A Configurable Radio Jamming Prototype for Physical Layer Attacks Against Malicious Unmanned Aerial Vehicles

Giulio Caforio*, Davide Scazzoli*, Luca Reggiani*, Maurizio Magarini*,
Yannick Le Moullec†, Muhammad Mahtab Alam†

*Dept. of Electronics, Information and Bioengineering, Politecnico di Milano, Milano, Italy,
(e-mail: giulio.caforio@mail.polimi.it, {davide.scazzoli, luca.reggiani, maurizio.magarini}@polimi.it)
†Department of Electronics, Tallinn University of Technology,
12616 Tallinn, Estonia (e-mail: firstname.lastname@taltech.ee)

***Abstract*—The goal of this paper is to design and prototype a radio jamming system that is able to interfere the communication drone-remote control, in particular, disabling the motion control system. The drone adopted in the experimental session is the AEE Toruk AP10 Pro, characterized by a digital wireless control system centered at 868MHz. We have created a configurable jamming prototype for limit as much as possible the interference with other radio systems and study the effect of the signal band on the motion control system. We will present our system with both simulation and experimental validation.**

***Index Terms*—UAVs, Jamming, Digital Communication, Wireless Communications, RF systems**

I. Introduction

In these days the usage of drones, or Unmanned Aerial Vehicles (UAVs), has become very popular because of their low cost, high mobility, wide coverage, and on-demand deployment. UAVs have been extensively used in both military and civilian applications, such as search and rescue, inspection and surveillance and cargo transportation [1]. The prosperous global market of UAVs is also envisioned to bring new and valuable opportunities to the future wireless communication industry, such as the 5G cellular network [2]. On the other hand, drones could be also used for a plethora of nefarious or illegal purposes, from voyeurism, to assault or even terrorism [3]. For this reason, it is ever more important to find countermeasures to identify and stop illegal activities using drones. Several methods for identifying the presence of drones, based on InfraRed (IR), acoustic or radio signal detection are available [4] and other works have focused on methods to stop drones. From Software Defined Radio attacks on the communications [5], to tricking their GPS receiver [6] or even employing UAVs equipped with nets to physically capture another UAV [7].

In this paper we propose and design a new jamming system for physical layer attacks. In particular, we want to create a configurable system, in band and frequency, that gives the possibility to limit as much as possible the interference with other radio services operating on frequencies that are close to the wireless control system of the drone. We want also to study the effect of the band of the signal transmitted through computer simulations and experimental validations.

978-1-7281-9444-8/20/$31.00 © 2020 IEEE

The rest of the paper is divided as follows: in Sec. II we present the technical specifications of the drone used for experimental validation, its relevant characteristics and those of a typical transceiver used for its control. In Sec. III we will introduce the structure and principle of our jamming solution and we show both simulations and experimental results in Sec. IV. Finally, Sec. V concludes the paper.

II. The AEE Toruk AP10 Pro and the Transceiver Si44631b

A. The AEE Toruk AP10 Pro

The AEE Toruk AP10 Pro is a professional drone for civilian use [8]. It is characterized by:

- 20 minutes flight time;
- three wireless systems centered at different frequencies: one used for video transmission at 2.4GHz, one used for the motion control system at 868MHz (experimentally found) and the last used for GPS (around 1.5GHz);
- a maximum distance achievable from the remote control in Line Of Sight (LOS) and in absence of interference of 700m;
- an automatic flight control system: when there is a strong interference (or the remote control is switched-off) and the quadcopter does not regain signal from the remote control within 2 seconds, the drone enters failsafe mode, and initiates automatic flight control to fly back to the Home Point (HP). The quadcopter will continue to hover for 15 seconds and evaluate vertical distance to the HP. If the distance is more than 25 meters, the quadcopter will commence to fly back to the HP. If the distance is less than 25 meters, the drone will fly up vertically to 25 meters higher than the HP, and then commence to return. When the drone reaches the HP it will hover for 5 seconds

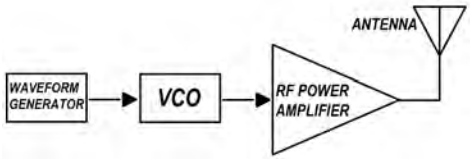

Fig. 1. System block diagram.

and then automatically land [8]. This procedure is done in case of optimal GPS signal condition.

B. The Transceiver Si44631b - A Brief Description

The transceiver Si44631b, that belongs to the family Si446x, is an high-performance, low-current, wireless Industrial, Scientific and Medical (ISM) transceivers that covers the sub-GHz bands [9]. The transceivers adopted in our experiment are two: one drives the AEE Toruk AP10 Pro and the other its remote control. Both transceivers are directly connected to their own MicroController Units (MCUs), whose codes are unknown.
The Si446x operates as a Time-Division Duplexing (TDD) transceiver where the device alternately transmits and receives data packets. The chip also supports different modulation options and can be used in various configurations to tailor the device to any specific application or legacy system for drop in replacement. The modulations supported by Si466x are: Gaussian Frequency Shift Keying (GFSK), Frequency-Shift Keying (FSK), Four-Level GFSK (4GFSK), Four-Level FSK (4FSK), and On-Off Keying (OOK). Minimum shift keying (MSK) can also be created by using GFSK settings. GFSK is the recommended modulation type as it provides the best performance and cleanest modulation spectrum. However, the Si446x family supports frequency hopping, TX/RX switch control, and antenna diversity switch control to extend the link range and improve performance [9].

III. System model

The radio jamming system designed follows a similar approach to the one proposed in [10]. The device is composed by four parts: a periodic waveform generator, a Voltage-Controlled Oscillator (VCO), a Radio-Frequency (RF) amplifier, and, obviously, an antenna (Fig. 1). The jamming technique adopted is the *Sweep Jamming* technique where the attacker jams different frequencies at different time [11].

A. The Waveform Generator

The waveform generator proposed is a triangular waveform generator. The circuit designed can be represented by a simple block diagram, shown in Fig. 2. The idea is to generate a triangular wave by integrating a square wave.

The first part of the system is composed by Arduino Uno, that is an MCU used in this application to generate a 0V-5V square wave with period of $T_w = 1/980Hz \approx 1ms$ by means of the instruction `analogWrite(out,127)` which generates a square wave signal with duty cycle 50%. In order to use this signal in a real integrator with Operational AMPlifier (OPAMP) the mean value of the wave must be 0V

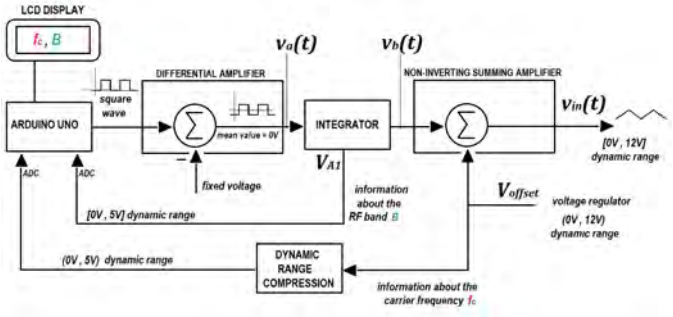

Fig. 2. The block diagram of the triangular waveform generator.

in order to avoid the saturation of the OPAMP. So, by using a differential amplifier we generate a ± 2.5V square wave $v_a(t)$ with period $T_w \approx 1ms$ (Fig. 3). This signal is the input of the real integrator whose transfer function can be approximated in this way

$$\frac{V_b(s)}{V_a(s)} = F(s) \approx -\frac{1}{s(R_5 + R_6)C_1} \tag{1}$$

(the approximation is valid since resistor R_7 has an high resistance). The Laplace transform of $v_a(t)$ can be easily derived by applying the definition for periodic signals of period T_w

$$G(s) = L[g(t)] = \frac{1}{1 - e^{-sT_w}} \int_0^{T_w} e^{-st} g(t)dt. \tag{2}$$

The result for $v_a(t)$ is

$$V_a(s) = \frac{2.5V}{s} \tanh\left(\frac{T_w}{4}s\right). \tag{3}$$

The output of the integration stage $V_b(s)$ is given by the product of the two Laplace transforms (1) and (3). By applying the inverse Laplace transform to $V_b(s)$ we obtain, in the steady state, a triangular wave with zero mean and period $T_w \approx 1ms$ whose expression is

$$v_b(t) \approx K\left[t + 2\sum_{m=1}^{\infty}(-1)^m(t - mT_w/4) - T_w/4\right] \tag{4}$$

with

$$K = -\frac{2.5V}{(R_5 + R_6)C_1}. \tag{5}$$

Expression (4) is defined for $t \geq 0s$. Its voltage range can be easily derived by a simple difference between the maximum and the minimum value reached by the wave

$$\Delta V(R_5) = v_b\left(n\frac{T_w}{2}\right) - v_b\left((n+1)\frac{T_w}{2}\right) \tag{6}$$

for $n \in \mathbb{N}$ and n even. The result is

$$\Delta V(R_5) = -K\frac{T_w}{2} = \frac{2.5V}{(R_5 + R_6)C_1}\frac{T_w}{2}. \tag{7}$$

By modifying the value of the potentiometer R_5 we can adjust the voltage range according to our requirements. Specifically, $\Delta V(R_5 = 470k\Omega) \approx 116mV$ and $\Delta V(R_5 = 0\Omega) \approx 2.58V$.

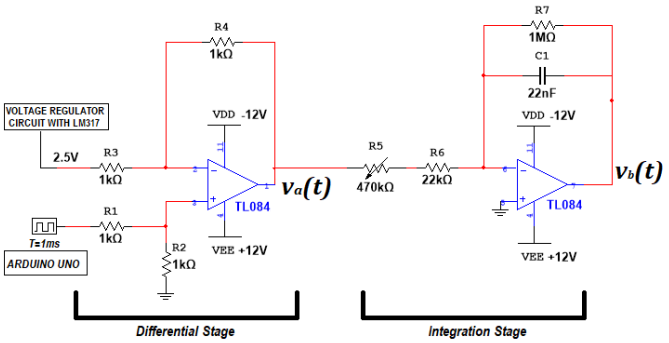

Fig. 3. A differential amplifier followed by a real integration stage [12] [13] .

Fig. 4. The RF stage of the jamming system: VCO (left), RF amplifier (center) and Yagi antenna (right).

Maximum and minimum value are respectively $\pm 116mV/2 = \pm 58mV$ and $\pm 2.58V/2 = \pm 1.29V$.

The wave obtained in equation (4) is sent to a non-inverting summing amplifier that adds the desired mean component, that we can call V_{offset}. So, we can choose the voltage range by modifying the value of R_5 and the mean value by changing V_{offset} (the value of V_{offset} is generated from a voltage regulator circuit and can be manually modified [12]). The result is a controllable signal

$$v_{in}(t) = v_b(t) + V_{offset}, \tag{8}$$

which will be the input of our VCO.

B. The RF Stage of the Jamming System

The RF stage of the entire device is composed by three parts: a VCO, an RF amplifier and an antenna.

The VCO (manufacturer FLAMESER) used in this project is a small module of size 22mm x 45mm which can work from 515MHz up to 1150MHz characterized by an RF SubMiniature version A (SMA) output male connector (characteristic impedance $Z_C = 50\Omega$) (Fig. 4). The Input-Output (I/O) characteristic, which is reported in Table I alongside other parameters, can be approximated by the linear relation

$$f(v_{in}) \approx 798MHz + (v_{in} - 4.45V) \cdot 60\frac{MHz}{V}, \tag{9}$$

where f is the output frequency and v_{in} the input voltage. The approximation has been made more and more accurate and precise around the motion control system of the drone (868MHz).

v_{in} [V]	Output Frequency [MHz]	Output Power [dBm]
0.5	560	-7.6
1	601	-6.19
2	671	-3.2
3	731	-2.4
4	784	-1.62
5	833	-1.77
6	885	-0.76
7	948	0.77

TABLE I
VCO REAL I/O CHARACTERISTIC (6V POWER SUPPLY). THE INPUT VOLTAGE v_{in}, FROM TECHNICAL SPECIFICATION OF THE DEVICE, CAN VARY FROM 0V TO 12V.

The next stage of the device is constituted by the RF amplifier. The amplifier, from FLAMESER (Fig. 4), is characterized by the following properties:

- working frequencies: 1MHz÷930MHz;
- maximum input power: 0dBm;
- power gain of approximately 30dB in the range of interest (around 868MHz);
- power supply: 12V;
- RF I/O connectors: SMA male ($Z_C = 50\Omega$).

The antenna selected for the project is a Yagi antenna (from LPRS, Fig. 4) because it is a very directive antenna and so it is more effective than an omnidirectional one. The antenna characteristics are the following:

- nominal impedance or load impedance: $Z_L = 50\Omega$;
- active element: folded dipole. The folded dipole is characterized by a low quality factor (Q), which means that is a wideband antenna;
- number of directors/reflectors: 7/1;
- working frequencies: 824MHz÷960MHz;
- maximum gain: 13dBi at 900MHz;
- maximum input power: 100W;
- Front-to-Back ratio (F/B ratio) $>$ 15dB;
- RF connector: SMA female ($Z_C = 50\Omega$).

All RF components are connected via coaxial SMA cables characterized by $Z_C = 50\Omega$ in order to have the maximum transfer of power to the load (impedance matching) and to avoid undesired reflections.

C. System Parameters Control and the RF Spectrum

In this subsection we will explain how the prototype gives the possibility to control two important parameters, which are the band and the carrier (or center) frequency.

The signal transmitted is a chirp signal. Its mathematical expression is

$$s(t) = Acos(2\pi f(t)t). \tag{10}$$

By substituting the instantaneous frequency $f(t)$ in (10) with expression (9) and by using also (8), after some manipulation the oscillation frequency of the cosine wave can be seen as the sum of two component

$$f(t) = f(v_{in}(t)) = f_0 + v_b(t)60\frac{MHz}{V}. \tag{11}$$

The first component, f_0, is a constant value and it is called carrier frequency. The other term, instead, is an instantaneous component that set the signal frequency range.

The value of the carrier frequency can be set by changing the mean value of $v_{in}(t)$ (V_{offset}). The MCU obviusly knowns expression (9) so, by using a dynamic range compression system (Fig. 2), we send the value of V_{offset} to the Analog-to-Digital Converter (ADC) of Arduino Uno that prints the corresponding frequency value on the LCD. Clearly, dynamic range compression is done in order to adapt the signal to the dynamic of the ADC.

Let's see now how we can obtain information about the instantaneous component that characterized the frequency range of the signal. We can call this parameter band, or RF band, of the chirp. The value of the RF band can be decided according to the value of voltage drop V_{A1} of the dual potentiometer R_5 that drives the closed-loop gain of the real integrator. This potentiometer is composed by six pins, three of them are connected to the circuit and the other three are isolated and generally used to read the value of the resistance. With reference to Fig. 5 we can write

$$V_{A1} = \frac{5V}{470k\Omega}(470k\Omega - R_5) = \frac{5V}{470k\Omega}R_B, \qquad (12)$$

with $0\Omega \leq R_B \leq 470k\Omega$. The RF band is a function of this voltage V_{A1} and, in particular, it follows an exponential trend, because the closed-loop gain is not a linear function of R_5 (see expression (1)). We can approximate the shape (derived also experimentally in Fig. 6) with this expression, known by the MCU

$$B \approx \begin{cases} 4\frac{MHz}{V}V_{A1} + 4MHz \\ \qquad\qquad \text{if } \ 0V \leqslant V_{A1} < 3V \\ 11\frac{MHz}{V}(V_{A1} - 3.25V) + 18MHz \\ \qquad\qquad \text{if } \ 3V \leqslant V_{A1} < 4V \\ 90\frac{MHz}{V^2}(V_{A1} - 4V)^2 + 28MHz \\ \qquad\qquad \text{if } \ 4V \leqslant V_{A1} \leqslant 5V \end{cases} . \qquad (13)$$

The overall system is now ready and able to print band and carrier frequency on the LCD. An example is reported in Fig. 7.

The signal at the output of the VCO reaches the input of the RF amplifier. Here, since the VCO output power corresponds to the maximum input power of the RF amplifier (Sec. III-B), some undesired component is generated (Fig. 8). This component is very weak and its power is around -20dBm, $i.e.$ it is 50dB less then the main one and can be neglected in our experiments.

IV. Simulations and Experimental Results

This final section shows the effectiveness of the jamming system, shown in Fig. 10, by means of experimental results. The quality of the interference has been also evaluated by a Simulink model in terms of Bit Error Rate (BER).

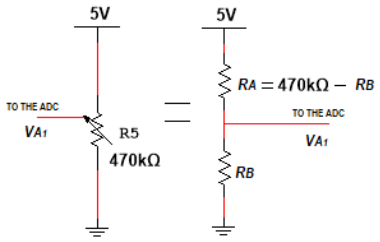

Fig. 5. The three pins of the dual potentiometer R_5 isolated from the circuit. The equivalent model is reported on the right.

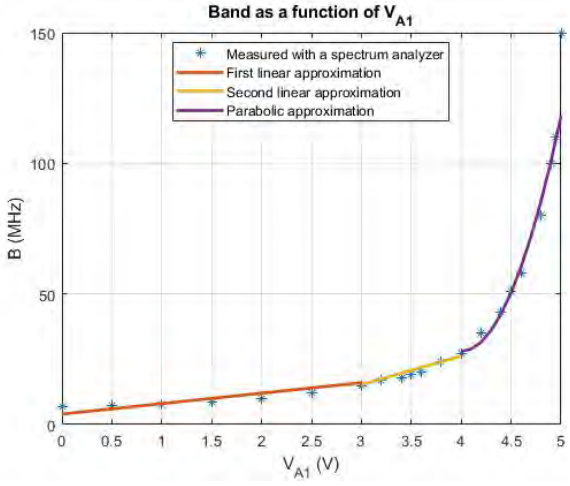

Fig. 6. The RF bandwidth of the chirp signal as a function of V_{A1}.

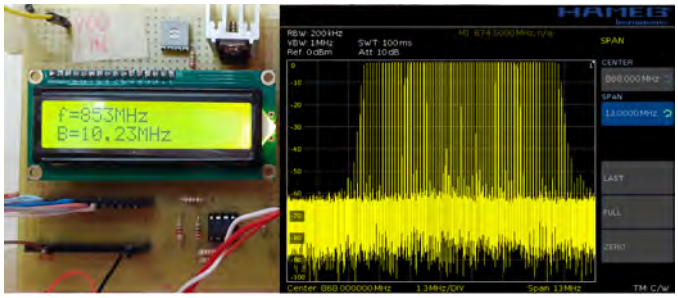

Fig. 7. VCO output spectrum for $R_5 = 470k\Omega$ (right side). The values of the RF band and the carrier frequency are printed on the LCD (left side).

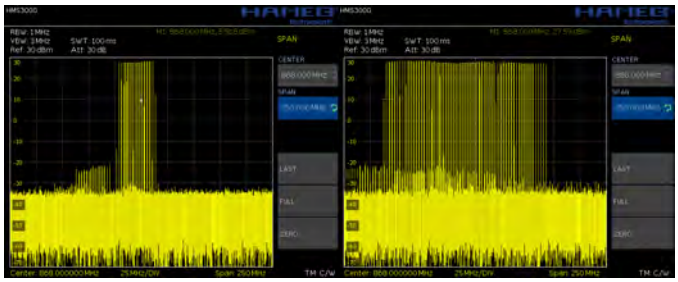

Fig. 8. In the figure are visible the main component and the undesired smaller component in the narrowband (left) and wideband case (right) at the output of the RF amplifier.

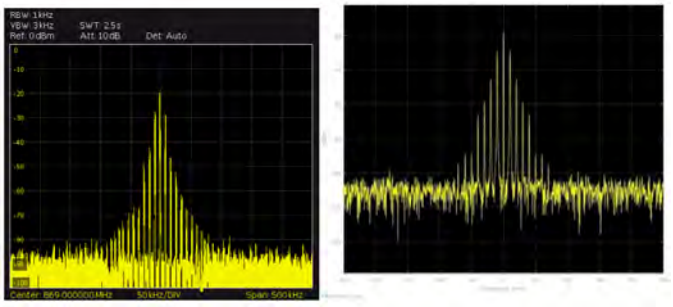

Fig. 9. The real remote control radio spectrum detected by a spectrum analyzer (left side) and the one generated by Simulink (right side).

A. Simulation Results

The objective of the simulation part is to study the performance of a baseband unidirectional GFSK transmission in presence of a radio interference. For the sake of simplicity we do not consider source coding, channel coding, Doppler shifts and diversity schemes. Moreover, since the experiments were done in rural areas, the Air-to-Ground channel model can be approximated as an AWGN channel (LOS channel) with just one path. The equivalent passband model of the system is reported in Fig. 11 (simulations were done in Simulink). The drone-remote control GFSK digital wireless link is characterized by $h = 0.5$, $BT = 0.9$, frequency space $\Delta f = 10kHz$, bit time $T = 1/(2\Delta f) = 50\mu s$ and traceback depth equal to 45 (*i.e.*, the number of trellis branches used to construct each traceback path). Fig. 9 shows a comparison of the simulated and measured spectrum.

The demodulation process is done with a correlator followed by a Maximum-Likelihood Sequence Detector (MLSD) that searches the paths through the state trellis for the minimum Euclidean distance path. When the modulation index h is a rational number, there are a finite number of phase states in the symbol. The block uses the Viterbi algorithm to perform MLSD [14].

We assume a transmitted power of -17dBm by the remote control which uses a $\lambda/4$ dipole antenna with 3dBi of gain. The drone receiving antenna gain is assumed to be omnidirectional since it is a wire placed on the landing gear. For the jamming system, the transmitted power is 30dBm (1W) and the antenna gain is assumed to be constant and equal to 13dBi. Field free space attenuation is obviously considered for both signals.

The interference is a complex chirp with an initial frequency (greater or equal to 0Hz) and a target frequency reached at a given target time.

The simulation scenario consists in moving the drone towards the area where the jamming device is placed, considering an example application in which the device is used to create a no-fly zone. In other words, the drone is moving away from the remote control and it approaches the zone where there is the interference. Thus, it is expected to see a worsening of the BER as the distance drone-remote control d_{rc-d} increases. The other simulation parameters are:

- chirp bandwidth $B = 25MHz$ and $B = 150MHz$ around $f = 0Hz$;
- triangular wave period of 1ms;
- simulation time of 1.5s;
- the following condition is always valid: $d_{rc-d} + d_{j-d} = 50m$, where d_{j-d} is the distance between the drone and the jamming device (Fig. 12).

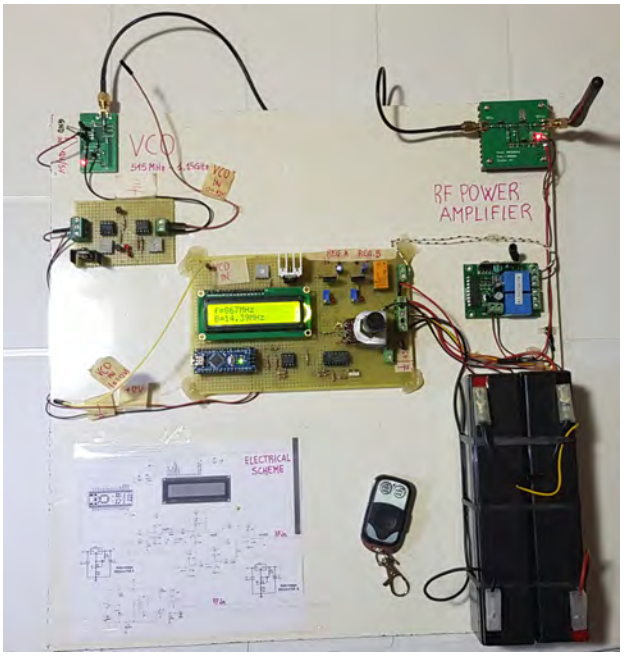

Fig. 10. The prototype of the radio jamming device (version with Arduino Nano). The circuit is also radio-controlled by a 433MHz wireless system.

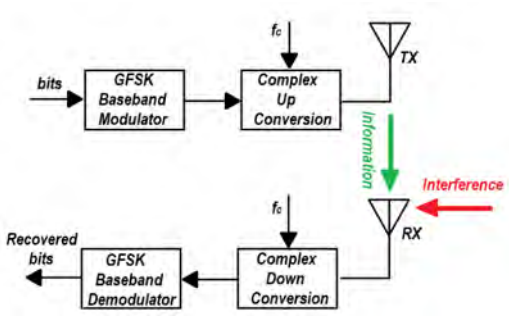

Fig. 11. The block diagram of the unidirectional GFSK transmission subject to radio interference. This is the passband equivalent model.

The plot of the BER in Fig. 13 shows that the effect of the system designed is very good. However, it can be observed a better performance in the narrowband case: this is simply due to the fact that the electromagnetic energy of the chirp signal is concentrated in a small frequency range. In other words, we are transmitting most of the time in the motion control system band.

B. Experimental Results

Experimental results were done Thursday, August 13, 2020 in rural area from 6:30 AM to 8:00 AM, so the effect of the wind is negligible early in the morning. However, there are no

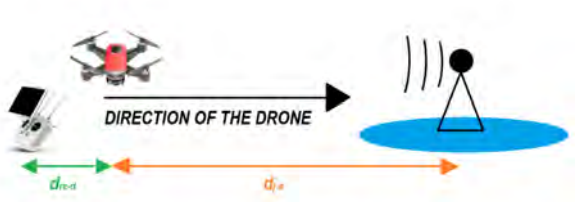

Fig. 12. Scenario considered for simulations and experiments

Bandwidth (B)	**Carrier Frequency** (f_0)	**Average** d_{j-d}
6.7 MHz	868.770 MHz	No effect registered
16 MHz	868.770 MHz	No effect registered
35 MHz	868.770 MHz	No effect registered
45 MHz	868.770 MHz	39.27 m
60 MHz	868.770 MHz	44.43 m
78 MHz	870 MHz	40.3 m
103 MHz	872 MHz	43.9 m

TABLE II
EXPERIMENTAL RESULTS. THE VALUE OF d_{j-d} IS THE DISTANCE WHERE THE RADIO CONTACT IS COMPLETELY LOST.

obstacles in the site, so the AWGN channel model chosen for the simulation is a good approximation.

We remind that the communication between the drone and its remote control occurs at $f_0 = 868MHz$ in TDD, *i.e.* uplink and downlink use the same radio channel at different time. The results are reported in Table II. From the outcomes we can see that the interference signal is ineffective when $B = 6.7MHz, 16MHz, 35MHz$: this is simply due to the frequency hopping adopted by the transceiver described in Sec. II-B. As the band increases, we can see the effect of the interference on the system but the outcomes do not follow the same approach obtained in Simulink. In this case simulation and experimental results don't match each other because of uncontrollable parameters, which are channel coding, the transmitted power, multiple fading (reflection from the ground), antenna gains not constant at different frequencies and Doppler effect. Nevertheless, the system designed works well if the band is large enough $B > 35MHz$ to block the frequency hopping technique.

V. CONCLUSIONS

The objective of this paper was to develop and prototype a configurable radio jamming system which is able to interfere the communication of a drone with its remote control by following the same approach of [10] but driving the overall apparatus with a triangular waveform generator instead of a sawtooth one since, in a time period T_w, we span two times the band of interest.

The prototype has revealed good results since, despite the countermeasure adopted by the target wireless link, we have demonstrated how to obtain an outage for a strong digital wireless communication through an analog device. The device is also able to preserve other wireless systems by correctly setting the RF parameters from the LCD: this is good because there is no need to use a spectrum analyzer.

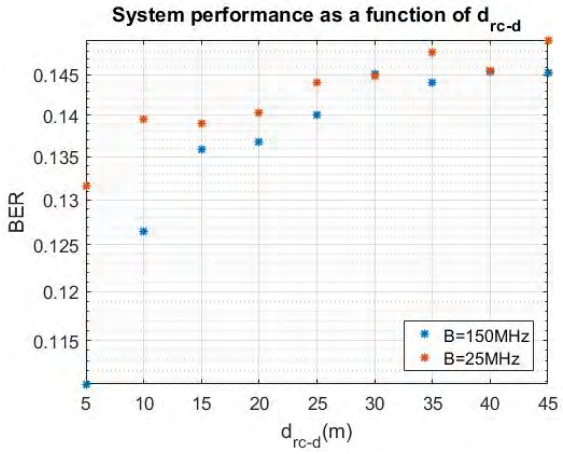

Fig. 13. BER as a function of d_{rc-d} for $B = 25MHz$ and $B = 150MHz$.

We conclude this paper announcing that, for our future works, we intend to develop other strategies to hijack control of a drone altogether.

ACKNOWLEDGMENT

This project was partly funded by NATO-SPS funding grant agreement No. G5482.

REFERENCES

[1] G. Zhang, Q. Wu, M. Cui, and R. Zhang, "Securing uav communications via joint trajectory and power control," *IEEE Transactions on Wireless Communications*, vol. 18, no. 2, pp. 1376–1389, 2019.
[2] Q. Wu, W. Mei, and R. Zhang, "Safeguarding wireless network with uavs: A physical layer security perspective," *arXiv preprint arXiv:1902.02472*, 2019.
[3] A. Roder and K.-K. R. Choo, "Unmanned aerial vehicles (uavs) threat analysis and a routine activity theory based mitigation approach," in *National Cyber Summit*. Springer, 2019, pp. 99–115.
[4] P. Stoica and C. Molder, "Comparative analysis of methods to detect radio-controlled commercial uavs," *Scientific Bulletin" Mircea cel Batran" Naval Academy*, vol. 21, no. 1, pp. 1–6, 2018.
[5] K. Pärlin, M. M. Alam, and Y. Le Moullec, "Jamming of uav remote control systems using software defined radio," in *2018 International Conference on Military Communications and Information Systems (ICMCIS)*. IEEE, 2018, pp. 1–6.
[6] 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.
[7] X. Meng, X. Ding, and P. Guo, "A net-launching mechanism for uav to capture aerial moving target," in *2018 IEEE International Conference on Mechatronics and Automation (ICMA)*. IEEE, 2018, pp. 461–468.
[8] "Toruk ap10 pro drone," https://www.pnj.fr/en/shop/toruk-ap10-pro-drone/, accessed: 26-11-2019.
[9] "Silicon labs, high-performance low-current transceiver si446x." [Online]. Available: https://www.silabs.com/documents/public/data-sheets/Si4464-63-61-60.pdf
[10] H. Zhang, H. Zhang, X. Liu, and T. A. Gulliver, "A new electromagnetic jamming system for unmanned aerial vehicles," in *2017 IEEE Pacific Rim Conference on Communications, Computers and Signal Processing (PACRIM)*. IEEE, 2017, pp. 1–5.
[11] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, "A survey on jamming attacks and countermeasures in wsns," *IEEE Communications Surveys & Tutorials*, vol. 11, no. 4, pp. 42–56, 2009.
[12] T. Instruments, "Lm317 3-terminal adjustable regulator," *Acesso em*, vol. 3, 1997.
[13] D. TL084, "General purpose j-fet quad operacional amplifiers," 2001.
[14] J. B. Anderson, T. Aulin, and C.-E. Sundberg, *Digital phase modulation*. Springer Science & Business Media, 2013.