UNIVERSITÀ POLITECNICA DELLE MARCHE
Repository ISTITUZIONALE

Good Vibes: A PWM-Enabled Covert Channel for Securing UAVs Operations

This is the peer reviewd version of the followng article:

Original
Good Vibes: A PWM-Enabled Covert Channel for Securing UAVs Operations / Ciattaglia, G.; Bertocco, M.; Brighente, A.; Gambi, E.; Peruzzi, G.; Pozzebon, A.; Spinsante, S.. - ELETTRONICO. - (2025). (20th IEEE Sensors Applications Symposium, SAS 2025 Newcastle, United Kingdom 08-10 July 2025) [10.1109/SAS65169.2025.11105128].

Availability:
This version is available at: 11566/353952 since: 2026-03-08T10:04:05Z

Publisher:
Institute of Electrical and Electronics Engineers Inc.

Published
DOI:10.1109/SAS65169.2025.11105128

Terms of use:

The terms and conditions for the reuse of this version of the manuscript are specified in the publishing policy. The use of copyrighted works requires the consent of the rights' holder (author or publisher). Works made available under a Creative Commons license or a Publisher's custom-made license can be used according to the terms and conditions contained therein. See editor's website for further information and terms and conditions.
This item was downloaded from IRIS Università Politecnica delle Marche (https://iris.univpm.it). When citing, please refer to the published version.

Publisher copyright:

IEEE - Postprint/Author's Accepted Manuscript

©2025 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works. To access the final edited and published work see 10.1109/SAS65169.2025.11105128

(Article begins on next page)

23 April 2026

Good Vibes: a PWM-Enabled Covert Channel for Securing UAVs Operations

Gianluca Ciattaglia
Dept. of Information Engineering
Università Politecnica delle Marche
Ancona, Italy
g.ciattaglia@univpm.it

Matteo Bertocco
Dept. of Information Engineering
Università di Padova
Padova, Italy
matteo.bertocco@unipd.it

Alessandro Brighente
Department of Mathematics
Università di Padova
Padova, Italy
alessandro.brighente@unipd.it

Ennio Gambi
Dept. of Information Engineering
Università Politecnica delle Marche
Ancona, Italy
e.gambi@univpm.it

Giacomo Peruzzi
Dept. of Information Engineering
Università di Padova
Padova, Italy
giacomo.peruzzi@unipd.it

Alessandro Pozzebon
Dept. of Information Engineering
Università di Padova
Padova, Italy
alessandro.pozzebon@unipd.it

Susanna Spinsante
Dept. of Information Engineering
Università Politecnica delle Marche
Ancona, Italy
s.spinsante@univpm.it

***Abstract*—This paper proposes an innovative vibration-based communication system on a wireless medium for Unmanned Aerial Vehicles (UAVs), in which a covert channel is established by relying on the inherent characteristics of vibration signatures generated by the motors and propellers mounted on the UAV. Different vibration patterns, generated by purposely varying the Pulse Width Modulation (PWM) signals driving the UAV motors according to a predefined scheme, can be remotely detected by measurements performed with a radar sensor deployed at, for instance, a Critical Infrastructure (CI) to be safeguarded. The system analyses the vibrational patterns, via frequency and displacement measurements exploiting a Discrete Fourier Transform (DFT) approach, to decode information symbols on a constellation diagram. As a result, a localised channel is created. The latter is also inherently secure against attacks like jamming and spoofing, typical of traditional Radio Frequency (RF) communications. Experimental results validate the feasibility of the proposal, by identifying four encoded symbols that can be potentially exploited to set up a communication protocol.**

***Index Terms*—Vibration-Based Wireless Communication, UAVs, PWM, Radar Measurements, Secure Communication.**

I. INTRODUCTION

Vibrations coming from the motors and propellers of an Unmanned Aerial Vehicle (UAV), or the physical features of a particular model and make, produce unique vibrational patterns similar to fingerprints for the UAV at hand. This makes it particularly challenging for an adversary to impersonate, spoof, or replicate such a communication remotely, thus making this type of link intrinsically secure. Because it communicates through mechanical vibrations, rather than Radio Frequency (RF) media as it usually happens, this implicitly avoids common vulnerabilities related to RF (e.g., jamming, interception, etc.). Specifically, RF channels can be tampered over long distances, contrarily to vibrational signals that are highly localised in the surroundings of the drone. Indeed, the localisation of such signals makes interference from outsiders less of an issue, and guarantees that communication remains fully confined to the intended physical vicinity between the two end-points of the link. Such a feature can be used in high-security operations, or other sensitive applications like safeguarding a Critical Infrastructure (CI), as reliable backups or primary channels to enable communications when the RF spectrum is clogged with adversarial transmitters, or other insecure conditions. For instance, in so doing UAVs can authenticate themselves to ground stations belonging to a specific CI by means of a vibrational signature, ensuring that only a genuine, expected UAV is the one in control. At the same time, UAVs can wirelessly communicate towards the ground stations sensitive information by relying on an enhanced level of security. Albeit such an approach is promising, it also presents some challenges and drawbacks, that do not undermine its viability. Amid the most important ones is the intrinsic limited data-rate associated with such a type of communication, as well as the need for filtering techniques at the receiver side allowing to discard background ambient noise. Nonetheless, for all those applications requiring integrity and confidentiality of communications, exploiting a vibration-based channel represents a robust, reliable, and innovative solution complementing, or even overtaking, conventional RF techniques.

To this end, this paper aims at presenting a measurement methodology to remotely detect, by resorting to a radar sensor, vibration frequencies and amplitude displacements due to the rotation of the motors and propellers of a UAV. Specifically, the drone motors are controlled by modulating their driving Pulse Width Modulation (PWM) signal according to a predefined rule, which in turn modulates the associated vibrational pattern. This allows to exploit the resulting vibrational frequency and displacement values to identify symbols, properly arranged on a constellation diagram, to be exploited in a vibration-based communication scheme on a wireless medium. In particular, those symbols can be encoded starting from mean values and standard deviations of the vibrational frequency peaks associated with the aforementioned modulating PWM driving signals. This can potentially set up a Voronoi diagram, having frequency and displacement as axes, to map symbols on which ad-hoc communication protocols can be devised.

The rest of this paper is drawn up as follows. Section II presents related works dealing with the topic. Section III shows the system model, as well as the description of the covert channel. Section IV outlines the radar measurements setup. Section V introduces the experimental tests, while Section VI shows and discusses the relative results. Finally, Section VII concludes the paper.

II. RELATED WORKS

UAVs are strategic assets in many applications, from industrial to military ones, where they can support dedicated activities, especially the ones that a human operator cannot perform. In a military context, malicious drones are designed to satisfy special requirements like low detectability and high mileage. In a civil context, drones must always be recognizable, especially if moving around CIs. For this reason, similarly to civil aircraft, they can be equipped with Automatic Dependent System-Broadcast (ADS-B) systems to transmit UAV information [1]. Such a method can be ineffective if the drone does not want to be identified. For this reason, other methods are proposed to fulfil this task. Bounding the envisioned scenario to a smart city where drones are used to perform different operations, the simplest way to identify a drone is by a computer vision system [2]. Such systems are very powerful in identifying types of drones, but fail in some circumstances. For example, a camera-based system cannot properly work in the presence of smoke, dust, or fog. Also, it is ineffective in revealing malicious drones or tampered ones. An attacker can use a drone of the same type as the authorized one, fooling the identification system. Other approaches can exploit audio sensing systems, which are an efficient method if the drone wants to be identified [3]. The malicious drone can emit a sound to try to replicate an authorized one, thus bypassing the identification system. In [4], a radar based method is proposed to identify the drone: this work further demonstrates how radar is the best choice in the proposed scenario [5], [6]. There is a key aspect that is dependent on the physical features of the drone and is the vibration of its chassis. Such a phenomenon is measurable with a radar sensor [7], and, if obtained from a drone, it can unlock different possibilities. Indeed, it can be used to measure rotational speed of the propellers or to reveal the installed type [8], [9]. The main advantage of this type of measurement is the complexity of maliciously replicating the drone signature, since it is particularly difficult to obtain the same vibration signature by changing the components of the drone. Furthermore, provided that different rotation speeds imply chassis vibrations at different speeds, this can be used as a covert channel to exchange information between parties in a stealthy fashion. Leveraging this fact, in this work, the drone vibration is used as a covert channel to transmit information. Modulating the PWM signal based on a predefined rule, in fact, embeds desired components in the vibration signal, whose frequency and amplitude can be used to identify a transmitted symbol. Even if a malicious drone with similar characteristics tried to replicate the communication, it would not be able to mimic typical displacement and frequency values of the authorised drone. Furthermore, leveraging a covert channel creates out-of-band communications that an attacker is not aware of, thus increasing secrecy. Covert channels for authentication purposes are common in the cybersecurity literature, with relevant examples on Controlled Area Network (CAN) bus [10], Local Area Networks (LAN) [11], and air-gapped networks [12]. Implementations that leverage a vibrational covert channel are presented in [13], [14], but these cases are based on contact sensors. The approach proposed here leverages a radar sensor able to measure contactless target vibrations. This work aims at demonstrating the feasibility of this novel covert channel by means of preliminary experimental tests, thus filling the current gap present in the literature.

III. SYSTEM MODEL AND COVERT CHANNEL

We consider a CI where drones are deployed to deliver missions such as monitoring and surveillance. To gather reliable information and ensure that no malicious drone enters the CI area, we need a system able to identify drones to distinguish between legitimate and malicious ones. Hence, we assume that the CI is equipped with a staring radar system to detect and track drones [15]. However, detection and tracking do not aid the identification task, which aims at distinguishing legitimate and non-legitimate drones.

To provide the CI with identification capabilities, we propose a novel covert channel that a legitimate drone and the CI can use to exchange drone-specific authentication tags. We assume that those tags are known only by the CI and each legitimate drone and are provided to them during a bootstrap phase. To create the covert channel, we propose that drones encode their authentication tag in the PWM signal they use to drive their motors. This causes their chassis to vibrate at different frequencies, and we propose to associate a specific modulation symbol to each possible frequency. By leveraging the radar system, the CI estimates these frequencies and demodulates them according to our proposed scheme. Malicious drones invading the CI are not aware of this covert channel and do not have a valid authentication tag, they can hence be identified by the CI.

IV. RADAR METHOD AND MEASUREMENT SETUP

In this Section, the radar sensing method used to extract the vibration containing the communication symbol is described. The Section also contains the description of the equipment used to prove the feasibility of the proposed approach.

A. *Radar Sensing System*

Radar technology has been pushed further in recent years, and compact radar sensors are nowadays available at a reasonable cost and form factor. Such an availability has raised novel unconventional applications opening new sensing possibilities. One of them is contactless vibration measurement. Radars' attitude in measuring vibrations is documented and demonstrated in literature [16], [17]. Independently from the radar modulation scheme, the vibration of a target can be quantified leveraging interferometry method that provides displacement measure. The core idea behind the displacement measurement method is revealing the target micro-motions, demodulating the so-called micro-Doppler effect. Such an effect is a superimposed modulation on the reflected signal enabling the measurement. Albeit multiple radar technologies can be used to measure the target's vibration, due to their commercial availability and high integration grade, a Frequency Modulated Continuous Wave (FMCW) radar is chosen in this work. In particular, the radar board used in this work is commercially available and developed by Texas Instruments for Advanced Driver Assisted System (ADAS) applications.

Despite the board was designed to target a different application, it is perfectly suited for the purposes of this work, mainly thanks to the wavelength of the transmitted signal. Generally, ADAS developed radars use two different bandwidths, 76 GHz to 77 GHz and 77 GHz to 81 GHz, for automotive long range and short range applications, respectively. The latter is exploited in this work as better suited for vibration measurement purposes. The waveform transmitted by FMCW radars is a linearly modulated chirp (see Fig. 1).

Referring to Fig. 1, the black solid line is the transmitted signal s_t, the dashed grey line is the received signal s_r, the t_c interval is the s_t transmitting time, Δ_t is the interval between the transmitting start instant and the instant at which the ADC starts to sample the beat signal. The parameters f_{start} and f_{stop} represent the start and the stop frequencies of the chirp, respectively. Their difference provides the bandwidth indicated with B.

The chosen radar board has the peculiarity of being configurable, and this makes it possible to customize the transmitted waveform to be suited for the vibration measurement. The selected radar configuration must fulfil two requirements: allowing effective target detection, and providing satisfactory extraction of the vibration signal.

Target detection is performed by processing the beat signal (s_b), obtained from the multiplication of s_t and s_r. Information about the target distance and its velocity can be obtained from this intermediate frequency signal. The most salient parameters that influence the range and velocity quantification are the sampling frequency f_s of the beat signal, the chirp slope S, and the Pulse Repetition Interval (PRI). The latter parameter will influence the sampling time of the measured target vibration. In [9] it is demonstrated how the method developed in [7] can be applied to the drone context. The vibration measured by the radar can be used for authentication purposes, like installed propeller identification, or drone tampering. To obtain a good vibration measure with FMCW radars, the PRI must be set accordingly to the vibration bandwidth.

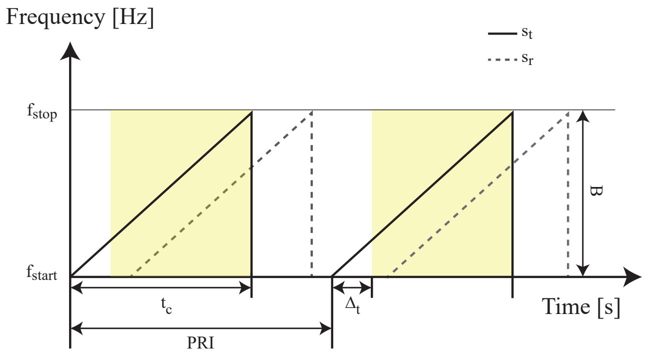


Fig. 1: FMCW radar transmitted waveform. The yellow zone represents the sampling time window of the Analog-to-Digital Converter (ADC).

Another remarkable feature that improves the radar vibration measure capability is Multiple Input Multiple Output (MIMO). This technology in general provides the possibility of separating the targets in angle and measuring the Angle of Arrival (AoA). Exploiting MIMO for vibration measurement makes it possible to better separate targets and improve displacement measurements. Once the target is correctly detected, it is possible to extract its vibration by applying the method described in [7]. The vibration signal is contained inside the phase of s_b and indicated with $\psi_b(t)$, and it can be written as:

$$\psi_b(t) = \frac{4\pi f_c R_0 + 4\pi\, f_c\, x(t)}{c}, \tag{1}$$

where R_0 is the target distance, f_c the carrier frequency and $x(t)$ the vibration signal. By analysing the displacement signal $x(t)$, and, in particular, by evaluating its amplitude and frequency, it is possible to extract the encoded symbol.

The radar chosen configuration, according to the aforementioned requirements, is reported in Table I.

B. *Validation Setup*

We deployed a customizable quadcopter mounted on a metal tripod to validate the proposed measurement methodology. Such a custom UAV includes the frame of a DJI F450 as chassis, featuring four motor slots. The central part of the frame is made of metal and plastic, while the arms are made of plastic, with a wheelbase measuring 450 mm. The frame was

TABLE I: Radar configuration parameters.

Parameter	Value
N_s	512
f_s	12 MHz
S	70.006 MHz/µs
t_c	57 µs
Δ_t	6 µs
B	2940 MHz
PRI	2 ms

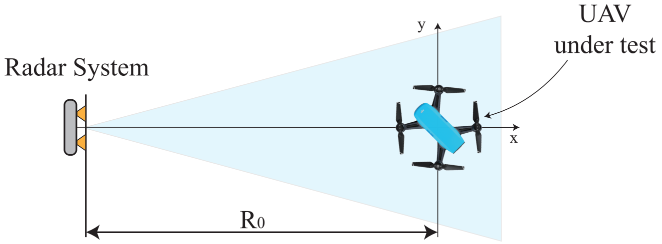


Fig. 2: Measurement setup block scheme.

Fig. 3: Gemfan 51499 propeller used in the arranged setup.

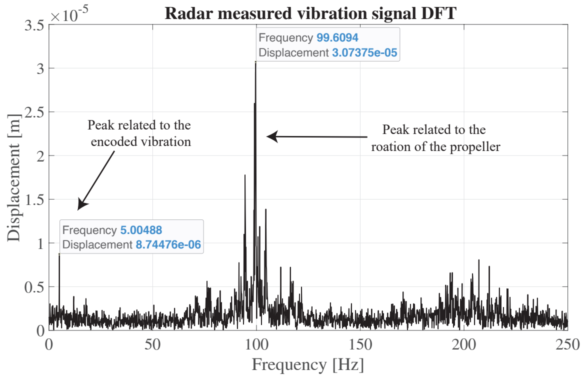


Fig. 4: Example of DFT spectrum computed on the extracted vibration signal. The identified peaks are related to the rotation speed of the propeller and to the encoded vibration.

equipped with four Brushless Direct Current (BLDC) motors, featuring a $K_v = 1000$ Revolutions Per Minute (RPM)/V, that were powered by as many $40\,\mathrm{A}$ Electronic Speed Controller (ESC) drivers, controlling the motors speed via PWM signals, receiving power from an external $12\,\mathrm{V}$ power supply unit. Owing to this experimental setup, the motors can reach a maximum speed of $12000\,\mathrm{RPM}$. The driving PWM signals operate at a frequency of $50\,\mathrm{Hz}$, with a T_{on} time between $1\,\mathrm{ms}$ and $2\,\mathrm{ms}$, thus translating into a duty cycle, D_c, ranging from $5\,\%$ to $10\,\%$. Indeed, a D_c greater than $5\,\%$ is required to start propellers rotation, while a D_c of $10\,\%$ enables the motors to reach the maximum speed. The PWM signals have an amplitude of $5\,\mathrm{V}$, and they are generated by a National Instruments myRIO-1900, providing the same control signals to all four motors. A scheme of the used setup is reported in Fig. 2.

For the PWM signals, a main set point was selected in order to ensure a rotational speed of the propellers. This rotation produces a specific related vibration that must be outside the range of the ones chosen for the symbol encoding. Indeed, different propellers can rotate at different RPMs for the same D_c value, because of their physical characteristics (e.g., shape, weight, number of blades, material, etc.). Specifically, we selected a T_{on} of $1.7\,\mathrm{ms}$, ensuring a rotational speed of $6130\,\mathrm{RPM}$ for the selected propeller type (i.e., the Gemfan 51499 depicted in Fig. 3). The value is measured with a laser tachometer. In so doing, the vibration to encode the symbols can be easily detected, being different.

To encode a communication symbol in a specific vibrational pattern of the drone chassis, the PWM driving signals must be tuned on purpose. Specifically, a slight variation of T_{on} is added to a specific time period indicated as T_{PWM}. Then, the amplitude of the encoded vibration is controlled by accordingly changing the entity of the PWM signal around the defined set point indicated as Δ_{PWM}. Therefore, by mapping specific displacement and frequency values of the measured vibration signals to communication symbols, a vibration-based communication protocol can potentially be set up.

V. EXPERIMENTAL TESTS

The first part of this Section is devoted at describing the method to modulate the vibration signature to encode a symbol, to potentially establish a communication protocol. The second part describes the method to decode the vibration signature for communication purposes. The idea behind the proposed encoding method is to measure the chassis displacement with the radar, and assign a communication symbol to a specific frequency peak. The spectrum is obtained by computing the Discrete Fourier Transform (DFT) of the collected vibration signal. To better explain this idea, Fig. 4 reports the spectrum of a vibration signal obtained with the radar sensor.

As remarked in Fig. 4, two main peaks are present in the DFT of the vibration signal. The highest one is related to the rotation speed of the propellers. Its frequency is $100\,\mathrm{Hz}$, that corresponds to $6000\,\mathrm{RPM}$. The second highlighted peak is related to the encoded vibration, in fact the figure is referred to a case in which Δ_{PWM} equals $0.005\,\mathrm{ms}$ and T_{on} amounts to $200\,\mathrm{ms}$. Such parameters generate an encoded vibration with a frequency of $5\,\mathrm{Hz}$ and a displacement of $8.7\,\mathrm{\mu m}$.

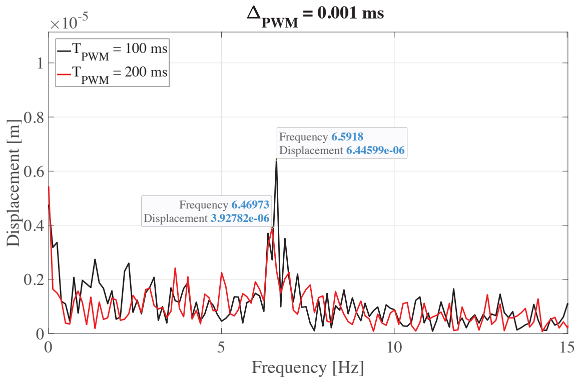


Fig. 5: Example of DFT spectrum obtained for the Δ_{PWM} of $0.001\,\mathrm{ms}$ and T_{PWM} of $100\,\mathrm{ms}$ and $200\,\mathrm{ms}$.

By combining different values of Δ_{PWM} and T_{PWM}, it is possible to define different points in a *displacement-frequency* plot, where each point is related to a communication symbol. To define the lowest encoded vibration that the radar can reveal, different values of T_{PWM} were tested, and it was discovered that the minimum value is $0.005\,\mathrm{ms}$. On the other hand, Fig. 5 reports the spectrum of the vibration measured for a Δ_{PWM} of $0.001\,\mathrm{ms}$, and T_{PWM} of $100\,\mathrm{ms}$ and $200\,\mathrm{ms}$. In this setting, the only peak present in the range of interest is around $6\,\mathrm{Hz}$, and it is not related to the vibration coding. Due to this, the exploited values to encode the PWM signal are: Δ_{PWM} set to $0.005\,\mathrm{ms}$ and $0.01\,\mathrm{ms}$ and T_{PWM} set to $100\,\mathrm{ms}$ and $200\,\mathrm{ms}$. The combination of these four values would make it possible to encode sequences composed of two bits assigned to the position of the peak in the *displacement-frequency* diagram, thus allowing to encode four symbols.

VI. RESULTS AND DISCUSSION

As a first approach, acquiring a long vibration signal with the radar is preferred. The reason is the DFT extraction method of the encoded vibration, which can better reveal harmonics if more samples are provided. Due to this, the radar acquires $10\,240$ samples for each test. Four tests were performed for the different values of Δ_{PWM} and T_{PWM}. Therefore, for each measured vibration signal, the DFT is computed to extract a communication symbol. The obtained DFTs plots are reported in Fig. 6.

Considering the highest peak of the DFT in the frequency range $0\,\mathrm{Hz}$ to $50\,\mathrm{Hz}$, it is possible to observe how its coordinates (i.e., displacement and frequency) are related to the control PWM signal. By assigning a communication symbol to each peak, it is possible to transmit information that can be discovered by the radar sensing system. The resulting four symbols, each related to one peak, are also shown in the *displacement-frequency* diagram of Fig. 7.

VII. CONCLUSIONS

The proliferation of applications requiring drone support has created the need for strong UAV identification methods. In a scenario where a CI must be secured from drone attacks, novel robust solutions are explored. In this work, the focus is on using the intrinsic vibration of the drone's chassis to exchange information on a covert channel. This method can be safer as a non-compliant drone will fail to communicate according to a predefined protocol through vibration. To demonstrate this approach, a radar sensing system is employed to measure the drone chassis vibration. An especially encoded PWM signal is used to control the rotation of the motors to produce a vibration useful to encode information. Preliminary tests demonstrated the feasibility of encoding four symbols, exploiting the displacement and frequency values of the detected vibration.

Future developments will investigate other aspects of the possible communication system like minimum symbol duration, drone stability and flight attitude compatible with the encoded PWM signal.

ACKNOWLEDGMENT

E.G. and S.S. acknowledge this work was partially supported by the European Union - Next Generation EU under the Italian National Recovery and Resilience Plan (NRRP), Mission 4, Component 2, Investment 1.3, CUP E63C22002070006, partnership on "Telecommunications of the Future" (PE00000001 - program "RESTART").

REFERENCES

[1] F. Minucci, E. Vinogradov, and S. Pollin, "Avoiding collisions at any (low) cost: ADS-B like position broadcast for UAVs," *Ieee Access*, vol. 8, pp. 121 843–121 857, 2020.

[2] B. Yilmaz and U. Kutbay, "YOLOv8 Based Drone Detection: Performance Analysis and Optimization," *Computers*, vol. 13, no. 9, p. 234, 2024.

[3] A. Brighente, M. Conti, G. Peruzzi, and A. Pozzebon, "ADASS: Anti-drone audio surveillance sentinel via embedded machine learning," in *2023 IEEE Sensors Applications Symposium (SAS)*. IEEE, 2023, pp. 1–6.

[4] D. Vovchuk, M. Khobzei, V. Tkach, O. Eliiashiv, O. Tzidki, K. Grotov, A. Glam, and P. Ginzburg, "Micro-Doppler-Coded Drone Identification via Resonant Tagging," *IEEE Transactions on Antennas and Propagation*, 2025.

[5] A. Coluccia, G. Parisi, and A. Fascista, "Detection and classification of multirotor drones in radar sensor networks: A review," *Sensors*, vol. 20, no. 15, p. 4172, 2020.

[6] J. S. Patel, F. Fioranelli, and D. Anderson, "Review of radar classification and RCS characterisation techniques for small UAVs or drones," *IET Radar, Sonar & Navigation*, vol. 12, no. 9, pp. 911–919, 2018.

[7] G. Ciattaglia, G. Iadarola, G. Battista, L. Senigagliesi, E. Gambi, P. Castellini, and S. Spinsante, "Displacement Evaluation by mmWave FMCW Radars: Method and Performance Metrics," *IEEE Transactions on Instrumentation and Measurement*, 2024.

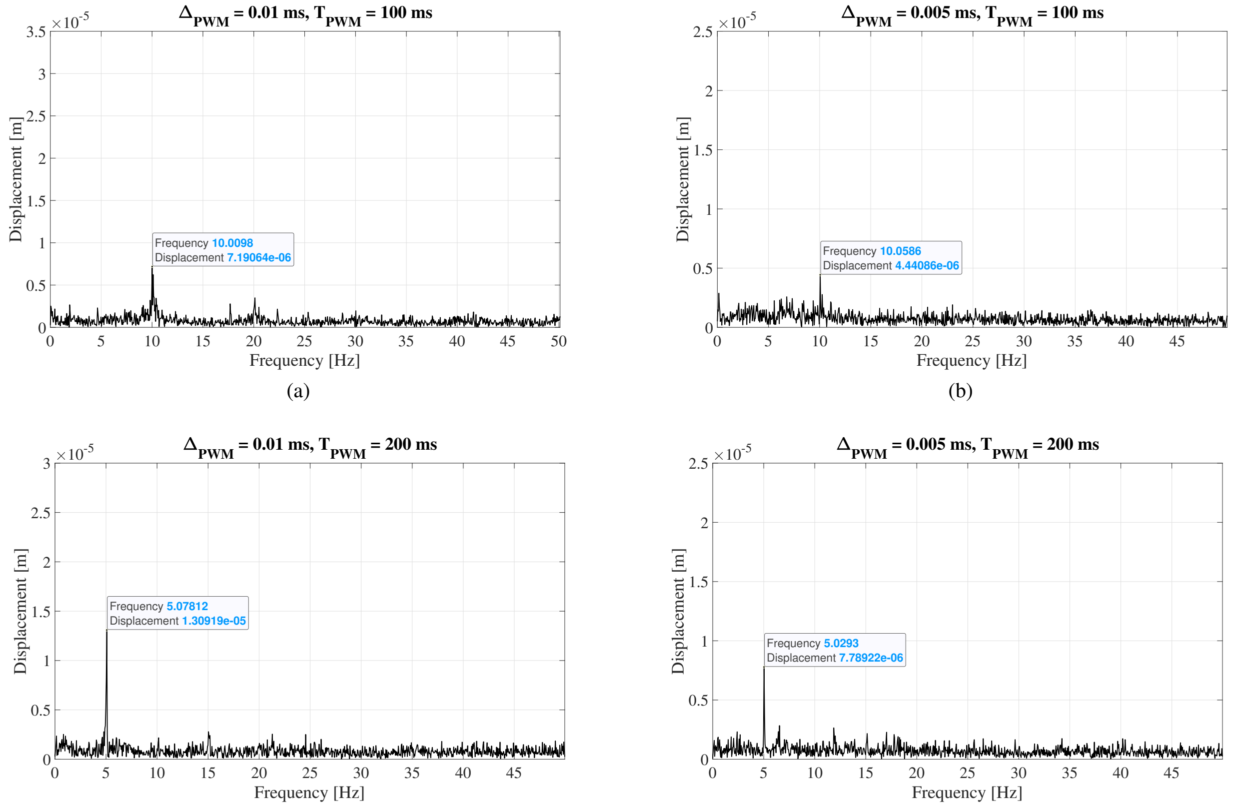
[8] G. Ciattaglia, G. Iadarola, L. Senigagliesi, S. Spinsante, and E. Gambi, "UAV propeller rotational speed measurement through FMCW radars," *Remote Sensing*, vol. 15, no. 1, p. 270, 2023.

[9] A. Brighente, G. Ciattaglia, E. Gambi, G. Peruzzi, A. Pozzebon, and S. Spinsante, "Radar-Based Autonomous Identification of Propellers Type for Malicious Drone Detection," in *2024 IEEE Sensors Applications Symposium (SAS)*. IEEE, 2024, pp. 1–6.

[10] X. Ying, G. Bernieri, M. Conti, L. Bushnell, and R. Poovendran, "Covert channel-based transmitter authentication in controller area networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 4, pp. 2665–2679, 2021.

[11] T. E. Calhoun, R. Newman, and R. Beyah, "Authentication in 802.11 LANs using a covert side channel," in *2009 IEEE International Conference on Communications*. IEEE, 2009, pp. 1–6.

[12] M. Guri, "ETHERLED: sending covert Morse signals from air-gapped devices via network card (NIC) LEDs," in *2022 IEEE International Conference on Cyber Security and Resilience (CSR)*. IEEE, 2022, pp. 163–170.



(a) (b) (c) (d)

Fig. 6: DFT peak identification in the frequency range $0\,\mathrm{Hz}$ to $50\,\mathrm{Hz}$: (a) $\Delta_{PWM} = 0.01\,\mathrm{ms}$ and $T_{PWM} = 100\,\mathrm{ms}$, (b) $\Delta_{PWM} = 0.005\,\mathrm{ms}$ and $T_{PWM} = 100\,\mathrm{ms}$, (c) $\Delta_{PWM} = 0.01\,\mathrm{ms}$ and $T_{PWM} = 200\,\mathrm{ms}$, and (d) $\Delta_{PWM} = 0.005\,\mathrm{ms}$ and $T_{PWM} = 200\,\mathrm{ms}$.

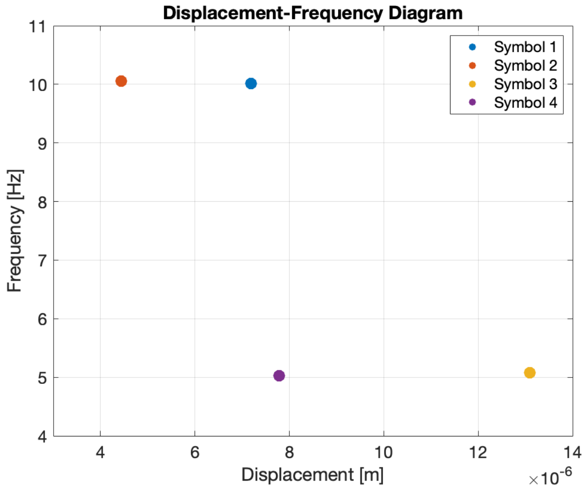


Fig. 7: The resulting four symbols arranged in a *displacement-frequency* diagram.

[13] N. Matyunin, Y. Wang, and S. Katzenbeisser, “Vibrational covert channels using low-frequency acoustic signals,” in *Proceedings of the ACM Workshop on Information Hiding and Multimedia Security*, 2019, pp. 31–36.

[14] M. Guri, “Exfiltrating data from air-gapped computers via ViBrAtIoNs,” *Future Generation Computer Systems*, vol. 122, pp. 69–81, 2021.

[15] J. Yun, D. Anderson, and F. Fioranelli, “Estimation of drone intention using trajectory frequency defined in radar’s measurement phase planes,” *IET Radar, Sonar & Navigation*, vol. 17, no. 9, pp. 1327–1341, 2023.

[16] F. Barbon, G. Vinci, S. Lindner, R. Weigel, and A. Koelpin, “A six-port interferometer based micrometer-accuracy displacement and vibration measurement radar,” in *2012 IEEE/MTT-S International Microwave Symposium Digest*. IEEE, 2012, pp. 1–3.

[17] V. C. Chen, “Doppler signatures of radar backscattering from objects with micro-motions,” *IET signal processing*, vol. 2, no. 3, pp. 291–300, 2008.