Jamming of UAV Remote Control Systems Using Software Defined Radio

Karel Pärlin
Rantelon Ltd
Tallinn, Estonia
karel@rantelon.ee

Muhammad Mahtab Alam, Yannick Le Moullec
Thomas Johann Seebeck Department of Electronics
Tallinn University of Technology
{muhammad.alam, yannick.lemoullec}@ttu.ee

***Abstract*—Unmanned aerial vehicles (UAVs) have become widely available and their potential unlawful usage introduces new security risks. It has therefore become highly desirable to restrict the unauthorized usage of UAVs in certain areas such as airports, nuclear power plants, etc. Most commercially available UAVs rely on spread spectrum techniques, such as direct sequencing and frequency hopping, in the remote control systems to reduce the impact of interference from neighboring communication systems (including e.g. other remotely controlled UAVs), to increase resistance to jamming and to prevent detection.**

In this paper, an efficient protocol-aware UAV remote control jamming system is proposed and implemented using an open-source software defined radio (SDR) platform. Experimental results show that for FASST and ACCST remote control systems, the proposed jammer achieves successful jamming at relatively low jam-to-signal ratios (JSRs) as compared to a sweep jammer, therefore requiring less transmitted power to achieve similar results. Furthermore, the proposed jammer impacts other communication systems significantly less than the sweep jammer.

***Index Terms*—Unmanned aerial vehicle, jamming, spread spectrum, software defined radio.**

I. Introduction

UAVs have made the leap from military to consumer grade and are being widely used for hobbies such as aerial photography and drone racing, as well as in industries such as cinematography [1]. Their possible usage in several other fields is currently being investigated by many researchers, e.g. the use of UAVs to deploy small base station cells is emerging as an effective technique for providing wireless services to ground users in a variety of scenarios [2]. Goldman Sachs aerospace and defense research analysts forecast a $100 billion market opportunity for drones between 2016 and 2020 [3]. This increase in the availability of consumer grade UAVs has lead to new challenges in security and surveillance. Specifically, there is a need for restricting the usage of UAVs in areas such as airports, nuclear power plants, prisons, national borders, and military controlled areas where UAVs might cause accidents or be used for illegal purposes. On the other hand, authorized UAVs, e.g. for providing ground users with wireless services, can become targets for hijacking and thus require secure operation.

UAVs operate with various degrees of autonomy. Generally, they either have a flight route preprogrammed and use global navigation satellite system (GNSS) signals and various sensors to follow that route, or they are being remotely piloted. If the UAV has a flight route preprogrammed and it is not itself transmitting any signals, then it can be detected for example by visual or radar based methods, but not by passively analyzing the radio frequency (RF) spectrum. If the UAV is being remotely controlled, or if it is transmitting e.g. video feedback or positional information, then the transmitted signals can be distinguished in the RF spectrum. Depending on how an UAV is operated, the detection and neutralization methods which can be applied are therefore quite different.

In this paper we investigate the possibilities of neutralizing remotely controlled UAVs by RF jamming (Figure 1 illustrates the threat model). Our work focuses on commercially available UAVs which typically do not adhere to a public standard such as WiFi and use proprietary protocols with dissimilar channel frequencies, modulation types and spread spectrum techniques [4]. In order for a single system to be able to detect and efficiently neutralize a variety of UAV remote control systems with different parameters, the neutralization system needs to be flexible.

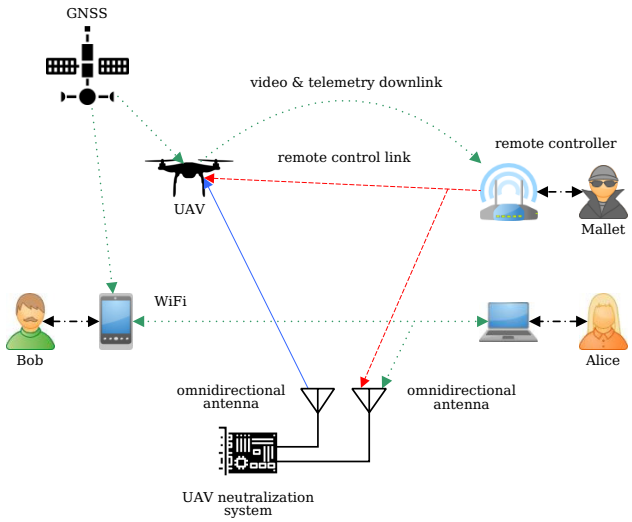

Fig. 1. The considered threat model. The UAV remote control signal is shown with a dashed line. The jamming signal used for neutralizing the UAV is shown with a solid line. The signals which are not considered or should not be interfered with are shown with dotted lines.

978–1–5386–4559–8/18/$31.00 ©

Besides the usage of different communication protocols, most commercially available UAVs are operating in either 2.4 GHz or 5.8 GHz industrial, scientific, and medical radio (ISM) unlicensed bands, along with other communication systems such as wireless local area networks (WLANs). This further complicates the detection of the targeted remote control systems, but also makes it desirable to minimize the jammer's impact on the performance of other communication systems.

We thus propose to use a jamming technique referred to as protocol-aware jamming, which takes into account the characteristics of the targeted communication system (channel frequencies, modulation type and spread spectrum techniques) to achieve power efficiency and limit the influence on other communication systems. Our main contribution is an implementation based on a software defined radio (SDR) platform that applies the protocol-aware jamming technique against a variety of UAV remote control systems with different communication protocols and RF parameters. By using the SDR approach these parameters can be configured on the fly. The proposed jammer demonstrates superior efficiency (in terms of the required transmitted power) as compared to less flexible jammers. It is also shown to interfere with WLANs significantly less than the alternative jamming techniques.

The rest of this paper is organized as follows. Section II highlights related work. Simulation results are presented in Section III. Section IV describes both the design considerations of the proposed system and its implementation. Section V presents the experimental setup and experimental results. Finally, Section VI concludes the paper.

II. Related Work

Several commercial systems exist for detecting and jamming remotely piloted UAVs. However, the literature discussing the neutralization of UAVs remote control systems is not very vast. To the best of our knowledge, works focusing directly on protocol-aware jamming of UAV remote control systems have not been published in openly available literature.

The jamming effectiveness of commercially available low-cost jammers against UAVs has been studied in [5] where it is concluded that jamming of the GNSS signal reception can be achieved from a fair distance (a couple of hundred meters from the UAV). On the other hand, the study finds that jamming of the remote control signals with the considered jammers is not effective, even when the jammer is much more closer to the UAV than the pilot with the remote controller. Although the above only reflects the performance of low-cost generic jammers, it clearly emphasizes that the simplest jamming techniques are not so effective in jamming UAVs and motivates the implementation of a specifically UAV targeted jammer.

A somewhat similar approach to the one we propose in this paper has been used in [6] to develop a reactive detection and jamming framework for interfering with WiFi and WiMAX networks. That framework senses the spectrum for the targeted signals and selectively applies jamming if it detects one. Both [6] and the system proposed in this paper are developed on an SDR platform and the digital signal processing (DSP) algorithms are implemented in a field-programmable gate array (FPGA). However, the system proposed in this paper targets UAVs and features a versatile jammer which is used to evaluate both the effectiveness and efficiency of protocol-aware jamming compared to other jamming techniques.

Taking over an UAV that is using a preprogrammed flight route has been demonstrated in [7]. UAVs with preprogrammed flight routes rely on the GNSS for positional information and by spoofing the GNSS signals the UAV can be misdirected. However, spoofing or jamming the GNSS signals still allows UAVs to be remotely controlled.

III. Simulation Results

We assessed the efficiencies of barrage, tone, sweep, and protocol-aware jamming techniques against a hybrid spread spectrum communication system, modeled in accordance with how popular UAV remote control systems work [4]. This assessment is conducted by means of simulations in Simulink. The communication system model uses a combination of frequency-hopping and direct-sequence spreading. We evaluated the simulated efficiencies of the different jamming techniques by measuring the bit error rates (BERs) caused in the communication system at different jammer-to-signal ratios (JSRs). JSR herein refers to the power of the jamming signal compared to the power of the signal which is jammed at the receiver, as shown in Equation 1.

$$JSR_{dB} = 10 * log_{10}\left(\frac{P_{jammer} + P_{noise}}{P_{signal}}\right) \quad (1)$$

While barrage, tone and sweep jammers are relatively simple, protocol-aware jammer uses *a priori* knowledge about the targeted communication system to increase the efficiency of jamming [8]. For example, if the target communication system uses frequency-hopping and the frequency-hopping pattern is known to the jammer, then the jammer can hop together with the targeted system and reduce the bandwidth which needs to be jammed at any time instant. Similarly, if direct-sequence spreading is used by the target communication system, then information about the spreading properties of the targeted signal can be used to generate a jamming signal with high correlation at the targeted receiver [9]. This complicates the reception of the spread signal at the targeted receiver and results in higher BERs than would be achievable for example with a tone or a sweep jammer, especially at low JSRs. A complete description of jammers and their taxonomy can be found in [8]; the purpose here is to compare their efficiencies when used against UAV remote control systems.

The simulated efficiencies of the considered jamming techniques against the hybrid spread spectrum communication system are plotted in Figure 2. From the simulation results it is evident that the barrage jammer can achieve high BERs at very high JSRs ($>$15 dB); however, in practical applications such high ratios might not always be attainable. Tone and sweep jammers achieve noteworthy BERs at much lower JSRs ($>$10 dB) than the barrage jammer. BER analysis per channel (not

shown in the paper) shows that, as expected, the tone jammer only affects one of the frequency-hopped channels, while the sweep jammer spreads the errors among all channels.

Finally, the simulation results clearly show that the protocol-aware jamming technique is considerably more efficient than the other techniques (approximately 10 dB less power required). This motivates the further study of the applicability and efficiency of the protocol-aware jamming technique in practical scenarios, as described in the next section.

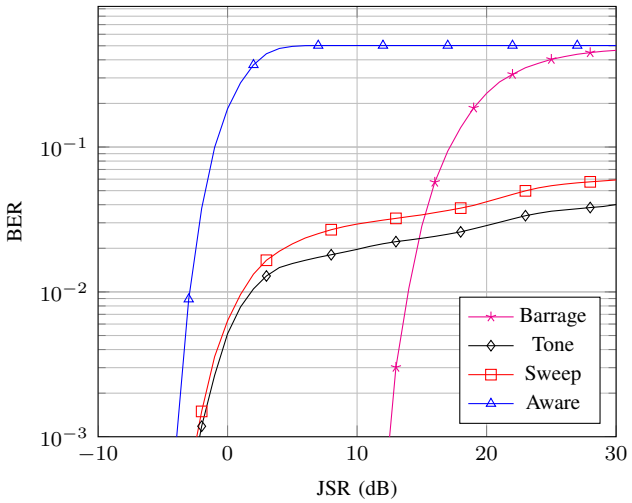

Fig. 2. Comparison of the four simulated efficiencies of different jamming techniques against a hybrid spread spectrum communication system model.

IV. Design Considerations & Implementation

In this section, an overview of the targeted UAV remote control systems, i.e. Futaba Advanced Spread Spectrum Technology (FASST) and Advanced Continuous Channel Shifting Technology (ACCST), is given and the implementation of the protocol-aware jammer is described.

A. Targeted UAV Remote Control Systems

The FASST and ACCST remote control systems have been selected because of their wide adoption in UAVs. Both of these systems use proprietary protocols and we have used several signal analysis techniques to determine their parameters which are relevant to jamming.

Both the FASST and the ACCST use frequency-shift keying (FSK) modulation with frequency-hopping spread spectrum (FHSS) and operate in the 2.4 GHz ISM band. In addition, the FASST applies Gaussian pulse-shaping filtering and direct-sequence spreading to the transmitted data. The FASST remote control system frequency-hops among 36 channels with a dwell time of 7 ms. Spacing between the channels is 2.048 MHz. It uses a chip rate of 1.536 Mbps and an 11 element pseudo noise (PN) code, therefore having a data rate of 139.6 kbps. The ACCST remote control system frequency-hops among 47 channels with a dwell time of 9 ms. Having more channels than the FASST, the ACCST is forced to space them more densely and uses a channel spacing of 1.5 MHz. The ACCST has a data rate of 100 kbps.

B. Implementation

In order to implement a protocol-aware jammer capable of targeting both of the discussed remote control systems, an SDR approach is used. For demonstration purposes, Nuand's BladeRF, an open-source SDR platform, is used as the target architecture. BladeRF features a Cyclone IV FPGA and an LMS6002 RF front-end which is capable of receiving and transmitting at frequencies from 300 MHz to 3.8 GHz.

Digital signal processing of the jammer is implemented inside the FPGA to reduce system component requirements (i.e., the system is autonomous and does not require a host computer) and to allow for efficient, real-time processing of the signals (Figure 3). Furthermore, controlling of the workflow and operation of the signal processing blocks is handled inside the Nios II soft core processor which runs in the FPGA, concurrently to the signal processing algorithms.

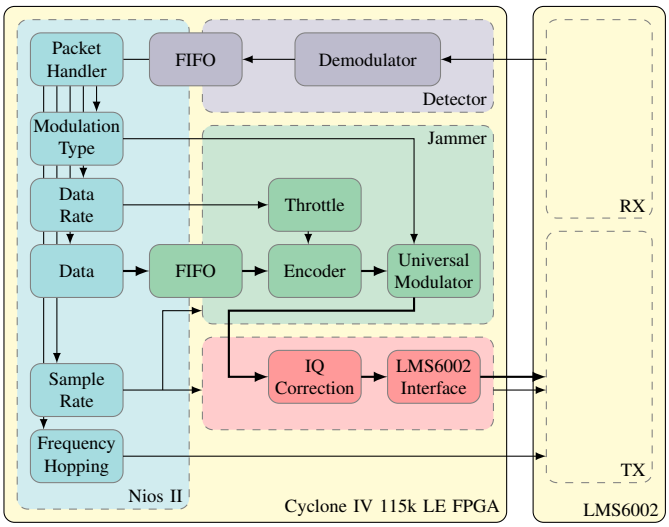

Fig. 3. Architecture of the SDR based UAV jamming subsystem.

The detection is based on baseband demodulation. In case a known signal is detected, the jammer is configured using the *a priori* knowledge about the detected system. The main blocks of the jammer are the encoder, throttle, demultiplexer and universal modulator blocks. The developed system allows transmitting arbitrary data, which is pulled from the soft core processor domain to the hardware domain by the encoder block. The encoder block applies direct sequence spreading by multiplying the data with a specified PN code and optionally applies pulse-shaping filtering. The throttle block is used to control the data rate from the encoder to the modulator. The demultiplexer directs the encoded bits to the appropriate input of the universal modulator based on the modulation type selection done in the Nios II soft core processor. The encoded data is processed by the universal modulator which is capable of applying amplitude-shift keying (ASK), frequency-shift keying (FSK) and phase-shift keying (PSK) modulations and uses the Coordinate Rotation Digital Computer (CORDIC) algorithm in rotation mode as the underlying mechanism for calculating the IQ samples.

V. Experimental Evaluation

In order to evaluate the efficiency of the developed protocol-aware jammer, we have measured the performance of FASST and ACCST based remote control systems when they are subject to its influence. In addition, to assess the impact that the developed jammer may have on other communication systems, we have also measured the performance of IEEE 802.11 based WLAN devices under the same conditions. For comparison, the measurements have also been carried out with a different jamming platform using tone and sweep jamming signals. In this section, we describe the experimental setups which were used to perform these measurements and give an overview of the results.

A. Experimental Setup

Figures 4 and 5 illustrate the experimental setups used for measuring the performances of the UAV remote control systems and WLAN devices under jamming conditions, respectively. The wireless signal propagation path between the transmitters and receivers was replaced with coaxial cables and RF attenuators. This guaranteed full control of the channel conditions and allowed both precise control and monitoring of the signal levels during the measurements. Attenuators protected the receiver inputs from excessive signal levels that could have damaged them. As the resulting signal propagation conditions corresponded closely to an ideal additive white Gaussian noise (AWGN) channel, uncontrolled random effects in the radio channel, such as external interference and fading, are not skewing the measurement results. The used jamming platforms had configurable output powers and all measurements were done in the range of -20 to 20 dB JSR.

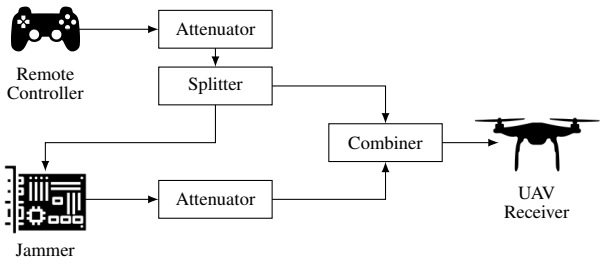

Fig. 4. Setup for measuring the efficiencies of different jamming techniques against UAV remote control systems.

Regarding the UAV measurements, both remote control systems feature indicators of total remote control link loss; however, none of them output bit or packet error rates. We therefore connected logic analyzers to the transceivers in the remote controllers and the UAVs. For the FASST case, we managed to compare the data from the remote controller prior to modulation to the data in the receiver of the UAV after demodulation and could thus calculate an approximate bit error rate. For the ACCST case, we were able to compare the number of packets received in the UAV against the number of packets transmitted by the remote controller and calculate the packet error rate (PER).

For the WLAN measurements, two MikroTik RB112 (AR5413) router boards with AR5413 wireless units were used. The channel between the transmitter and the receiver was divided to separate uplink and downlink branches using the main and auxiliary RF connectors of the targeted devices. By separating the uplink and downlink channels during the measurements, the acquired results are assured to represent the performance of the data stream and not the acknowledgement message exchange.

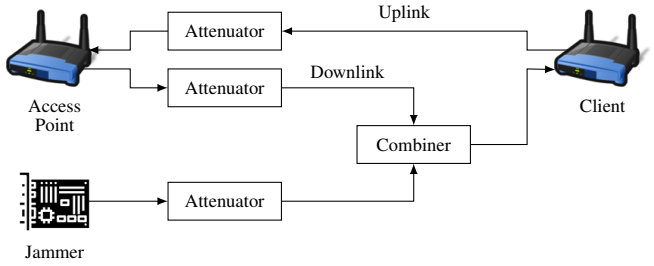

Fig. 5. Setup for measuring the interference caused to WLAN devices by different jamming techniques.

Performance of IEEE 802.11 based WLAN devices under various jamming signals, including tone and sweep jamming, has been previously studied in [10]. Likewise, we concentrate on the operation modes of 11 Mbps DSSS (802.11b) and 9 Mbps OFDM (802.11g) as these modes represent different physical layer technologies and are relatively robust against interference [10]. To measure the maximum throughput we used the bandwidth testing tools provided by the wireless router manufacturer in UDP traffic mode. UDP was used instead of TCP because of TCP's tendency to fail under bad channel conditions [11], concealing the lower layer capabilities. WLAN channel 7 (center frequency f_c = 2.442 GHz) was used during all the measurements.

Performance of both the UAV remote control systems and the WLAN devices was studied under jamming signals with the following parameters:

- **Tone** - a narrowband signal at the center frequency of a single channel of the targeted communication system;
- **Sweep** - a linear chirp swept across the entire 2.4 GHz ISM band at specified rates from 0.5 kHz to 200 kHz;
- **Protocol-Aware** - a signal imitating either FASST or ACCST; this is generated by the developed platform.

B. UAV Remote Control Experimental Results

Because the metrics used for measuring the performances of the two UAV remote control systems are different, the measurement results are presented separately. The measured efficiencies of different jammers against the FASST system are plotted in Figure 6 together with the simulation results from Section III. It is evident that the measurement results in general agree with the simulation results.

The tone jammer was incapable of successfully jamming the remote control link. However, based on the measured bit error

rates at high JSRs, it effectively jammed one of the channels used by the FASST system. The optimal sweeping rate for the sweeping jammer was found to be 1.5 kHz. The sweeping jammer affects enough bits in different packets to successfully jam the remote control link at 10 dB JSR. In comparison, the developed protocol-aware jammer achieved better results, i.e. successful jamming at 2 dB JSR. The thresholds for successful jamming are highlighted with black dots in Figure 6.

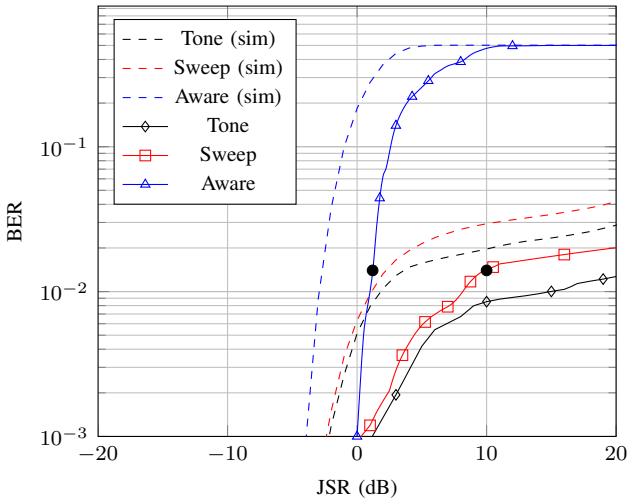

Fig. 6. Measured efficiencies of different jammers against FASST together with the simulated efficiencies. Black dots indicate jamming thresholds.

As mentioned in Section IV, the developed platform can be used to transmit arbitrary data. We studied the data protocol employed in FASST and managed to transmit valid FASST packets from the developed platform. Furthermore, we explored the possibility of taking over the remote control by transmitting valid packets and managed the takeover at 4 dB JSR. Taking over the UAV remote control is somewhat less power efficient than protocol-aware jamming. That is because the signal, which is taking over the remote control, must not only be strong enough to interfere with the reception of the remote control signal at the UAV, but must also be strong enough for the remote control signal to not interfere with it. Takeover also requires more knowledge about the targeted system than jamming, but it can be used to prevent the neutralized UAV from behaving unexpectedly.

The measured efficiencies of different jammers against the ACCST system are plotted in Figure 7. The system indicated loss of connection when the measured PER reached near 0.5 (black dots in Figure 7). The tone jammer effectively jammed one of the channels used by the ACCST system from 0 dB JSR and above. Although, and as was also the case for FASST, jamming only one of the channels is not enough to terminate the remote control link. The sweeping jammer was found to be most efficient with a sweeping rate of 6 kHz and achieved complete jamming of the ACCST system at 15 dB JSR. In comparison, the developed protocol-aware jammer accomplished complete jamming of the ACCST system at -1 dB JSR. Takeover of ACCST was not explored in this work.

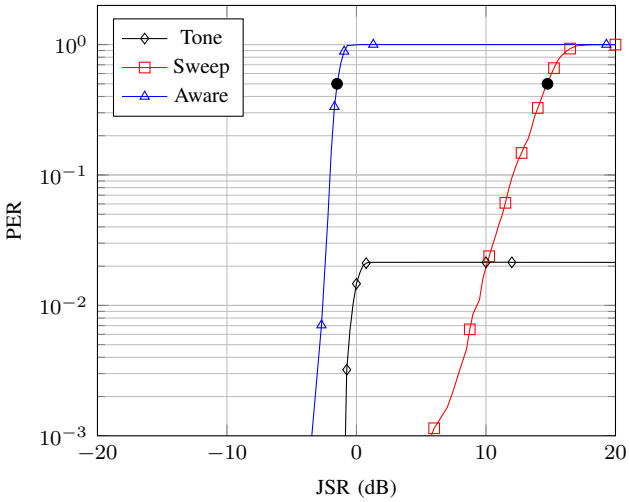

Fig. 7. Measured efficiencies of different jamming techniques against ACCST. The jamming thresholds are indicated by the black dots.

C. WLAN Experimental Results

We evaluated the performance of the WLAN link under sweep and protocol-aware jamming. Tone jamming measurements are omitted here; exhaustive measurements have been presented by others, e.g. in [12]. In Subsection V-B we used different sweeping rates against the FASST and the ACCST because different rates were found to be optimal. However, measurements against WLAN devices revealed very little variance when using those different sweeping rates; thus, we only present the performance of the WLAN devices under sweep jamming at single sweeping rate of 3 kHz.

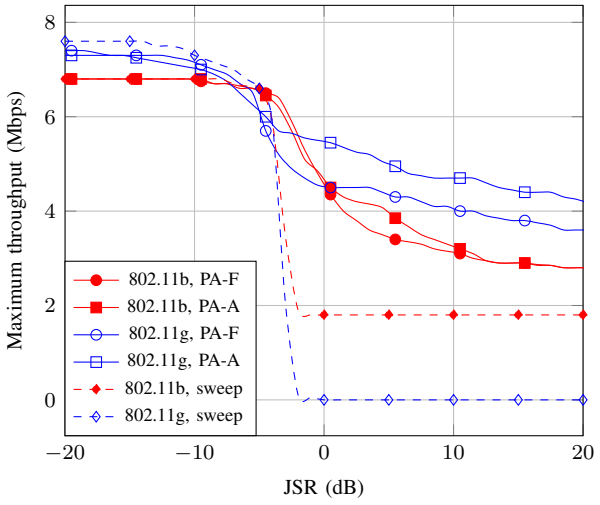

Fig. 8. Measured impacts of different jamming techniques on WLAN devices. PA-F indicates protocol-aware FASST and PA-A is protocol-aware ACCST.

The measured results are presented in Figure 8. The 11 Mbps DSSS mode (802.11b) tolerates sweep jamming better than the OFDM mode (802.11g), which is in accordance with the findings in [10]. The protocol-aware jammer, however, impacts the performance of the WLAN devices at high JSRs

considerably less than the sweep jammer, especially in case of the 802.11g standard when sweep jammer completely disables communication while protocol-aware jammer merely limits maximum throughput.

VI. Discussion & Conclusion

By generalizing the measurement results described in Section V considering the free-space path loss under line-of-sight conditions and assuming equal output powers for the jammer and the remote controller, the developed protocol-aware jammer is in principle capable of successfully jamming the remote control link of the FASST system from as far as 4/5th of the distance from the UAV to the remote control. In comparison, the sweeping jammer with optimal sweeping rate theoretically jams the FASST system successfully only as far as 1/3rd of the distance. Simply put, at similar output powers, the developed protocol-aware jammer has a longer working distance than the sweep jammer, as illustrated in Figure 9.

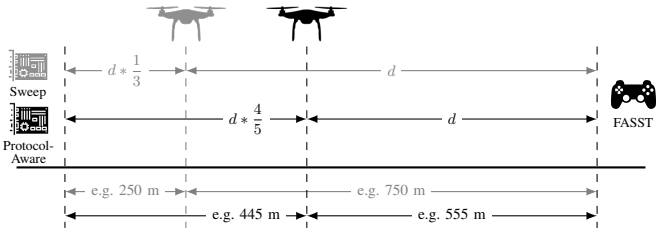

Fig. 9. Calculated successful jamming distances of the sweep and the protocol-aware jammers against the FASST system at equal output powers.

For the ACCST system, the calculated maximum working distance of the developed jammer is greater, being effective as far as 8/7th of the distance. On the other hand, the sweeping jammer is effective only as far as 1/5th of the distance (Figure 10). Thus, in either case protocol-aware jamming is considerably more power efficient than sweep jamming.

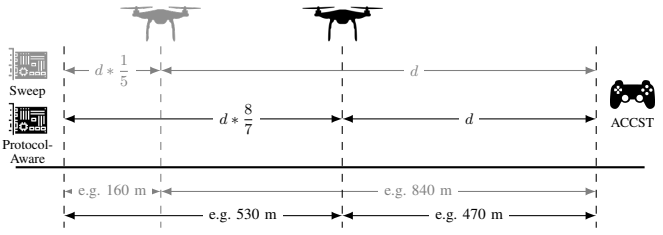

Fig. 10. Calculated successful jamming distances of the sweep and the protocol-aware jammers against the ACCST system at equal output powers.

To conclude, this paper proposes a versatile jamming system capable of applying protocol-aware jamming against different UAV remote control systems. The proposed system leverages the advantages of software defined radio to achieve such versatility.

Our results show that protocol-aware jamming is significantly more efficient than tone and sweep jamming. Although the tone jammer can successfully jam a single channel used by the remote control systems from relatively low JSRs, interference on a single channel is not sufficient to terminate the remote control link. The sweep jammer manages to spread the interference among all of the channels; however, it requires relatively high JSRs to completely prevent the communication. On the other hand, the developed protocol-aware jammer achieves successful jamming at relatively low jammer-to-signal ratios but requires significant knowledge about the targeted system.

When considering the impact that the jamming signals have on WLAN devices, there were notable differences between sweep jamming and protocol-aware jamming signals. In the most extreme cases the sweep jammer halted the WLAN communication while the protocol-aware jammer solely limited its maximum throughput.

Acknowledgment

This work has been conducted in cooperation with the Estonian company Rantelon. This work received funding from the European Union's Horizon 2020 research and innovation programme under Horizon 2020 ERA-chair grant "Cognitive Electronics COEL" H2020-WIDESPREAD-2014-2 (Agreement number: 668995; project TTU code VFP15051).

References

[1] Q. Galvane, J. Fleureau, F.-L. Tariolle, and P. Guillotel, "Automated cinematography with unmanned aerial vehicles," in *Proceedings of the Eurographics Workshop on Intelligent Cinematography and Editing*. Eurographics Association, 2016, pp. 23–30.

[2] A. Merwaday and I. Guvenc, "UAV assisted heterogeneous networks for public safety communications," in *Wireless Communications and Networking Conference Workshops (WCNCW), 2015 IEEE*. IEEE, 2015, pp. 329–334.

[3] Goldman Sachs Research. (2016) Drones: Reporting for Work. The Goldman Sachs Group, Inc. [WWW] http://www.goldmansachs.com/our-thinking/technology-driving-innovation/drones/.

[4] Rohde & Schwarz GmbH & Co KG. Protecting the Sky: Signal Monitoring of Radio Controlled Civilian Unmanned Aerial Vehicles and Possible Countermeasures. Rohde & Schwarz GmbH & Co KG. [WWW] http://www.rohde-schwarz-usa.com/rs/324-UVH-477/images/Drone_Monitoring_Whitepaper.pdf.

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

[6] D. Nguyen, C. Sahin, B. Shishkin, N. Kandasamy, and K. R. Dandekar, "A real-time and protocol-aware reactive jamming framework built on software-defined radios," in *Proceedings of the 2014 ACM workshop on Software radio implementation forum*. ACM, 2014, pp. 15–22.

[7] A. J. Kerns, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, "Unmanned aircraft capture and control via GPS spoofing," *Journal of Field Robotics*, vol. 31, no. 4, pp. 617–636, 2014.

[8] 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, 2016.

[9] H. Wang, J. Guo, and Z. Wang, "Evaluation of security for DSSS under repeater jamming," in *Communications, 2007. ICC'07. IEEE International Conference on*. IEEE, 2007, pp. 5525–5530.

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

[11] G. Holland and N. Vaidya, "Analysis of TCP performance over mobile ad hoc networks," *Wireless Networks*, vol. 8, no. 2/3, pp. 275–288, 2002.

[12] T. Karhima, A. Silvennoinen, M. Hall, and S.-G. Haggman, "IEEE 802.11 b/g WLAN tolerance to jamming," in *Military Communications Conference, 2004. MILCOM 2004. 2004 IEEE*, vol. 3. IEEE, 2004, pp. 1364–1370.