

# Keeping UAVs Under Control During GPS Jamming

Bertold Van den Bergh<sup>ID</sup> and Sofie Pollin<sup>ID</sup>

**Abstract**—Unmanned aerial vehicles (UAV) are being more and more widely deployed. Although, initially most UAVs were controlled by a pilot, autonomy has increased. This requires the flight controller in the UAV to accurately know the current system state. Knowing the current position is of crucial importance. Fortunately, this can be reliably obtained from a global navigation satellite system (GNSS) receiver. Recently, it was shown that criminal GNSS jamming frequently occurs. First, this paper analyzes the risk posed by off-the-shelf civilian GPS jammers to UAVs. Then, as the main contribution of this paper, a countermeasure is described and implemented using custom hardware and software that allows the control radio to be used as a backup navigation source. Finally, the proposed solution is tested in ideal and field conditions. It is shown that good performance can be obtained by the presented system, almost without additional system cost.

**Index Terms**—Aerospace safety, global positioning system, IEEE 802.15 standards, jamming, unmanned aerial vehicles.

## I. INTRODUCTION

UNMANNED aerial vehicles (UAVs), commonly called drones, are now an established part of modern society. They are employed for diverse applications such as entertainment, security, surveillance, and many more. While UAVs that are used by amateurs are often completely controlled by the hobby pilot, drones that are deployed for professional applications usually rely on an elaborate autopilot that takes care of the low-level tasks related to flying and stability of the drone [17]. The operator then only manages high level parameters related to the mission at hand. A typical example is specifying what the camera should film [10]. The UAV will then automatically attempt to keep this object in the frame. Semi-autonomous UAVs receive high-level mission constraints from a human, and execute most of their complex missions autonomously.

These semi-autonomous UAVs rely critically on estimating the current system state. Attitude and altitude information is required for keeping the UAV in the air. This information is easily obtained from an inertial measurement unit and air pressure sensor. Almost all missions require the drone to know its current location to keep track of the high-level mission progress and to control the drone. This information is used for waypoint navigation, loitering, return to home, and more. Usually, a global navigation satellite system (GNSS) receiver, for example GPS

Manuscript received September 18, 2017; revised March 12, 2018 and May 21, 2018; accepted August 17, 2018. Date of publication December 28, 2018; date of current version May 31, 2019. This work was supported by the Fonds Wetenschappelijk Onderzoek and the Scientific Research, Flanders (F.W.O.-Vlaanderen). (Corresponding author: Bertold Van den Bergh.)

The authors are with the Departement Elektrotechniek, Katholieke Universiteit Leuven, 3001 Leuven, Belgium (e-mail: vandenbergh@bertold.org; sofie.pollin@esat.kuleuven.be).

Digital Object Identifier 10.1109/JSYST.2018.2882769

and/or globalnaya navigazionnaya sputnikovaya sistema is used for UAV localization [17].

A significant problem with using GNSS technology is that the signals are very weak. The GPS L1 frequency allocation allows a transmission power up to 25.6 W. A whole-earth antenna with a gain of 13 dBi is used to obtain a final effective isotropic radiated power of 500 W. Due to the high path loss between the satellite and the earth, the power at the surface is only  $-130$  dBm (isotropic antenna). This is about 20 dB below the thermal noise floor, assuming the signal power is evenly spread in a 2-MHz bandwidth.

This extremely low signal power makes the technology very vulnerable to interference and deliberate jamming. In a GNSS-denied environment, UAVs working in an autonomous mode are forced to take corrective actions. Many drones will slowly descend and try to land. Others switch back to a manual mode, where the operator is supposed to intervene. We foresee that in the future significantly more autonomous drones will be deployed, potentially operating beyond visual line-of-sight from the operator. Furthermore, the scope of the mission may make traditional emergency measures such as landing infeasible. Therefore, it is needed to provide UAVs with a second localization system that can be used to guide the UAVs to their home location when GNSS reception fails.

The payload capabilities of UAVs, especially smaller amateur drones, is typically very constrained. As a result, it is not desirable to carry a second localization system that enables guidance of the UAV when the GNSS signal is jammed or lost. Ideally, this emergency localization system can be provided by the hardware already onboard for communication. In this paper, we study the performance of a multiantenna communication system on the drone for angle-of-arrival estimation of the ground home transmitter.

In the first section, an overview is given of the risks posed to UAVs by illegal consumer GNSS jamming devices. In the second section, the proposed countermeasure is described, which can be implemented at no or low cost and will significantly increase the safety of the UAV design. Then, in the third section, the implementation is explained. Finally, the results are presented in the fourth section.

## II. RISKS OF GNSS JAMMING

In this section, we analyze the risks of GNSS jamming for UAV receivers. First, we motivate that GPS jamming technology is available, and that jamming incidents occur frequently. Then, we analyze the jamming sensitivity of a typical UAV GPS system, consisting of a GPS receiver and antenna deployed at various heights. Finally, we propose a countermeasure, enabling



Fig. 1. Multitechnology jammer offered for sale on the Internet [19].

the UAV to find the direction of the ground station and fly in that direction.

#### A. GPS Jamming Feasibility and Incidents

Although usually considered as something that only happens in warzones, illegal GNSS jamming technology is readily available for purchase over the Internet and is deployed by ordinary civilians. They are often used to prevent GPS tracking of company cars. Criminals also like to use the technology for disabling anti-theft tracking devices.

Mitch *et al.* [23] analyze the waveforms of 18 different over-the-counter jammers. Many of the analyzed devices transmit tens to hundreds of milliwatts of RF power, although not always on the right frequency and often over an excessively wide bandwidth. This is likely due to the fact that the devices use a simple voltage-controlled oscillator without a phase-locked loop (PLL) to control the output frequency. All tested devices seem to transmit some form of a sweeping continuous wave (CW) signal over the L1 C/A band.

Fig. 1 shows a picture of a jammer being offered for sale. The website selling this product was easily found using Google [19]. The 135 Euro device claims a total output power of 15 W and jams many different applications. The output power in the GPS L1 band is stated as 33 dBm.

A joint study by the government of the United Kingdom and Chronos Technology was performed to investigate how common GPS jamming incidents are in practice [27]. They deployed 20 monitoring stations all over the United Kingdom. Several hundred events were detected by some sensors, which shows that the risk is very real.

#### B. UAV GPS Jamming Sensitivity

The risk to an UAV may be even more significant than the risks described in the previous section. Although the jamming signal will be quickly attenuated by buildings and other obstacles near the source, a drone at high altitude is likely to experience a much better line-of-sight path to the jammer [9]. This results in a greatly extended jamming range. In the worst case, if we assume free-space path loss the power at the receiver will be

given by

$$P_r = P_t G_t G_r \left( \frac{\lambda}{4\pi R} \right)^2. \quad (1)$$

Considering, for example, jammer 11 from [23] we see it has an output power of  $P_t = 244$  mW in the L1 band. An attenuation of 108 dB was required to stop it from interfering with the test receiver. This results in a received signal power of  $P_r = -84$  dBm, or an approximate free-space jamming range of 5 km assuming 2.1-dBi transmitter antenna gain.

Most UAV GPS receivers employ a patch antenna pointed at the sky. This will reduce the effect of the jammer since it will be in an unfavorable position with respect to the antenna pattern. Using data obtained from the specification of a typical GPS antenna [18], we see that a source at a 90° angle will have an attenuation of approximately  $-5.6$  dB. This reduces the jamming range in the example to approximately 2.5 km.

At first it may seem counterintuitive that such a strong signal is needed to jam the weak GPS signal. This is because the GPS system uses direct sequence spread spectrum (DSSS) with binary phase-shift keying (BPSK) modulation. All the jammers described in the study seem to use a swept CW signal, which is extremely suboptimal when jamming a DSSS signal, as the DSSS signal has a chip rate of  $R_c = 1.023$  MHz. The actual data rate is very low, only  $R_d = 50$  b/s. Thus, the theoretical processing gain is

$$G_p = 10 \log_{10} \frac{R_c}{R_b} = 43 \text{ dB}.$$

Therefore, the  $-84$ -dBm jamming signal will reduce the signal to interference ratio to approximately 2.8 dB, resulting in a BPSK bit error rate of 4%, and corrupting around 70% of all GPS L1 C/A navigation words.

Should the jammer transmit a signal using the GPS spreading sequences, it would be able to enjoy the same coding gain as the real GPS system. This would result in a significantly increased line-of-sight jamming range. The exact distance is not very useful, since it would exceed the radio horizon under almost all UAV operating parameters. Such jammers do not seem to be available on the open market, although they would not be significantly more difficult to build. Nevertheless, we can expect the jamming waveforms will evolve.

To illustrate the difference in jamming range between a UAV and a terrestrial receiver, we performed four simulations using Radio Mobile [24]. They show the distance at which jamming is successful using a transmitter placed 3 m above the ground. The terrestrial receiver is also assumed to be at this altitude. Two different UAV altitudes are simulated: 40 and 250 m. Fig. 2 shows the area in which a terrestrial GPS receiver at 3-m altitude would not function. This area is very small, on the order of a few tens of meters. The edges are often defined by the first obstruction. Note that the location of the jamming transmitter is marked with the red pentagram.

Figs. 3 and 4 show the jamming range when the receiver is an airborne UAV. It can be seen that the low-power jamming transmitter can cause disruption in a radius of a few kilometers. This represents a serious risk should UAV deployment become

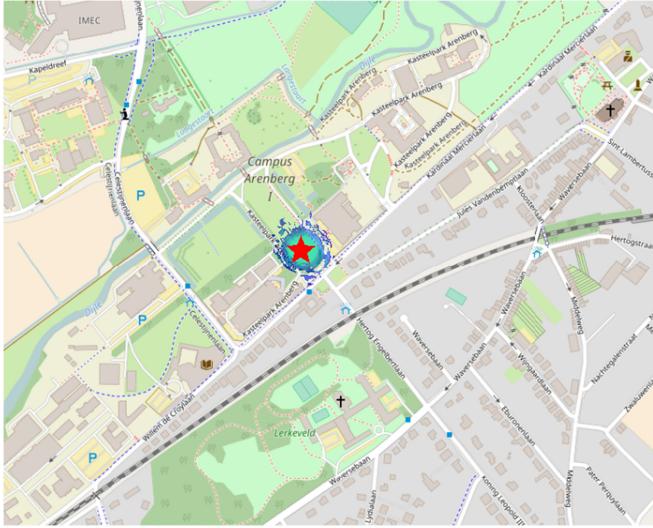


Fig. 2. Terrestrial receiver at 3 m altitude. The width of the map is 1182 m.

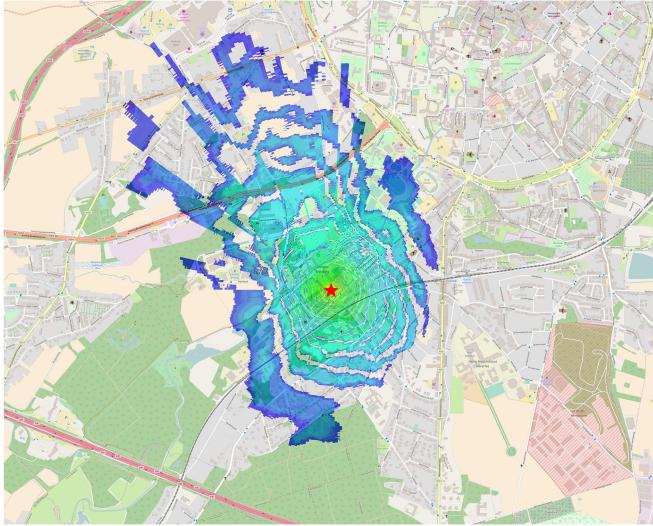


Fig. 3. UAV receiver at 50 m altitude. The width of the map is 4388 m.

ubiquitous, especially since the user of the jammer may not be aware of the problem (“It only works for a couple of meters, how can this possibly harm something?!”).

For completeness, a jammer that would create a signal that a GPS receiver can decode is studied. As such, it would enjoy the full processing gain, resulting in a significantly increased range. In this specific simulation we saw ranges from 25 to 40 km, as shown in Fig. 5.

### III. COUNTERMEASURE BASED ON REUSING COMMUNICATION HARDWARE FOR TRACKING THE BEARING TO THE GROUND STATION

Since we are focusing on civilian UAVs, there is no need to provide a solution that results in full performance when operating in a GPS-denied environment. It is expected that GPS jamming instances will stay relatively rare, allowing a safe mission abort and return to home to be acceptable. Also, we will

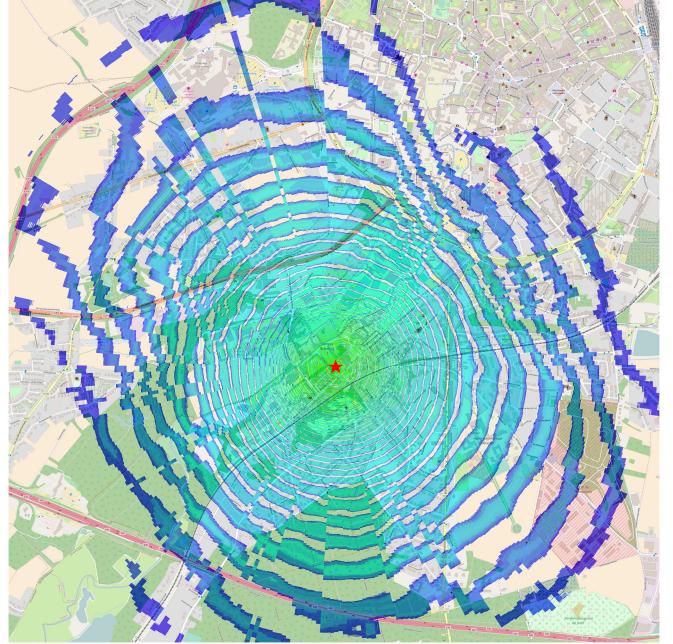


Fig. 4. UAV receiver at 250 m altitude. The width of the map is 4388 m.

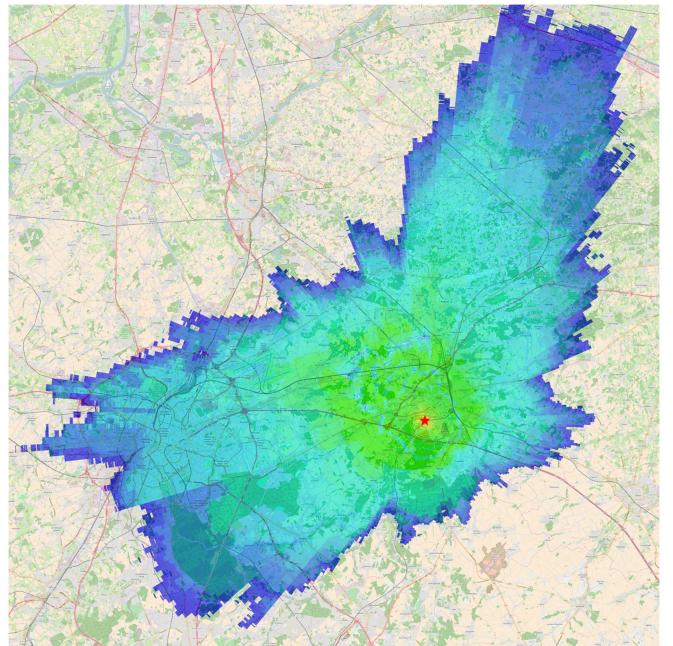


Fig. 5. UAV receiver at 250 m altitude attacked by a coherent jammer. The width of the map is 54 500 m.

only attempt to mitigate jamming effects that are collateral damage. As such, it is assumed that the UAV itself is not the intended target of the jamming, but merely within the range of a jammer.

Established countermeasures exist that will attempt to restore GPS reception in the presence of one or more jammers. A common solution [33] that can be employed regardless of the jamming waveform uses an antenna array to continuously create nulls in the direction of the interference sources. Since multiple antennas are required, this can result in unacceptably

high system dimensions and cost. In addition, on a mobile system the directions of these nulls need to be dynamically adapted based on the orientation of the platform with respect to the jamming sources. Null steering is not the only solution to recover GNSS reception in the presence of interference. When the waveform produced by the interference source does not match the spectrum of the GNSS signal, it is often possible to filter it out in the digital domain [4], [5]. Jammers utilizing a continuous or swept carrier wave can be removed from the baseband signal using a digital notch filter. Unfortunately, since the interfering signals can be, and often are, orders of magnitude stronger than the desired signal, this requires a receiver front end with a high dynamic range. Many low-end GNSS receivers use an analog to digital converter (ADC) with only 1 or 2 bits [13], [22], which makes it impossible to perform this kind of filtering. A method not requiring a high dynamic range front end would be to use a very narrow bandpass filter centered on the GPS L1 frequency. It is known that many tested commercial jammers use much wider sweep than necessary [23]. This likely means they use a cheap design with limited control on the output signal. A broad sweep is then required to guarantee the device will work despite inter-unit variations. A narrow bandpass filter might thus filter out a significant amount of the jamming energy, turning the continuous source into a pulsed source. A digital circuit can then disable correlator updates in the receiver during the jamming pulse to avoid performance degradation. Finally, since most civil GNSS signals are not authenticated, it is possible to transmit an entirely fake signal that is not just designed to cause interference but will instead be correctly decoded into a bogus position. If this attack is carried out successfully, it will not be possible to maintain the lock on the real satellite signals when only a single receiver antenna is used [12]. An additional difficulty may be that some types of countermeasures to make GNSS receivers more robust to interference are a controlled technology in many countries, leading to increased costs and time to market delays due to red tape.

In this section we present a method to offer a return-to-home functionality while relying on the communication technology already deployed on the UAV. As a result, there is no need for additional, expensive, hardware GPS countermeasures. The return-to-home functionality will enable the UAV to return to the ground station, if that ground station is transmitting return-to-home packets that can be used by the UAV to track the location of the ground station and fly toward the operator. Once the returned drone is within the visual range of the operator, it can be landed manually. To facilitate integration into commercial UAVs, it is very important that the system is cost effective. Therefore, we will try to use other systems already present in most UAVs to implement the countermeasure.

It should be noted that this system can also be used together with a hardened GNSS receiver to further improve the system resilience.

#### A. Direction of Arrival Methods

Almost all UAVs already have a radio for communication with one or more ground stations. It is assumed that the proba-

bility of simultaneous jamming of the command and control link and the GPS receiver is very unlikely unless done deliberately. Therefore, we propose to outfit the command and control radio with an angle-of-arrival detector. This will allow the UAV to know the bearing to the ground station. Many methods have been proposed in the literature for direction-of-arrival estimation of radio signals as we will discuss in this section.

*1) Physical Directional Antenna Array:* There are systems that employ an array of, typically four to six, directional antennas [15]. The device then measures and compares the power received by each antenna to estimate the direction of arrival. The main advantage is that the system only needs to measure signal strength. This measurement is available in almost all off-the-shelf radio chips since it is needed to be able to implement carrier sense multiple access and listen before talk. This method has significant disadvantages. For example, the accuracy is limited by the number of antennas. According to [15], a system with six antennas can determine the direction of arrival with an error of around 5°. This will likely lead to a high monetary cost.

Finally, it is likely that such a system is way too big for most consumer UAVs, especially since using small antennas close together may give rise to pattern distortion due to mutual coupling [6]. Some of these issues can be resolved by making use of a beamformed array [16].

*2) Rotating Antenna Systems:* In order to combat the drawbacks of the directional antenna array based systems, researchers have proposed using a single directional antenna that is installed on a rotor. This rotor allows physical pointing of the antenna or photodetector. By measuring the received signal strength, it is possible to estimate the direction of arrival [11], [21]. This mechanical setup is too complex and heavy for most UAVs.

The directionality of antennas is limited, which leads to poor accuracy since several degrees of error may lead to only a small difference in signal strength. Therefore, some systems use the null of the antenna, since this is almost always much more narrow [20].

Other researchers have extended this system using a rotor installed in the anchor nodes. The directional antenna is rotating at a fixed speed while transmitting. The zero bearing can then be obtained by solving the system of equations, or a signal can be transmitted by an omnidirectional antenna when the antenna is pointing to a reference bearing [32]. The UAV wishing to obtain the bearing would listen to this omnidirectional beacon. It would then measure the time delay between the beacon and the moment where maximum signal is received from the directional antenna. The measured time is proportional to the direction of arrival.

Of course, although only a single directional antenna is required this system also has significant drawbacks. The most important ones are the bulkiness and cost of the rotor system. This system is likely too unwieldy for most ground-station deployments. Like the previous systems, one only needs to measure the received signal strength.

A related system is used in full-size aircraft navigation. So-called very high frequency (VHF) omnidirectional range (VOR) beacons emit a related waveform with added direction to phase

encoding to facilitate easy angle recovery. VOR beacons use an electrically steered array instead of a mechanically scanned rotor.

3) *Electronically Steered Array*: Several systems implement an antenna of which the pattern can be changed dynamically. This can be done by using tunable parasitic elements [25], [31] or with an explicit switchable beamforming network [8]. The processing is the same as described in the previous two subsections.

4) *Doppler Direction Finding*: An antenna that rotates around a fixed point would see a signal with varying frequency due to the Doppler effect. The frequency would increase when the antenna is moving towards the source and decrease when it is moving away. The frequency would be equal to the frequency of the source when it is moving perpendicular to the propagation vector. This method can be used to obtain the direction of arrival [3].

It is more practical to use a virtual rotating antenna [26], since the angular velocities need to be very high to get a useful Doppler frequency. This moving antenna is emulated using a circular array of typically four omnidirectional antennas. These antennas are switched in a rapid fashion. The resulting signal is then FM demodulated. The phase offset between the rotation and the demodulated signal corresponds to the direction of arrival.

The main advantage of this method is that it is very simple to implement in systems that already use FM or frequency-shift keying (FSK) modulation since the required signals will be available in the receiver at no extra cost.

5) *Baseband Beamforming*: It is possible to estimate the direction of arrival from the downconverted signals using certain signal-processing algorithms. This is because when a wave hits an array of antennas, the signal will arrive earlier or later at each of the elements, depending on the angle of incidence.

Exploiting this requires that the raw signal can be captured from each antenna, often using complex and expensive software-defined radio setups.

In general, we can describe the signal received at the individual elements by the steering vector  $e$  as follows:

$$e = [a_0 \quad a_1 e^{j\theta_1} \quad a_2 e^{j\theta_2} \quad \dots \quad a_n e^{j\theta_n}] . \quad (2)$$

Should all antenna elements be deployed uniformly on a single axis, we can derive the ideal steering vector for this combination when exposed to a planar wave. Fig. 6 shows a diagram of a plane wave hitting two antenna elements. The ideal phase difference seen between the different elements is given by

$$\begin{aligned} \lambda &= \frac{c}{f}, \\ \theta &= 2\pi \frac{d \cdot \sin \alpha}{\lambda} \end{aligned}$$

where  $c$  is the speed of light,  $f$  is the frequency,  $d$  is the distance between the elements, and  $\alpha$  is the angle of incidence. Should this array be extended with more elements, also uniformly spaced by  $d$ , these elements would experience a multiple of  $\theta$ . Thus, extending this formula to an array with  $n$  elements

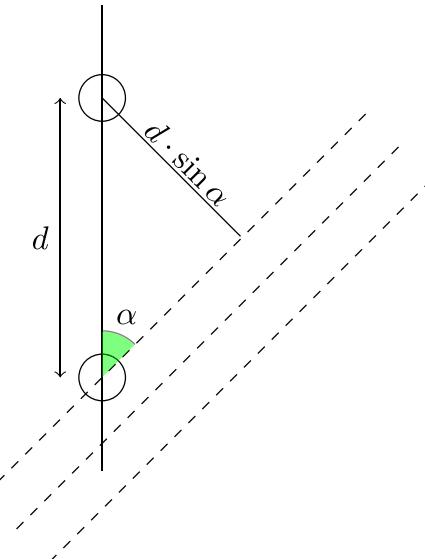


Fig. 6. Uniform linear array with two elements. The circles indicate antenna elements and the dashed lines represent the incident electromagnetic field.

yields

$$\theta_n = 2\pi \frac{(n \cdot d) \cdot \sin \alpha}{\lambda} = n \cdot \theta.$$

This allows us to rewrite (2) for this specific case as

$$e = [1 \quad e^{j\theta} \quad e^{j2\theta} \quad \dots \quad e^{jn\theta}] \quad (3)$$

where all  $a_i$  have been set to one since there is no difference in amplitude. This is allowed since we assume that the antenna spacing is very small compared to the target distance.

After measuring the value of  $\theta$ , the angle of arrival  $\alpha$  can be calculated as follows:

$$\alpha = \arcsin \frac{\theta \lambda}{2\pi d}.$$

We will present a miniaturized system implementing this method in a way that adds no or very little hardware cost. Most UAV control radios already use several antennas for diversity reception [29]. Usually, this is a simple switched diversity. Two or three antennas are connected to a single receiver based on the signal power measured during the preamble. We add a circuit that can measure the phase of the incoming signal. By measuring the amplitude and phase it is possible to calculate the direction of arrival.

#### IV. IMPLEMENTATION OVERVIEW

In this section, an overview will be given with respect to the software and hardware implementation of the system.

##### A. Hardware

In this paper, we present a custom wireless platform developed for this application on which the implementation has been done. An STMicroelectronics STM32F405 (high-performance) or STM32F401 (low-power) microcontroller is combined with an Atmel AT86RF233 IEEE 802.15.4 compatible radio.

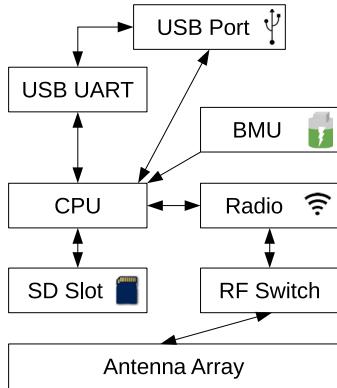


Fig. 7. Developed wireless system.

To facilitate long range applications, the system supports a 100-mW power amplifier. Fig. 7 shows a picture of the wireless system. The radio is connected, through a series of RF switches, to three antenna ports. This makes it possible to implement the direction-of-arrival-based GNSS interference countermeasure explained in this paper. This radio can compare the phase of the incoming signal to an internal reference, making it valuable for distance measurements [14]. Functionality is provided that allows easy programming and debugging of the microcontroller software over USB, negating the need for external programming dongles. For battery-powered use, power management functionality for a rechargeable lithium polymer battery and an SD card for datalogging are present. Finally, a USB universal asynchronous receiver/transmitter is provided for legacy applications that don't support a direct USB connection. A block diagram is shown in Fig. 8.

Two expansion connectors are provided for connecting external modules. This has been used, for example, for connecting a LoRa radio and an acoustic sensing system.

#### B. Time-Slotted Channel Hopping (TSCH) for Direction-Finding Protocol

A special protocol and software package was developed specifically focused on UAV command and control. On a high level, this software stack takes pulse-position modulation (PPM) commands from the remote control and transmits these wirelessly. The receiver module in the UAV will then convert the radio signals into PPM and pulsedwidth modulation signals that are delivered to the flight controller installed in the drone. Furthermore, it is possible to use a second channel, as required for many flight controllers, that is used for high-level remote control, typically using the micro air vehicle link (MAVLink) protocol.

To reduce the risk of interference to the command and control (C&C) link, a frequency-hopping scheme is employed. This is loosely based on 802.15.4e TSCH, although the hopping sequence is generated dynamically using a seekable cipher, advanced encryption standard (AES)-128 in counter mode. This makes it impossible to predict the frequency that will be used next unless the key is known, thereby making it significantly more difficult to jam the radio. The attacker would need to resort to barrage jamming, which has a very low power efficiency.



Fig. 8. Block diagram of the wireless system.

Alternatively, he would need to use a fast receiver to detect the signal before the timeslot ends, which is complicated and assumed to not be readily available to the general public. To prevent spoofing, the packets themselves are encrypted and authenticated using the standard AES-galois counter mode (GCM) mode.

An important feature is precise time synchronization between the nodes taking part in the network. This is done using hardware timers inside the CPU for reception and transmission timing. Each packet contains the timestamp at which it should have been sent (slot and frame number). The receiver then compares its local clock with the arrival timestamp. After subtracting the processing delay a clock error measurement is obtained. This measurement is used with a proportional/integral clock discipline algorithm, making it possible to synchronize the different parties to within 1–2  $\mu$ s. Lower synchronization variance allows smaller inter-packet dead times, increasing system efficiency.

While the dead-time gain on normal packets is not very huge, taking up to 1 ms at 2 mb/s, other parts of the protocol can greatly benefit. For example, because not only the absolute offset is corrected, but also the frequency error (clock drift), both nodes can maintain the hopping sequence for a significant time without being in contact. This allows quick recovery after link loss since no partner search procedure is required. Should the system be extended to ranging, this synchronization is also required to reduce turnaround dead time [28].

As said before, the main contribution of this paper is the development of a direction-of-arrival module that allows peers in the radio network to know their relative bearing. This has been implemented using phase and amplitude measurements obtained from an antenna array. It should be noted that most UAVs are already equipped with two or more antennas for diversity reception. During the control stream, some timeslots are reserved for this measurement. During this slot, the originator transmits a continuous wave signal. The observing nodes measure the phase and amplitude of the received signal in quick succession for all antennas. This measurement is repeated over multiple channels to reduce the effect of multipath propagation. Currently, the channels are measured sequentially, but this is no requirement.

Although we exploit specific functionality present in this radio chip for measuring the phase of the incoming signal, the method can be adapted to other receiver designs with minimum effort and low cost. An off-the-shelf RF to baseband chip can be

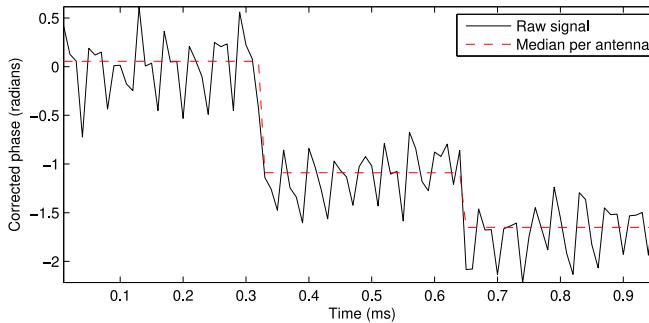


Fig. 9. Raw data received by the system. The contribution from the different antennas is clear.

used. During the measurement phase, the host microcontroller will sample the I and Q lines in order to collect the data. Most microcontrollers cannot sample two signals simultaneously, but since we are using an unmodulated carrier this is not required. Should no ADC be available, it is possible to measure the time difference between the zero crossings of the I and/or Q channel against an internal clock. In this way the relative phase can be measured. Most commercial UAV command and control radios work in three unlicensed bands: 433 MHz, 868/915 MHz, and 2.45 GHz. We present an example of a front-end IC that can be used to implement this solution for each band.

- 1) 433 MHz: Semtech SX1255: This chip features a digital baseband output that can be used with most microcontrollers. It has an integrated decimator and filter, reducing the amount of data to process.
- 2) 868/915 MHz: Semtech SX1257: The baseband output is already digital.
- 3) 2.45 GHz: Maxim MAX2831: A transceiver intended for wireless local area network (WLAN) applications. It has analog baseband outputs.
- 4) Licensed (high): Analog Devices ADRF6820: This chip covers 695–2700 MHz, which covers most licensed bands where long range UAV operations could take place. The baseband outputs are analog.
- 5) Licensed (low): Analog Devices ADRF6850: This chip covers 100 MHz to 1 GHz. This covers UHF and VHF applications. The baseband outputs are analog.

Fig. 9 shows the raw data as it is received by our system. The sample rate of the amplitude and phase component is  $10 \mu\text{s}$ . It can be seen that there is a continuous phase change caused by carrier-frequency offset. This is normally not a problem for angle-of-arrival processing, since most algorithms do not depend on specific signal parameters. However, since in our system the antennas are sampled sequentially the frequency offset has to be taken into account.

This can be compensated as long as the phase does not jump more than  $\pi$  radians per sample. The maximum allowed crystal offset can be calculated as follows. First, we calculate the maximum tolerated RF frequency offset

$$\Delta\theta = \pi$$

$$f_{\text{diff}} = \frac{\Delta\theta}{2\pi t_s} = \frac{1}{2t_s}.$$

In our case:  $t_s = 50 \text{ kHz}$ . Since the inaccuracy of the RF carrier is controlled by the offset of the PLL reference clock, it is required to calculate the relative offset

$$\Delta i = \frac{f_{\text{diff}}}{f_{\text{RF}}}.$$

In our case:  $\Delta i = 20.4$  pulse per minute (ppm). Since the system should be able to handle a worst case error on both sides, each crystal may at most contribute half this value: 10 ppm.

### C. Signal Processing

A digital beamforming method is used. In this section, we will look at three possible ways for processing the signals received by the antenna array. Foremost, all methods are frequency-domain beamforming algorithms. Therefore, a covariance matrix  $R$  is calculated from the observations made by the sensors, the row vector  $x$ , as follows:

$$R = E[(x - E[x])(x - E[x])^T].$$

Since the measurements represent a rotating vector in time, the expected value of each element of  $x$  ( $E[x_i]$ ) is zero. Thus, we can simplify the equation to

$$R = E[xx^T].$$

Finally, columnwise concatenating multiple measurement vectors  $x_i$  together into a matrix  $X$  allows  $R$  to be calculated as follows:

$$R = \frac{XX^T}{n}$$

where  $n$  is equal to the number of measurements. This scaling factor can be omitted when applying the algorithms described next, yielding

$$R' = XX^T.$$

Using this correlation matrix three different beamforming algorithms can be applied. The first one is the very well-known conventional beamformer, an extension of Fourier-based spectral analysis [2], which is obtained from the following formula:

$$p(\theta) = e^H R e$$

where  $p(\theta)$  is the power measured by the beamformer.

The disadvantage is the low resolution of the estimated direction of arrival. To increase the resolution, it is possible to use the Capon beamformer [7], which requires a matrix inversion. In the three-antenna case, the resulting covariance matrix is only three by three elements, making this computationally feasible, even on a weak-embedded processor. The formula for calculating this beamformer is as follows:

$$p(\theta) = \frac{1}{e^H R^{-1} e}.$$

Finally, to significantly increase the resolution, it is possible to employ the multiple signal classification (MUSIC) beamformer [30]. This algorithm performs an eigenvalue decomposition on the covariance matrix

$$R = USU^{-1}.$$

Note that due to  $R$  being symmetrical,  $U^{-1}$  can be replaced by  $U^H$ . The decomposition can then be split into two parts, one for the signal and one for the noise. This is done by classifying the  $n$  largest eigenvalues as being part of the signal ( $U_s$ ). To apply this algorithm, it is required to know how many signals will be present in the input signal. This can be estimated using statistical methods [1], but in this application we know that the number of signals will be one since there is only a single transmitter. The remaining eigenvalues and eigenvectors are considered to be part of the noise ( $U_n$ ).

The MUSIC algorithm then uses the noise eigenvectors  $U_n$  and  $U_n^H$  in the Capon beamformer

$$p(\theta) = \frac{1}{e^H U_n U_n^H e}.$$

The main advantage of this method is the very high resolution, but it is more computationally intensive. Thanks to its high resolution, it can handle multiple closely spaced (uncorrelated!) signals, although that capability is not used here.

#### D. UAV Control

The output of the system described in this section is a bearing to the ground-control station. To implement a practical return to home solution, it is required to couple this system to the flight controller installed in the UAV. Deep inside, many flight controllers is a basic software algorithm to orient the UAV to a certain heading, as this is frequently the output of higher level navigation controllers. Thus, here would be the ideal point to feed our own target bearing. This could be done for example by setting the flight controller to the right mode and feeding the bearing via the MAVLink protocol.

## V. MEASUREMENTS AND RESULTS

To evaluate the performance of the system, several measurements have been performed. The following three measurements were performed in realistic environments.

- 1) *Anechoic Chamber:* This is a room where RF absorbers are attached to the walls. This significantly reduces the reflections (“echos”) from the environment. As such, it is a simulation of a UAV at a high altitude far away from buildings. A picture of the setup is shown in Fig. 10. The calibration measurement has also been performed here.
- 2) *Outdoors Position 1:* This measurement was performed freestanding on a roof of an industrial type building. It represents a UAV that is flying over buildings. A picture is shown in Fig. 11.
- 3) *Outdoors Position 2:* This measurement uses the same roof as position 1, but is close to a wall of the building. It attempts to simulate a UAV flying near buildings.

Finally, for completeness, we have also performed a measurement indoors. This was done in a cafeteria/meeting room with many objects and obstructions, resulting in significant multipath.

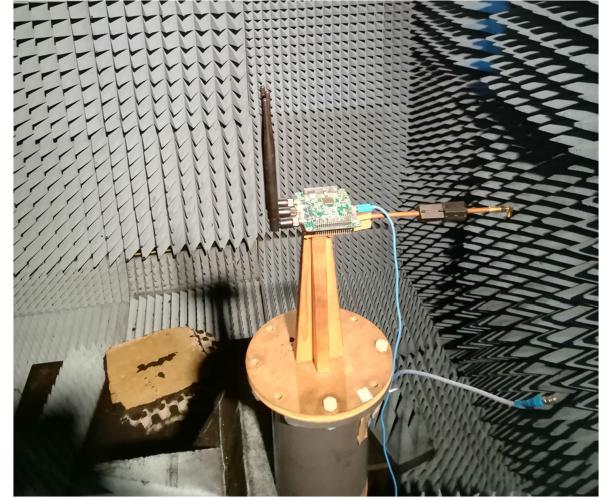


Fig. 10. Measurement in anechoic chamber.



Fig. 11. Roof-measurement setup (position 1).

#### A. System Calibration

It is important to relate the phases obtained from the steering vector to a good estimate of the direction of arrival. This can be done by measuring the value of  $e$  for a transmitter at a known angle to the receiver array. A phase offset will be obtained for each antenna that can be used to calibrate the system. However, an array of closely spaced omnidirectional antennas will exhibit a significant directionally sensitive mutual coupling. Note that this measurement was performed in the anechoic chamber to rule out multipath effects. Therefore, it is required to perform a calibration for different angles. The results presented are obtained using a calibration every  $9^\circ$ , although a measurement was made every  $3^\circ$  to increase the resolution of the figures.

Please note that no recalibrations have been performed after the initial calibration. All measurements use the same set of calibration coefficients collected in the anechoic chamber. This reduces accuracy since multipath errors are not taken into account in the steering vector, but this scenario is realistic in case the receiver is moving. After all, in practical applications there

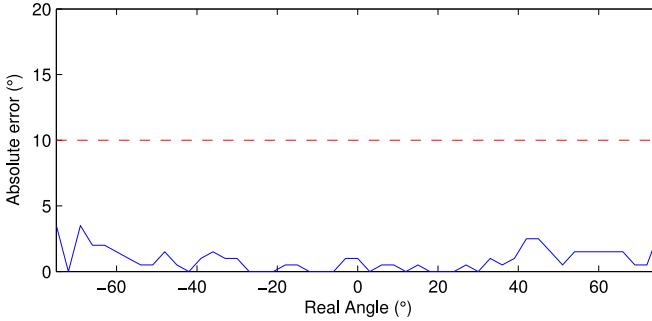


Fig. 12. Estimation error after performing the measurement in the same location the calibration was done. The system was restarted and there were several hours between both measurements. As expected, the error is very small.

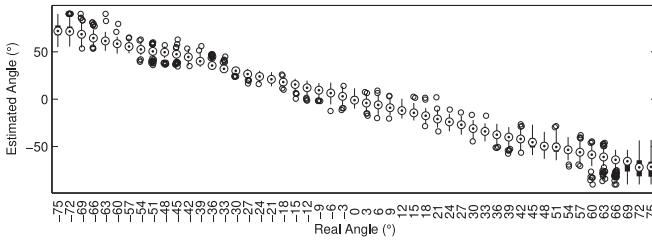


Fig. 13. Boxplot analysis for the verification measurement. It is clear the variance of the measurements at different frequencies is low. In most bins, the variance is so low that the boxplot is invisible. This is expected since the environment has little multipath.

would be no way to perform a calibration on the spot before measuring the bearing.

To show the repeatability of the calibration, two measurements were performed in the same position with several hours in between. The calibration measurement used 9° steps. The steering vector was interpolated using a smoothing spline. The accuracy of the verification measurement is shown in Fig. 12. As seen, the error is well below 5° on most points. In a practical product, it may be undesired to perform this type of calibration in an anechoic room. Fortunately, the UAV will have GPS coverage most of the time. As such, it is possible to perform the measurement online and store the resulting steering vector together with the calculated bearing. This is basically how our calibration was performed, although all measurements were done sequentially one after another.

To combat multipath, the estimation is repeated over different frequencies in the ISM band (2405–2480 MHz, 500 kHz spacing) and then median filtered. Fig. 13 shows a series of boxplots. The height of the box and the number of outliers is an indicator of the amount of multipath propagation present in the environment.

The small circle in the center of the black bar indicates the median of the estimated direction of arrival over all frequency bins. The thick black bar indicates the interquartile distance. The thin black whiskers indicate the minimum and maximum of the data with outliers removed. Finally, the small circles are points discarded as outliers. Outliers are selected based on a scaled median absolute deviation (MAD) method. The scaling

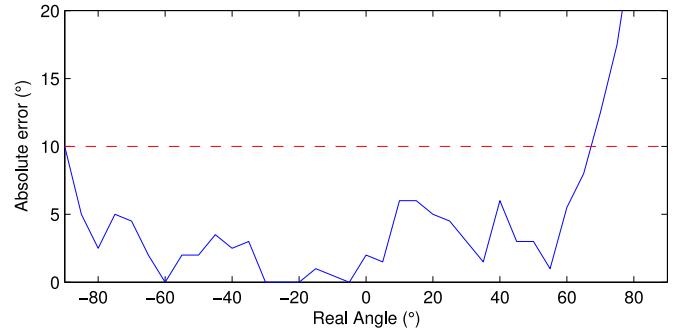


Fig. 14. Measurement accuracy in the outdoor case (position 1). The error is well below 10°, except when the angle-of-arrival is coming close to 90°.

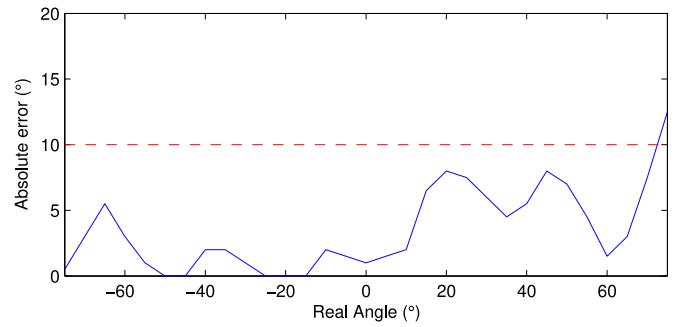


Fig. 15. Measurement accuracy in the outdoor case (position 2). The error is well below 10°.

factor used is 0.6745 and a point is considered an outlier when it is more than 3 scaled MAD away from the median.

### B. Measurement Results

In this section, a representative sample of results is reported. The MUSIC algorithm has been employed using the full calibration. First, we will examine the measurements performed during the different outdoor measurements. Figs. 14 and 15 show the accuracy of the measurements. Note that a manual positioner was used and, thus, small pointing inaccuracies cannot be avoided. A significant pointing error occurred in the second measurement, which has been corrected in post processing.

It can be seen that in both cases the error stays well below 10°, which is more than enough to fly back to the base station using the bearing obtained from the sensor system. In addition, many measurements will be taken during the return to home maneuver. This reduces the impact of errors on individual measurements as long as they are not systematic. The error increases when we get close to 90°; a solution is provided in Section VI. As we can see from the boxplots shown in Figs. 16 and 17, there is significantly more multipath in this outdoor environment than in the anechoic chamber.

Finally, we examine the results that are obtained in the indoor environment. This environment is included as a worst-case result and is not typical for a UAV that would be using this system since there is no indoor GPS coverage anyway. Although the

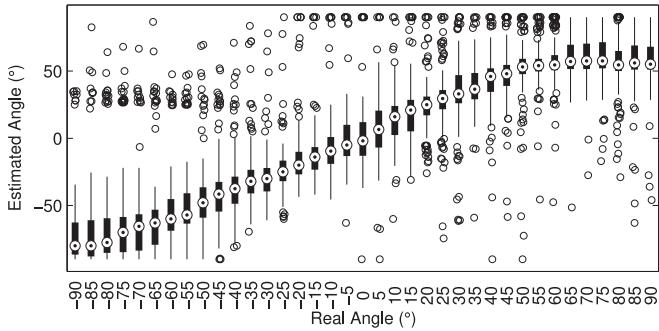


Fig. 16. Boxplot analysis of the outdoor measurement (position 1). It is clear that although there is significantly more multipath visible, the results are still good.

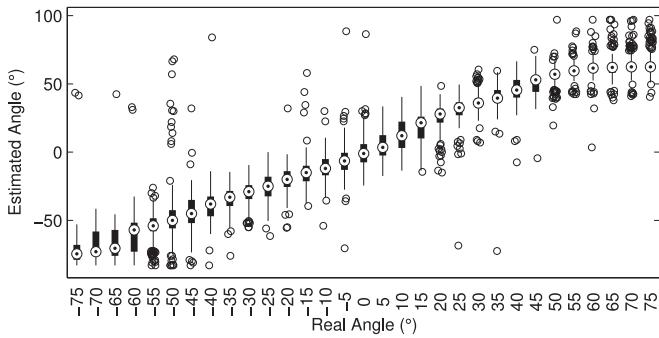


Fig. 17. Boxplot analysis of the outdoor measurement (position 2).

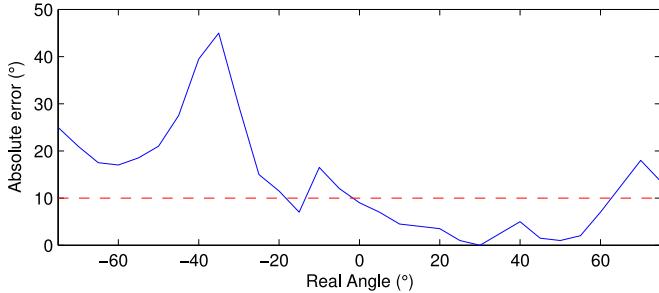


Fig. 18. Results in the cafeteria. This is an environment with many large metallic reflectors and scatterers.

error shown in Fig. 18 is significant in some angles, there is still a strong correlation between the direction of arrival and the measured value. A navigation system could still determine whether to go left or right based on this measurement, which may be sufficient to ultimately return to base. Finally, Fig. 19 confirms the existence of severe multipath effects when using the system in an indoor environment. However, in outdoor high-altitude situations, we can rely on line-of-sight performance. It is expected that similar results would be encountered in densely cluttered areas such as urban canyons, indicating that the system is unlikely to operate well in such cases. In any case, a simple bearing is not enough in this environment to return to the ground-control station, since obstructions are likely to be in the path between the UAV and the source. Other methods such as computer vision will be required.

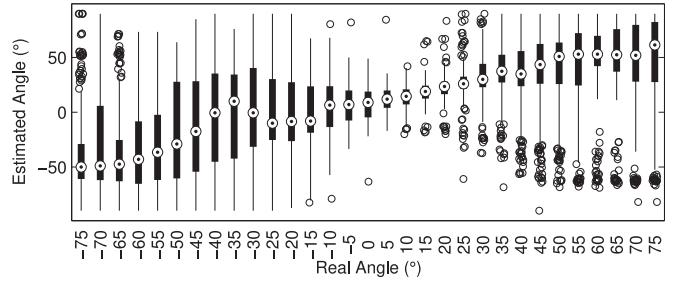


Fig. 19. Boxplot analysis for the cafeteria measurement. Clearly, the measurement quality is lower, although a simple left/right bearing can still be obtained in most cases.

Unfortunately, due to strict regulations regarding UAV usage in Belgium it was not feasible to carry out actual end-to-end flight testing in the context of this paper. However, we feel that the ground-testing performance will lead to worse results than what would be obtained on an airborne platform since the ground environment will have a rich scattering context. It is expected that an airborne terminal will experience less multipath which will result in a more accurate angle-of-arrival estimate.

## VI. AMBIGUITY RESOLUTION

As shown before, all measurements have been performed using a uniform linear array with three antennas, although for planar direction-of-arrival measurements only two antennas are needed. This is required to mitigate a critical limitation of the previous setup. If all antennas are installed in one plane, it will be impossible to distinguish whether a signal is coming from the front or back of the array. This is clear from the formula

$$\theta = 2\pi \frac{d \cdot \sin \alpha}{\lambda}$$

which gives the phase  $\theta$  in function of the incidence angle  $\alpha$  since  $\sin \alpha = \sin(\pi - \alpha)$ .

This would make returning home purely on the obtained bearing impossible. However, using a third antenna, as shown in Fig. 20, makes it possible to directly resolve this ambiguity. One way to achieve this is by placing one antenna slightly forward in a triangular fashion.

The diagonal element can be seen as part of a new two-element linear array formed by itself and one of the previous elements. Intuitively, this will form another array with a different alias angle making it possible to resolve the front-to-back ambiguity.

Knowing the distance  $d_2$ , it is possible to calculate the angle  $\beta$  from  $\alpha$ . First,  $\gamma$  is obtained from  $d_2$  and  $d$  as follows:

$$\cos \gamma = \frac{d}{2d_2}.$$

Then,  $\eta$  is obtained from  $\alpha$  and  $\gamma$  as follows:

$$\eta = \frac{\pi}{2} + \alpha - \gamma$$

and knowing this,  $\beta$  is obtained as follows:

$$\beta = \frac{\pi}{2} - \eta = \frac{\pi}{2} - \left( \frac{\pi}{2} + \alpha - \gamma \right) = \gamma - \alpha.$$

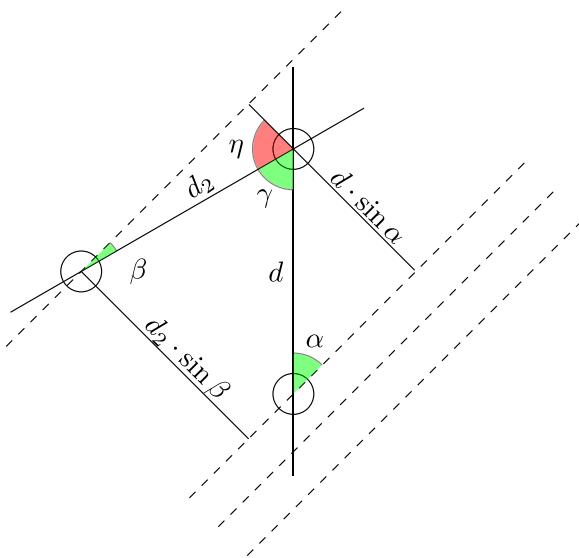


Fig. 20. Triangular array with three elements. The circles indicate antenna elements and the dashed lines represent the incident electromagnetic field.

Finally, the following equation is obtained:

$$\beta = \arccos \frac{d}{2d_2} - \alpha \quad (4)$$

which gives the steering vector for this arrangement as

$$\begin{aligned} \theta_1 &= 2\pi \frac{d \cdot \sin \alpha}{\lambda} \\ \theta_2 &= 2\pi \frac{d \cdot \sin \beta}{\lambda} \\ e &= [1 \quad e^{j\theta_1} \quad e^{j\theta_2}] \end{aligned} \quad (5)$$

It can be seen that since  $\alpha$  and  $\beta$  are offset from each other, the ambiguity introduced by  $\sin \alpha = \sin(\pi - \alpha)$  can be resolved with at least three antennas.

As an alternative, since the UAV is mobile, it may be possible to resolve this ambiguity by taking continuous measurements at different baseline angles while the system is moving.

## VII. ELEVATION

As said before, a measurement is only performed in the horizontal plane. In our opinion, this is sufficient for UAV return-to-home functionality, since the UAV is expected to be far away compared to its altitude. If this was not the case, the drone could simply be landed by the operator.

To make sure the  $\alpha = 0$  array calibration holds, the vertical direction of arrival should not be excessive. The vertical angle-of-arrival depends on the altitude of the UAV  $h_r$ , the transmitter  $h_t$ , and the distance  $d$  between them. The angle  $\alpha$  is then given by

$$\alpha = \arctan \left( \frac{h_t - h_r}{d} \right).$$

We can assume the UAV to be out of view from the operator when it is over 500 m away. If we want to keep the vertical angle below 15°, the maximum altitude difference ( $h_t - h_r$ ) can be

134 m which should be enough in almost all use cases. If vertical coverage is desired, one or more antennas could be placed such that they are not in the horizontal plane.

## VIII. CONCLUSION

In this paper, we have analyzed the risk GNSS jamming poses to civilian UAVs. It was shown to be a significant concern. To combat this, a system is proposed that makes it possible for the UAV to safely execute a return-to-home maneuver under the presence of GPS jamming. This system is based on novel reuse of the communication radio as an angle-of-arrival receiver. By employing this system, the UAV can continuously measure the bearing to the ground station. Furthermore, it was shown that reusing the frequency-domain diversity that is already present in most frequency-hopping UAV C&C radios significantly improves the accuracy of the system. The effectiveness was shown in a practical setting on the ground. Due to legal reasons, it was not possible to test the system in an actual UAV, something that should be done as future work.

## REFERENCES

- [1] H. Akaike, "Information theory and an extension of the maximum likelihood principle," in *Proc. of the 2nd International Symposium on Information Theory*, B. N. Petrov and F. Csaki, Eds. Budapest, Hungary: Akademiai Kiado, 1973, pp. 267–281.
- [2] M. S. Bartlett, "Smoothing periodograms from time series with continuous spectra," *Nature*, vol. 161, no. 4096, pp. 686–687, 1948.
- [3] J. M. Beukers, "Doppler direction finder," U.S. Patent 3 121 871, Jan. 4, 1966.
- [4] D. Borio, "A multi-state notch filter for GNSS jamming mitigation," in *Proc. Int. Conf. Localization GNSS*, Jun. 2014, pp. 1–6.
- [5] D. Borio, C. O'driscoll, and J. Fortuny, "Tracking and mitigating a jamming signal with an adaptive notch filter," Inside GNSS Media & Research LLC, Red Bank, NJ, USA. [Online]. Available: <http://insidengnss.com/auto/marapr14-WP.pdf>
- [6] A. Camps, F. Torres, J. Corbella, J. Bará, and P. De Paco, "Mutual coupling effects on antenna radiation pattern: An experimental study applied to interferometric radiometers," *Radio Sci.*, vol. 33, no. 6, pp. 1543–1552, 1998.
- [7] J. Capon, "High-resolution frequency-wavenumber spectrum analysis," *Proc. IEEE*, vol. 57, no. 8, pp. 1408–1418, Aug. 1969.
- [8] H. T. Chou and C. T. Yu, "Design of phased array antennas with beam switching capability in the near-field focus applications," *IET Microw. Antennas Propag.*, vol. 9, no. 11, pp. 1120–1127, 2015.
- [9] B. Van den Bergh, A. Chiumento, and S. Pollin, "LTE in the sky: Trading off propagation benefits with interference costs for aerial nodes," *IEEE Commun. Mag.*, vol. 54, no. 5, pp. 44–50, May 2016.
- [10] DJI. *Mavic Pro*. (Jun. 2017). [Online]. Available: <https://www.dji.com/mavic>
- [11] K. Von Ehr, S. Hilaski, B. E. Dunne, and J. Ward, "Software defined radio for direction-finding in UAV wildlife tracking," in *Proc. IEEE Int. Conf. Electro Inf. Technol.*, May 2016, pp. 464–469.
- [12] Z. Haider and S. Khalid, "Survey on effective GPS spoofing countermeasures," in *Proc. 6th Int. Conf. Innovative Comput. Technol.*, Aug. 2016, pp. 573–577.
- [13] Maxim Integrated. *MAX2769. Universal GPS Receiver*. (Feb. 2018) [Online]. Available: <https://www.maximintegrated.com/en/products/comms/wireless-rf/MAX2769.html>
- [14] Atmel Inc. *RTB Evaluation Application Software User's Guide*. (Feb. 2013). [Online]. Available: [http://www.atmel.com/Images/Atmel-8443-RTB-Evaluation-Application-Software-Users-Guide\\_Application-Note\\_AVR2152.pdf](http://www.atmel.com/Images/Atmel-8443-RTB-Evaluation-Application-Software-Users-Guide_Application-Note_AVR2152.pdf)
- [15] A. Joshua and P. Lee, "Sensor network localization via received signal strength measurements with directional antennas," in *Proc. Allerton Conf. Commun. Control Comput.*, pp. 1861–1870, Sep. 2004.
- [16] P. Kułakowski, J. Vales-Alonso, E. Egea-López, W. Ludwin, and J. García-Haro, "Angle-of-arrival localization based on antenna arrays for wireless

- sensor networks," *Comput. Elect. Eng.*, vol. 36, no. 6, pp. 1181–1186, 2010.
- [17] H. Lim, J. Park, D. Lee, and H. J. Kim, "Build your own quadrotor: Open-source projects on unmanned aerial vehicles," *IEEE Robot. Automat. Mag.*, vol. 19, no. 3, pp. 33–45, Sep. 2012.
- [18] Taoglas Limited. *4 mm Thick GPS/Galileo Patch Antenna*. (Apr. 2015). [Online]. Available: <http://www.taoglas.com/wp-content/uploads/2015/04/GP.1575.25.4.A.02.pdf>
- [19] Wolves Team Limited. 6 Antenna Mobile Phone GPS WiFi Jammer. (Jun. 2017). [Online]. Available: <http://www.jammermanufacturer.com/6-antenna-cell-phone-gps-wifi-jammer-remote-control-p-44.html>
- [20] M. Malajner, P. Planinsic, and D. Gleich, "Angle of arrival estimation using RSSI and omnidirectional rotatable antennas," *IEEE Sensors J.*, vol. 12, no. 6, pp. 1950–1957, Jun. 2012.
- [21] C. D. Mcgillem and T. S. Rappaport, "A beacon navigation method for autonomous vehicles," *IEEE Trans. Veh. Technol.*, vol. 38, no. 3, pp. 132–139, Aug. 1989.
- [22] STMicroelectronics. Automotive Fully Integrated RF Front-End Receiver for GPS Applications. (Feb. 2018). [Online]. Available: <http://www.st.com/en/automotive-infotainment-and-telematics/sta5620a.html>
- [23] R. H. Mitch *et al.*, "Signal characteristics of civil GPS jammers," in *Proc. 24th Int. Tech. Meeting Satell. Division Inst. Navigation*, Sep. 2011, pp. 1907–1919.
- [24] Radio Mobile. RF Propagation Simulation Software. (Jun. 2017). [Online]. Available: <http://radiomobile.pe1mew.nl/>
- [25] T. Ohira and K. Gyoda, "Hand-held microwave direction-of-arrival finder based on varactor-tuned analog aerial beamforming," in *Proc. Asia-Pacific Microw. Conf.*, Dec. 2001, vol. 2, pp. 585–588.
- [26] D. Peavey and T. Ogumfunmi, "The single channel interferometer using a pseudo-doppler direction finding system," in *Proc. IEEE Int. Conf. Acoust. Speech Signal Process.*, Apr. 1997, vol. 5, pp. 4129–4132.
- [27] C. Curry, "Sentinel Project: Report on GNSS Vulnerabilities," Chronos Technologies, Lydbrook, U.K., Feb. 2014. [Online]. Available: [http://www.chronos.co.uk/files/pdfs/gps/SENTINEL\\_Project\\_Report.pdf](http://www.chronos.co.uk/files/pdfs/gps/SENTINEL_Project_Report.pdf)
- [28] J. Rapinski and M. Smieja, "Zigbee ranging using phase shift measurements," *J. Navigat.*, vol. 68, no. 4, pp. 665–677, 2015.
- [29] FrSKY Electronic Co. Instruction Manual for FrSky D4R-II. (Feb. 2012). [Online]. Available: <http://www.frsky-rc.com/download/down.php?id=99>
- [30] R. Schmidt, "Multiple emitter location and signal parameter estimation," *IEEE Trans. Antennas Propag.*, vol. 34, no. 3, pp. 276–280, Mar. 1986.
- [31] C. Sun, A. Hirata, T. Ohira, and N. C. Karmakar, "Fast beamforming of electronically steerable parasitic array radiator antennas: theory and experiment," *IEEE Trans. Antennas Propag.*, vol. 52, no. 7, pp. 1819–1832, Jul. 2004.
- [32] A. V. Tondwalkar and P. Vinayakray-Jani, "Terrestrial localization by using angle of arrival measurements in wireless sensor network," in *Proc. Int. Conf. Comput. Intell. Commun. Netw.*, Dec. 2015, pp. 188–191.
- [33] M. D. Zoltowski and A. S. Gecan, "Advanced adaptive null steering concepts for GPS," in *Proc. IEEE Military Commun. Conf.*, vol. 3, Nov. 1995, pp. 1214–1218.

**Bertold Van den Bergh** received the Ph.D. degree from the Katholieke Universiteit Leuven, Leuven, Belgium, in 2017, as a member of the Networked Systems Group within TELEMIC.

His research interests include communication solutions for unmanned aerial vehicles and other systems with complex size, weight, power, and reliability requirements.

**Sofie Pollin** received the Ph.D. degree from the Katholieke Universiteit Leuven, (KU Leuven), Leuven, Belgium, in 2006.

From 2006 to 2008, she continued the research on wireless communication, energy-efficient networks, cross-layer design, coexistence, and cognitive radio with the University of California, Berkeley, CA, USA. In 2008, she returned to IMEC, where she was a Principal Scientist with the Green Radio Team. She is currently an Associate Professor with the Electrical Engineering Department, KU Leuven. Her research interests include networked systems that require networks which are ever denser, heterogeneous, battery powered, and spectrum constrained.