A linear chirp sweep across the ISM band with various sweep frequencies (Fig. 1b).

For the second case when assuming the knowledge of the protocol, i.e., the frequencies and bandwidth of the carriers but not the sequence, the following group of jamming signals was used:

- A tone signal at each of the 14 subcarriers (Fig. 1c).
- A GFSK signal at each of the 14 subbands (Fig. 1d).
- A 500-kHz-wide noise signal at each of the 14 subcarriers (Fig. 1e).



(a) Wideband noise (b) Triangular chirp

(c) Tone on carriers (d) GFSK on carriers

(e) Noise on carriers (f) Frequency hopping

Fig. 1. Concept spectrograms of the jamming signal waveforms used in the measurements.

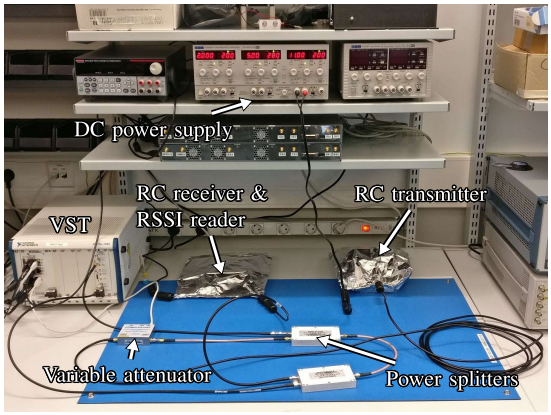


Fig. 2. The measurement setup.

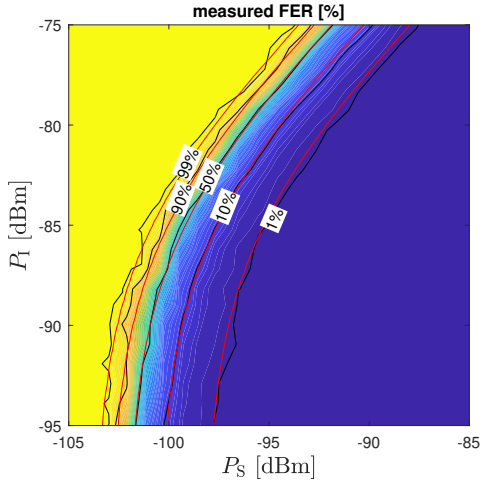


Fig. 3. FER with a 80-MHz-wide noise jamming signal. Red contours are obtained with the fitted model.

- A GFSK signal at each of the 14 subbands and a tone at each subcarrier. The ratio of the GFSK signal power to the tone power was 3 dB.
- A GFSK signal at each of the 14 subbands with linear sequence frequency-hopping with various sweep frequencies (Fig. 1f).

C. Measurement Setup

The measurement setup consists of an NI PXIe-5645R vector signal transceiver (VST), a variable attenuator (viz. Mini-Circuits RCDAT-6000-30), power splitters (viz. Mini-Circuits ZN2PD2-50-S+), 10 dB and 30 dB attenuators and the RC transmitter and the RC receiver. The RC transmitter is connected with 10 dB and 30 dB attenuators together with a variable attenuator to a power combiner which combines the jamming signal coming from the VST with the RC transmit signal. Then, the total signal is fed to a power splitter which splits the signal to the receiver (RX) port of VST and to the RC receiver. The output power of the jamming signal is controlled by the VST and the output power of the RC transmitter by the variable attenuator. The attenuation range of the variable attenuator is from 0 to 30 dB. The RX port of the VST is used to measure the actual RC signal power P_S and the interference power P_I from the jamming to calibrate them to the chosen values at the RC receiver antenna connector. The attenuation is kept constant during a single measurement across the whole frequency band, i.e., no frequency-selective fading is considered. This approximates the case when the jammer has a clear line of sight to the targeted flying drone.

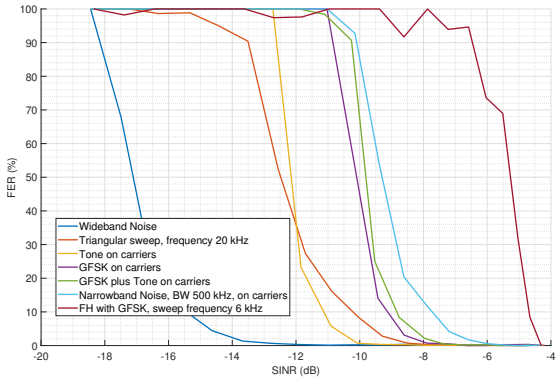


Fig. 4. Comparison of the FER achieved with different jamming signals using $P_\mathrm{S} = -87.5$ dBm.

The measurement setup is shown in Fig. 2. The RC transmitter and receiver are enclosed in electromagnetic interference (EMI) shielding pouches to suppress the unintended radiation from the printed circuit board (PCB) of the RC transmitter and to shield the RC receiver from receiving noise from the ISM band. The cables are covered with ferrite beads to suppress the EMI coupling from the cable shields.

III. Experimental Results

The FER is measured from the RC receiver with signal powers of $P_s = -105, -104, ..., -85$ dBm and jamming powers of $P_I = -95, -94, ..., -75$ dBm. The FER with this power grid for the 80-MHz-wide noise jamming signal is shown in Fig. 3. Each obtained FER value is the average of five consecutive measurements for which the RC transmitter has been restarted in between. The plot shows the contours for FER levels at 1%, 10%, 50%, 90% and 99%.

From the ratio of P_I and P_S, the signal-to-interference-and-noise ratio (SINR) can be calculated by

$$\mathrm{SINR} = \frac{P_\mathrm{S}}{P_\mathrm{I} + P_\mathrm{N}} = \frac{1}{1/\mathrm{SIR} + 1/\mathrm{SNR}} \tag{1}$$

with $\mathrm{SNR} = P_\mathrm{S}/P_\mathrm{N}$ (signal-to-noise ratio) and $\mathrm{SIR} = P_\mathrm{S}/P_\mathrm{I}$ (signal-to-interference ratio). Herein the noise power P_N is an unknown parameter, but it can be estimated by fitting a model for FER(SINR) by minimizing the mean absolute error when the jamming signal is Gaussian noise and we assume that the inherent receiver noise is the same. Consequently, we get $P_\mathrm{N} \approx -84.77$ dBm for the 80-MHz receiver noise level. The actual noise floor for the RC receiver is lower, due to it

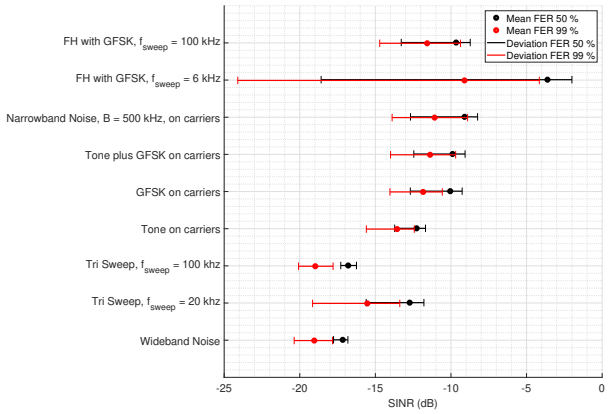


Fig. 5. Jamming performance achieved with 50 % and 99 % FER with deviation lines for different jamming signals.

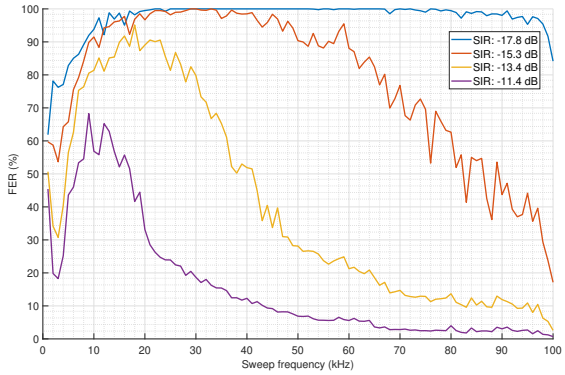


Fig. 6. Jamming performance achieved with varying sweep frequencies for triangular sweep waveform.

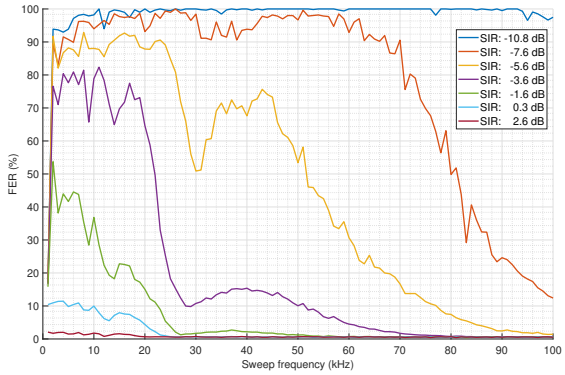


Fig. 7. Jamming performance achieved with varying sweep frequencies for frequency hopping GFSK signal.

only receiving with a bandwidth of approximately 600 kHz based on our experiments. The estimated noise floor for this is 21.25 dB lower, pushing the RC receiver noise floor down to -106 dBm. Figure 3 also shows the predicted contours of the model (1) with the estimated P_{N}.

The FER as the function of SINR is shown in Fig. 4 with fixed power level $P_{\mathrm{S}} = -87.5$ dBm as an average of five measurements. The power level is chosen so that P_{I} is the dominating component in (1) and P_{N} has negligible effect to the curves. The SINR in this case is calculated taking into account the P_{I} over the whole ISM band to compare the performance from the jammer's perspective. The specific parameter values used for the waveforms were the best found during testing.

Figure 5 shows both the average and the maximum deviation in the SINR value required to cause the defined FER level for different jamming methods. The distribution is calculated from five measurements of the $\{P_{\mathrm{I}}, P_{\mathrm{S}}\}$ grid, and for all measurement runs, the limit SINR values for 50% or 99% FER levels are calculated. Thus, the diagram shows the average SINR at which the desired FER level was reached and also the minimum and maximum SINR within the measurement set at which the FER level was reached.

Figures 6 and 7 show the obtained average FER for GFSK frequency hopping and linear chirp sweep jamming signals as a function of the sweep frequency. For each sweep frequency and SIR value, the result is an average of 20 measurements. For the frequency hopping GFSK signal in Fig. 7, the hopping goes through all the carriers once in one cycle, whereas for the linear chirp sweep, the jamming signal sweeps from the beginning of the band to the end and back within one cycle.

IV. Analysis and Discussion

In the analysis of the measurement results, we focus on the following two FER thresholds that represent jamming against different RC systems:

- When FER $> 50\%$, we assume that the remote control of consumer multicopters would be prevented.
- When FER $> 99\%$, we assume that the targeted activation of radio-controlled roadside bombs would be prevented.

From Fig. 3, the two regimes of operation can be seen. For $P_{\mathrm{S}} < -95$ dBm and $P_{\mathrm{I}} < -85$ dBm, is seen that the receiver noise P_N starts to limit the obtained FER, i.e., FER starts to depend more on SNR and the receiver sensitivity than the SIR. In the operational regime $P_{\mathrm{S}} > -95$ dBm, the SIR dominates the FER performance which is most interesting for jamming signal analysis. For the case when the exact protocol of the RC receiver is not known, the linear chirp performs best with 4 dB difference to the wideband noise jamming in the 50% average FER level. If protocol-awareness is assumed, GFSK plus tone on carrier frequencies and GFSK with frequency hopping work best in jamming. Introducing the frequency hopping to the jamming GFSK signal increases the power density for the RC frame bandwidth resulting in 5 dB improvement in the minimum SINR required for average 50% FER level.

The difference between the SINR values required to obtain similar jamming performance for the best and worst jamming signals is 12 dB. This is a drastic improvement in efficiency, implying that similar jamming performance can be obtained with 6.3% of the jamming power needed for the wideband

noise. If free-space propagation is assumed with distance dependence $P_\mathrm{I} \sim 1/r^2$ and jamming power is kept constant, the jamming distance of the FH with GFSK jamming signal is four times that of the wideband noise jamming signal.

However, for the frequency hopping and swept chirp jamming signals, the deviation in the obtained FER with time varies significantly with the sweep frequency as seen in Fig. 5. With FH GFSK sweep frequency 6 kHz, the average FER is better but the deviation in SINR to obtain 50% or 99% FER level is wider than for higher sweep frequencies. Thus, if 99% FER is needed with good confidence, FH GFSK sweep frequency 100 kHz or narrowband noise on all carriers are better. Figs. 6 and 7 highlight the difference that with larger sweep frequencies higher jamming power is needed to achieve the same average FER value as for smaller sweep frequencies.

Syncing and matching the FH pattern to the one used by the target RC transmitter would theoretically be the optimal method for jamming the RC receiver in our studied case. This would require the jammer to find out the exact pattern used by the RC transmitter and sync its own transmission to the start of the pattern. Such operation would require the jammer to have a receiver and add further complexity to the system. For these reasons, synced FH operation was not investigated for this project. Some kind of a protocol-aware jamming which targets the specific parts of the frame, such as the preamble, could bring even further improvement. These aspects are considered to be future research directions.

The possibility of pulsing the GFSK with FH signal by turning it on and off periodically was also investigated during the measurements. This means that the duty cycle of jammer is reduced while ensuring that the frequency sweep coincides with each subband at least once in the period of the frame length. Pulsing reduces the average power of the jamming operation which could in theory reduce the power consumption of the jamming operation considerably. This would also allow for a receiver to listen on the spectrum during the downtime between pulses, for instance to confirm the existence of the target signal, or to record its FH pattern.

Unfortunately, due to only having access to the FER information, the effect of a pulsed waveform was found to be disadvantageous compared to continuous transmission. It was speculated that this was caused by the RC receiver only dropping the frames that had their preamble portion jammed. Furthermore, this means that the performance of the sweeping waveforms with high FER variance could in reality be better than presented, since the actual number of frames dropped due to erroneously received data bits could be larger. Thus, the results given in this paper should be considered pessimistic. However, considering the reliability requirement in the case of preventing a remotely activated bomb from exploding, certainty is necessary.

V. Conclusion

We evaluated the performance of various jamming signals against typical off-the-shelf RC radios operating in the ISM band with ADHFS which uses GFSK together with frequency-hopping spread spectrum. Jamming signals ranging from wideband noise and linear chirp sweep to protocol-aware signals including frequency hopping GFSK were evaluated by measuring the FER of the RC receiver. The results show that the most effective signal, GFSK with FH, obtained 50% average FER with 12 dB less power than the wideband noise signal. This corresponds to four times longer jamming distance in free-space. It was noted that varying the sweeping frequency for linear chirp sweep and of the frequency hopping causes a significant difference in the variance of the FER obtained with time. With higher sweep frequencies, the variance becomes smaller but the average FER will not be as high as with lower sweep frequencies. The results obtained could be extended to other RC systems using a similar waveform.

References

[1] BBC. 'Well-organised' gang flew drones carrying drugs into prisons. [Online]. Available: https://www.bbc.com/news/uk-england-45358876

[2] ——. Gatwick runway reopens after drone chaos. [Online]. Available: https://www.bbc.com/news/uk-england-sussex-46643173

[3] J. Mietzner, P. Nickel, A. Meusling, P. Loos, and G. Bauch, "Responsive communications jamming against radio-controlled improvised explosive devices," *IEEE Communications Magazine*, vol. 50, no. 10, pp. 38–46, Oct. 2012.

[4] E. Bond, B. Crowther, and B. Parslew, "The rise of high-performance multi-rotor unmanned aerial vehicles-how worried should we be?" in *Proc. Workshop on Research, Education and Development of Unmanned Aerial Systems*, Nov. 2019, pp. 177–184.

[5] J. R. Dermody. (2018, July) Letter from FAA office of airports on guidance on use of counter UAS systems at airports. Federal Aviation Administration, U.S. Department of Transportation. [Online]. Available: https://www.faa.gov/airports/airport_safety/media/Attachment-1-Counter-UAS-Airport-Sponsor-Letter-July-2018.pdf

[6] T. Karhima, A. Silvennoinen, M. Hall, and S.-G. Haggman, "IEEE 802.11b/g WLAN tolerance to jamming," in *Proc. IEEE Military Communications Conference*, Nov. 2004, pp. 1364–1370.

[7] I. Harjula, J. Pinola, and J. Prokkola, "Performance of IEEE 802.11 based WLAN devices under various jamming signals," in *Proc. IEEE Military Communications Conference*, Nov. 2011, pp. 2129–2135.

[8] B. Levitt, "FH/MFSK performance in multitone jamming," *IEEE Journal on Selected Areas in Communications*, vol. 3, no. 5, pp. 627–643, Sept. 1985.

[9] J. Farlik, M. Kratky, and J. Casar, "Detectability and jamming of small UAVs by commercially available low-cost means," in *Proc. International Conference on Communications*, June 2016, pp. 327–330.

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

[11] 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.

[12] 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.