# Detecting Indoor Tiny Autonomous Malicious Drones within Critical Infrastructures: An Innovative Algorithm based on Harmonic Radar-Equipped Mini-Drones

ATHANASIOS N. SKRAPARLIS[1], KLIMIS S. NTALIANIS[1], MARIA S. NTALIANI[2], FILOTHEOS S. NTALIANIS[3], NIKOS E. MASTORAKIS[4]
[1]University of West Attica,
28, Agiou Spyridonos Str., 122-44, Egaleo,
GREECE

[2]Agricultural University of Athens,
75, Iera Odos Str., 118-55, Athens,
GREECE

[3]University of Piraeus,
80, A. Dimitriou & M. Karaoli Str., 185-34, Piraeus,
GREECE

[4]Industrial Engineering Department,
Technical University of Sofia,
Sofia,
BULGARIA

*Abstract:* - Critical infrastructures play a central role in the welfare of contemporary societies and they should properly function 24/7. Since their role is so important, they regularly become targets of malicious parties, terrorists, industrial spies, and even hostile governments. In this paper, the scenario of cyber or physical attacks to CIs from tiny autonomous malicious drones is analyzed. In particular, this work focuses on indoor spaces, protected by mini-drones. The mini-drones are equipped with harmonic radar and run a novel algorithm, which guides them to scan the whole area. Assuming that the malicious drones behave as non-linear systems, the mini-drones transmit signals and analyze the received signals, creating a non-linear system 3D location map for the whole space. In the consecutive scans, any changes on the 3D location map indicate that the malicious drone has changed location. Simulated results and comparisons to state-of-the-art approaches exhibit the cost-effectiveness and time efficiency of the proposed scheme as well as its limitations.

*Key-Words:* - Malicious drone, Autonomous, Critical Infrastructure, Mini-drone, Harmonic Radar, Indoor.

Received: December 15, 2023. Revised: August 14, 2024. Accepted: September 17, 2024. Published: October 14, 2024.

## 1 Introduction

Critical infrastructures (CIs) are the backbone of modern societies, encompassing vital sectors such as energy, transportation, communication, and water supply. Their proper functioning is crucial for economic stability, public safety, and national security. Any disruption or compromise of these infrastructures could have far-reaching and severe consequences, impacting not only the economy but also the well-being of citizens. Recognizing and safeguarding CIs is essential to ensure resilience against potential threats, both natural and man-made and to maintain the overall stability and functionality of a nation.

On the other hand, CIs can be subjected to cyber or physical attacks by tiny malicious drones. In the scenario of this paper, a malicious staff member of the CI brings the tiny autonomous malicious drone within the premises (indoors) of the CI and places it at an unattended location. During the night (or other circumstances), when the CI operates in low capacity with a minimum number of personnel, the tiny malicious drone may move to specific offices and record (for a specific timeframe) sensitive conversations (industrial espionage), interfere with

various critical systems and devices of the CI and/or install malicious software (electronic war), destroy parts of the CI by e.g. setting fire (physical damage), etc. In other words, it is like a virus inside a human body. After completing its mission, the tiny malicious drone may autonomously leave the CI and return to its base, or it may be picked up by the malicious staff member.

As it can be understood, such threats are very serious and should be efficiently tackled. Our previous research has focused on the physical security of CIs. In particular, in [1] a real-time threat assessment framework has been proposed to protect CIs from trucks carrying explosive substances. In [2] an innovative screening architecture has been introduced to protect CIs from various threats, such as guns, explosives, and radioactive substances. The current work extends our previous research by detecting tiny autonomous malicious drones. The proposed scheme focuses on indoor spaces of CIs. More specifically, it is assumed that the CI is protected by a mini-drone. The mini-drone is equipped with a harmonic radar and runs the proposed algorithm, which guides the mini-drone to scan the whole indoor space by moving on a 3D grid. It is also assumed that the tiny malicious drone behaves as a non-linear system. Each time the mini-drone visits a new node of the grid, it transmits a signal and analyses the received signal. After visiting all nodes, the mini-drone creates a non-linear system location map for the whole indoor space. The 3D location map contains all non-linear devices, including the malicious drone. In the next scans, any changes on the 3D location map indicate that the malicious drone has moved to a new location. Experimental results and comparisons to state-of-the-art approaches exhibit the advantages of the proposed scheme.

To summarize, this paper offers the following major contributions:

- It examines the case of tiny autonomous malicious drones, which may not send or receive signals. This case has not been thoroughly studied in the literature.
- It investigates the protection of indoor CI spaces by mini-drones equipped with harmonic radar, an approach that is much more efficient and flexible compared to the state-of-the-art.
- It proposes a novel algorithm, which guides the mini-drone to scan the whole indoor space and create a 3D location map.
- Through extensive simulations, the study not only validates the effectiveness of the proposed algorithm but also compares it with state-of-the-art approaches, highlighting its advantages and limitations, thereby contributing valuable insights for future research in drone detection technology.

The rest of the paper is organized as follows: Section 2 provides related work and Section 3 describes the proposed scheme. Simulated results and extensive comparison to state-of-the-art methods are presented in Section 4. Finally, Section 5 concludes this paper.

## 2 Related Work

In the literature, there are some works related to malicious drones. In particular, [3] introduces an approach for identifying critical drones by leveraging distributed features, communication intensity, and communication scale. Initially, a dynamic communication prediction network is constructed for drone swarms. Then, a dynamic giant connected component-based scale-intensity centrality method is proposed. In [4] an anti-RF solution that possesses the capability to identify, detect, and disrupt the communication link between a miniature drone and its remote controller is presented. This countermeasure has been seamlessly integrated into a Software Defined Radio platform to secure No Fly Zones (airports, public events, etc.). In [5] various cybercrime usages of drones are examined and the requirements of future security systems are discussed. In [6] a computer vision-powered monitoring system employs a supervised machine intelligence model and SqueezeNet, a deep neural network-based image embedder, to identify a malevolent UAV carrying an extraneous payload. In [7] detection of malicious UAVs is achieved by a machine-learning algorithm. Initially, sensor nodes deployed in a Wireless Sensor Network gather environmental data and send them to the UAV. To ensure data security, a proxy re-encryption scheme encrypts the feedback packet containing the sensed input data. Finally, the feedback packet undergoes decryption at the base station, revealing the actual input information. In [8] the viability of employing wireless localization methods for identifying drones engaged in location spoofing attacks is explored. GhostBuster, a modular solution designed to detect rogue RID-enabled drones is introduced and a comprehensive experimental campaign, utilizing open-source data derived from real drone flights is carried out. In [9] a dataset encompassing five classes, including images of airplanes, birds, drones, helicopters, and malicious UAVs is utilized.

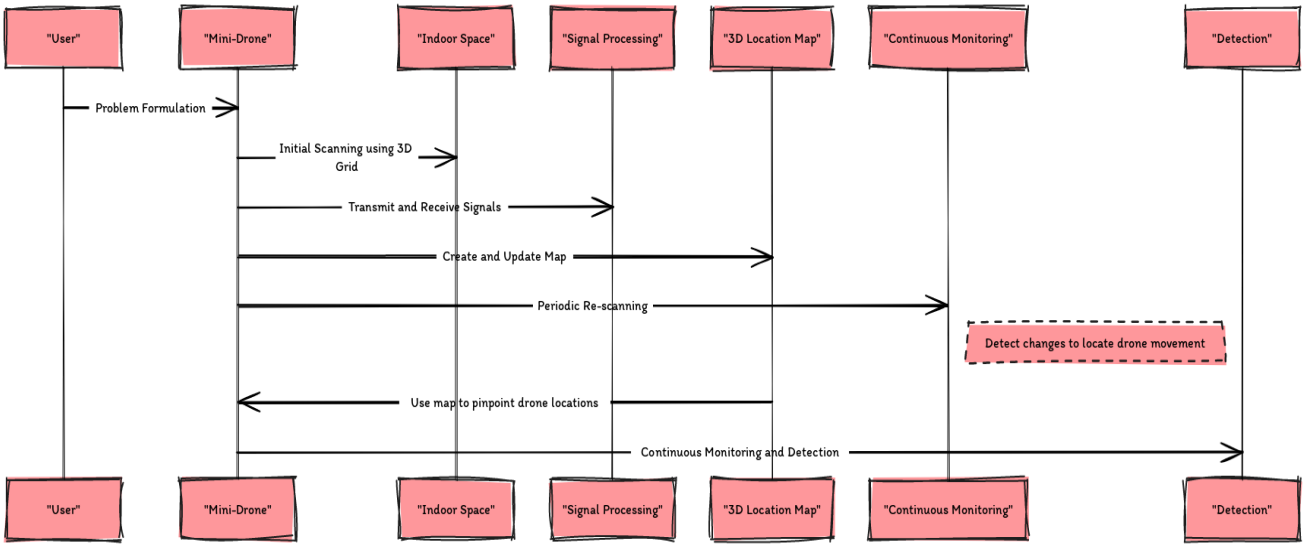



Fig. 1: Overview of the proposed scheme

Three distinct CNN models are employed to extract features from the images and the extracted features are classified using various machine learning methods. In [10] a protective framework designed to mitigate threats posed by malicious actors and to recover control of rogue UAVs is proposed. The framework implements a dynamic conceptual grid system overlaid on real-world geographical deployment, where the grid undergoes periodic shuffling or configurations based on abnormal behavior. In [11] unauthorized drones in an urban setting are detected through RF-based sensing, employing evenly distributed sensors. The study evaluates detection performance using the Neyman-Pearson criterion combined with Bayesian inference. In [12] a drone detection system designed for minimal prior configuration is introduced, utilizing affordable off-the-shelf hardware to identify privacy invasion attacks. By employing a model of the attack structure, statistical metrics for movement and proximity are derived and applied to the communication signals exchanged between a drone and its controller.

Additionally, there are several other works focusing on the detection of drones, [13], [14], [15], [16], [17], [18], [19], [20], [21], [22], [23], [24]. Most of them use computer vision techniques and may incorporate 3D depth maps, multi-spectral imaging, electro-optical sensors, multi-camera fields, and other approaches. Even though interesting, most of the aforementioned methods do not consider indoor spaces. Furthermore, they do not propose specific area scanning methods. Moreover, they cannot solve the problem of "silent" drones, which do not move (or move under cover) and do not receive or transmit signals. This paper confronts the aforementioned issues, by proposing a novel algorithm to scan indoor CIs and detect tiny malicious drones. The method is based on harmonic radar-equipped mini-drones and incorporates the concept of a 3D non-linear device location map.

# 3 The Proposed Scheme

## 3.1 Problem Formulation

Harmonic radar technology is a specialized radar system that functions through the transmission of a specific radio frequency signal and the detection of its harmonics, which are multiples of the original frequency that bounce back from a tagged object. Tags embedded with non-linear elements such as diodes produce these harmonic frequencies upon being struck by the radar's signal. This approach is distinguished by its ability to decrease environmental noise and clutter, given that natural reflections seldom imitate these exact frequency multiples. Therefore, harmonic radar proves to be highly efficient in monitoring small, tagged objects with precision and minimal disruption, rendering it well-suited for wildlife observation and other delicate tracking tasks. An overview of the proposed scheme is provided in Figure 1.

According to [25] and [26] many non-linear systems can be modeled by a power series. Let us assume that the malicious drone behaves as a non-linear system. Then the output of the system can be modeled by a power series:

$$E_r = \sum_{i=1}^{\infty} c_i E_t^i \quad (1)$$

If the input contains only one frequency, then the power series indicates that harmonics of that frequency will be generated by the non-linear

system. If:

$$E_t = E_0 \cos(\vartheta_0 t + \varphi) \quad (2)$$

then the response of the non-linear system can be written as:

$$E_r = c_0 + c_1 E_0 \cos(\vartheta_0 t + \varphi) + c_2 E_0^2 \cos^2(\vartheta_0 t + \varphi) + + c_3 E_0^3 \cos^3(\vartheta_0 t + \varphi) + \dots \quad (3)$$

where:

$$\cos^2(\vartheta_0 t + \varphi) = \frac{1}{2} + \frac{1}{2}\cos(2\vartheta_0 t + 2\varphi) \quad (4)$$

$$\cos^3(\vartheta_0 t + \varphi) = \frac{3}{4}\cos(\vartheta_0 t + \varphi) + \frac{1}{4}\cos(3\vartheta_0 t + 3\varphi) \quad (5)$$

Let us assume that $c_i = 0$, $i \geq 4$ and $E_0$ is small. Then the output $E_r$ can be written as:

$$E_r = c_0 + c_1 E_0 \cos(\vartheta_0 t + \varphi) + \frac{1}{2} c_2 E_0^2 \cos(2\vartheta_0 t + 2\varphi) + + \frac{1}{4} c_3 E_0^3 \cos(3\vartheta_0 t + 3\varphi) \quad (6)$$

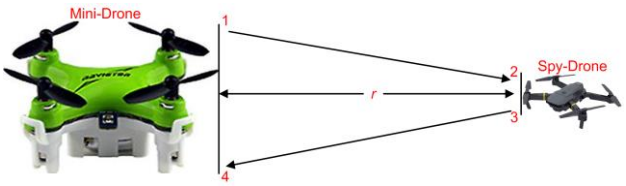



Fig. 2: The mini-drone's harmonic radar transmits a signal and receives its response from the malicious drone

Let us now examine Figure 2. In this figure the signal is transmitted from point 1, and it arrives at point 2 (target at a distance equal to *r* from the mini-drone's harmonic radar). The malicious drone behaves as a non-linear system and transmits back a signal from point 3. Finally, the mini-drone's harmonic radar receives the signal that returns back at point 4. The power at point "1" is:

$$P_1 = P_{tr} g_{tr} \quad (7)$$

where $P_{tr}$ is the power of the transmitted signal, while $g_{tr}$ is the gain of the mini-drones harmonic radar transmitter. Assuming that the signal spreads homogeneously (spherically) the power at point "2" is:

$$P_2 = \frac{P_1}{4\pi r^2} = \frac{P_{tr} g_{tr}}{4\pi r^2} \quad (8)$$

By modeling the relationship between the input and output signals that the non-linear malicious drone receives and transmits, according to Eq. (1) we have:

$$P_3 = \sum_{i=1}^{\infty} fa_i P_{2,in}^i \quad (9)$$

where $P_{2,in}^i$ is the input power received by the non-linear malicious drone (point "2") and $P_3$ is the output power of the non-linear malicious drone (point "3"). Furthermore, $fa_i$ is a factor, scaling *i*-th harmonic. $P_{2,in}^i$ is related to the effective aperture ($Ef_{sp}$) of the malicious drone (how much power the malicious drone can capture) and is calculated by:

$$P_{2,in}^i = P_2 Ef_{sp} \quad (10)$$

where $Ef_{sp}$ is for the lowest frequency (fundamental - $fr_{low}=\vartheta_0/2\pi$) of the transmitted signal (e.g. $\vartheta_0$ of Eq. (2)). More specifically, the effective aperture is related to the malicious drone's gain (antenna that receives the signal):

$$Ef_{sp} = g_{tar,r}^1 \frac{\lambda_{lF}^2}{4\pi} \quad (11)$$

where $g_{tar,r}^1$ is the malicious drone's gain for the lowest frequency of the transmitted signal and $\lambda_{lF}$ is the wavelength of the lowest frequency. By combining Eq. 9 and 10 for each harmonic *i*:

$$P_3^i = fa_i P_{2,in}^i = fa_i \left(P_2 Ef_{sp}\right)^i = = fa_i \left(\frac{P_{tr} g_{tr} Ef_{sp}}{4\pi r^2}\right)^i \quad (12)$$

Then the power of the *i*-th harmonic, leaving the non-linear malicious drone (point "3") can be expressed as:

$$P_{3,out}^i = g_{tar,t}^i P_3^i = g_{tar,t}^i fa_i \left(\frac{P_{tr} g_{tr} Ef_{sp}}{4\pi r^2}\right)^i \quad (13)$$

where $g_{tar,t}^i$ is the gain of the malicious drone's transmission antenna at the *i*-th harmonic. Considering a spherical spread back to the harmonic radar-equipped mini-drone, the power at point "4" can be expressed as:

$$P_4^i = g_{tar,t}^i fa_i \left(\frac{P_{tr} g_{tr} Ef_{sp}}{4\pi r^2}\right)^i \left(\frac{1}{4\pi r^2}\right) \quad (14)$$

Then, the power that the mini-drone's harmonic radar receives is estimated by incorporating the radar's effective aperture:

$$P_{4,in}^i = P_4^i Ef_{hr}^i = = g_{tar,t}^i fa_i \left(\frac{P_{tr} g_{tr} Ef_{sp}}{4\pi r^2}\right)^i \left(\frac{1}{4\pi r^2}\right) Ef_{hr}^i \quad (15)$$

where $Ef_{hr}^i$ is the effective aperture at the *i*-th harmonic and can be expressed as:

$$Ef_{hr}^i = g_{rv}^i \frac{\lambda_i^2}{4\pi} \quad (16)$$

where $g_{rv}^{i}$ is the gain of the mini-drone's harmonic radar receiver at the $i$-th harmonic and $\lambda_i$ is the respective wavelength.

By grouping all parameters of the non-linear malicious drone, we have:

$$k_i = g_{tar,t}^{i} f a_i \left(E f_{sp}\right)^i \quad (17)$$

Then Eq. (15) becomes:

$$P_{4,in}^{i} = \frac{g_{rv}^{i} \lambda_i^2 (P_{tr} g_{tr})^i k_i}{(4\pi)^{i+2} r^{2i+2}} \quad (18)$$

According to Eq. (18), the mini-drone's harmonic radar receives a power which is analogous to $\frac{1}{r^{2(i+1)}}$ for the ith harmonic frequency. Thus, as the mini-drone approaches the malicious drone, the power that the mini-drone's harmonic radar receives increases very fast. Additionally, the power that the mini-drone's harmonic radar receives is proportional to the power of the signal it transmits and the gain of its antenna. The gain is raised to $i$ (for the ith harmonic). Thus, if the mini-drone receives enough power, the existence of a malicious drone can be confirmed. However, in order to also estimate the distance between the mini-drone and the malicious drone, the phase of the received signal should also be analyzed.

Towards this direction, let us recall Eq. (2) for the transmitted signal at point "1". Then the analytic representation of Eq. (2), for $\theta_0 > 0$ is:

$$E_1 = E_0 e^{j(\theta_0 t + \varphi)} \quad (19)$$

where $\theta_0$ is the lowest frequency (fundamental), $\varphi$ is the initial phase of $\theta_0$, and $\lambda_{lF}$ is the wavelength of $\theta_0$. $E_0$ is the amplitude of the transmitted signal, related to the signal's power, which has already been discussed. The following analysis focuses on the phase of the signal ($\theta_0 t + \varphi$). In particular, the signal propagates from point "1" to point "2" traveling a distance $r$, which results in a change of its phase by $\Delta\theta_{1,2}$. More particularly:

$$if\ r = \lambda_{lF}\ then\ \Delta\theta_{1,2} = 2\pi \Rightarrow$$
$$\frac{r}{\Delta\theta_{1,2}} = \frac{\lambda_{lF}}{2\pi} \Rightarrow \Delta\theta_{1,2} = \frac{2\pi}{\lambda_{lF}} r \quad (20)$$

As a result, the signal at point "2" will be:

$$E_2 = E_0 e^{j(\theta_0 t + \varphi + \Delta\theta_{1,2})} \quad (21)$$

Again, by modelling the relationship between the input and output signals that the non-linear malicious drone receives and transmits, according to Eq. (1) we have:

$$E_3 = \sum_{i=1}^{\infty} ha_i E_2^i \quad (22)$$

where $ha_i$ corresponds to the amplitude of the ith harmonic of the signal transmitted back from the malicious drone.

For notation simplicity and by dropping $ha_i$ and $E_0$ (since they are not related to the signal's phase) we get:

$$\acute{E}_3 = \sum_{i=1}^{\infty} e^{ij(\theta_0 t + \varphi + \Delta\theta_{1,2})} \quad (23)$$

Finally, the signal propagates back from point "3" to point "4" traveling a distance $r$, which results in a change of its phase by $\Delta\theta_{3,4}^{i}$:

$$\acute{E}_4 = \sum_{i=1}^{\infty} e^{ij(\theta_0 t + \varphi + \Delta\theta_{1,2})} e^{j\Delta\theta_{3,4}^{i}} \quad (24)$$

or

$$\acute{E}_4 = \sum_{i=1}^{\infty} e^{j(i(\theta_0 t + \varphi + \Delta\theta_{1,2}) + \Delta\theta_{3,4}^{i})} \quad (25)$$

$\Delta\theta_{3,4}^{i}$ is different for each harmonic frequency $i$. More specifically and based on Eq. (20):

$$\Delta\theta_{3,4}^{i} = \frac{2\pi}{\lambda_i} r \quad (26)$$

where $\lambda_i$ is the wavelength of the ith harmonic frequency. Considering that:

$$\lambda_1 \equiv \lambda_{lF},\ \lambda_2 = \frac{1}{2}\lambda_{lF}, \lambda_3 = \frac{1}{3}\lambda_{lF}, etc. \quad (27)$$

we have that:

$$\Delta\theta_{3,4}^{i} = i\Delta\theta_{1,2} \quad (28)$$

Then Eq. (25) becomes:

$$\acute{E}_4 = \sum_{i=1}^{\infty} e^{j(i(\theta_0 t + \varphi + \Delta\theta_{1,2}) + i\Delta\theta_{1,2})} \Rightarrow$$
$$\acute{E}_4 = \sum_{i=1}^{\infty} e^{ji(\theta_0 t + \varphi + 2\Delta\theta_{1,2})} \quad (29)$$

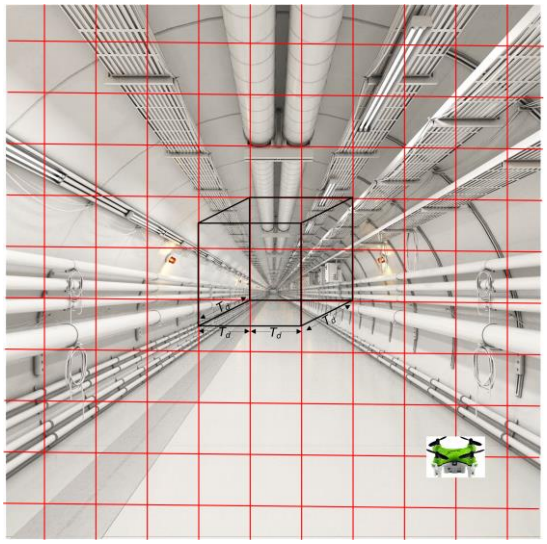


Fig. 3: Mini-drone scanning indoor space to create 3D non-linear device location map and detect tiny malicious drones

Athanasios N. Skraparlis, Klimis S. Ntalianis,
Maria S. Ntaliani, Filotheos S. Ntalianis,
Nikos E. Mastorakis

### 3.2 The Innovative Indoor Spy-Drone Detection Algorithm

According to Eq. (29) and assuming the existence of a malicious drone, the mini-drone will receive: (a) a signal with power calculated using Eq.(18) for $i$=1, frequency $fr_{low}$ (wavelength $\lambda_{lF}$) and phase $(\theta_0 t + \varphi + 2\Delta\theta_{1,2})$, (b) a signal (first harmonic) with power calculated using Eq.(18) for $i$=2, frequency $2fr_{low}$ (wavelength $\lambda_2$) and phase $2(\theta_0 t + \varphi + 2\Delta\theta_{1,2})$, which is double compared to the phase of $fr_{low}$ etc. Without loss of generality, if $\varphi$=0, then we have for $fr_{low}$:

$$\Delta\theta_{1,4} = 2\pi fr_{low} t + \frac{2\pi fr_{low}}{c} r \quad (30)$$

and since $\Delta\theta_{1,4}$ is measured by the mini-drone (since the mini-drone knows the transmitted and estimates the received signal), the distance of the malicious drone can be calculated by:

$$r = \frac{c}{2\pi fr_{low}} (\Delta\theta_{1,4} - 2\pi fr_{low} t) \quad (31)$$

Thus, if the indoor space is empty, it is straightforward to detect the malicious drone. However, in most cases the indoor space of a CI is not empty but it contains several electronic devices, which behave in a non-linear way, just as the malicious drone does. In order to detect the malicious drone in such an environment, the mini-drone runs the proposed innovative algorithm. In particular, the mini-drone, scans the whole indoor space by moving on a 3D grid. An example is provided in Figure 3. More specifically, the mini-drone can start from a node (where two red lines cross) and each time move by a distance equal to $T_d$, which defines the size of the scan-cube (represented in black color, within Figure 3). Each time it visits a new node $nd_i$, $i$=1, …,$n$, the mini-drone transmits a signal at $fr_{low}$ and analyses the received signal. After visiting all nodes, the mini-drone creates a non-linear system location map for the whole indoor space by using Eq. (31). The 3D location map contains all non-linear devices, including the malicious drone.

If the mini-drone could have been provided in advance with a legitimate location map, then it would be an easy task to detect the malicious drone. However, the creation of a legitimate map needs accurate and time-consuming preliminary work. The proposed algorithm does not need a legitimate map. To do so, the mini-drone periodically re-scans the indoor space. As long as the 3D location map remains the same, either there is not any malicious drone or the malicious drone does not move. If the malicious drone moves, then the 3D location map will change, leading to the detection of the malicious drone (new location within the 3D location map).

There is only one case, where the malicious drone may remain undetectable by the 3D location map method. In this case, it is assumed that the malicious drone is able to stick to the legitimate devices (approach as close as possible) that exist within the indoor space. Thus, when the mini-drone is far away during the scanning process, the malicious drone can move to the next legitimate device. However, in order to locate indoor legitimate devices, the malicious drone has to transmit a signal, operating in a similar - to the mini-drone- way. But, if a signal is transmitted, then the malicious drone reveals its existence. The same happens if the malicious drone is remotely operated. The aforementioned analysis results in Algorithm 1.

**Algorithm 1**: Indoor Space Scanning and Malicious Drones Detection

```
// ######## INITIALIZATION ########
mini_drone.move.to -> (x0, y0) // mini drone can start from any node, but for simplicity, it is assumed that it moves to initial node of the 3D grid e.g. bottom right
if (3D_map.available == "true") // 3D map of the indoor infrastructure is available at the system's server
then {
      mini_drone.receive -> 3D_map
      go.to(MALICIOUS DRONE LOCATION)
      }

// ######## CREATE 3D MAP ########
else {
SCAN(j):
      for (i=1:n)
         {
          mini_drone.move.to -> ndi //mini-drone moves to all nodes of the 3D grid
          mini_drone.transmit_signal = true  // mini-drone transmits signal to detect non-linear device (NLD)
          mini_drone.receive_signal -> P^i_{4,in} //Eq. (18)
          mini_drone.select -> max(P^i_{4,in}) // mini-drone keeps only the NLD providing the maximum value of P^i_{4,in}
          mini_drone.estimate.distance.max_NLD -> ri //Eq. (31)
          R_all-> (r1, r2, …, rn)  //all measured distances are stored in R_all
         }

       mini_drone.create(R_all)-> 3D_map(j) //R_all is used to create 3D_map
       system_server.receive-> 3D_map(j) // 3D_map is received by the system's server
     }

    // ######## MALICIOUS DRONE LOCATION########
while (mini_drone.on_duty == "true") // a specific mini-drone is on duty, scanning the indoor area. If it needs re-charging, then another mini-drone takes its place

do {
    3D_map(j) <- SCAN(j).return.3D_map //the mini-drone scans the whole 3D grid to provide the jth instance of the3D_map
    if (3D_map(j) ≠ 3D_map(i), for i ≠ j)  //if the jth instance of the 3D_map is different from the ith instance of the3D_map
       {
        spy_drone.detection = true // spy-drone is detected, occupying a
```

```
new position within the 3D_map
        spy_drone.location.(x,y,z)->(3D_map(j).(x,y,z)-
        -3D_map(i).(x,y,z)).nonzero // the location (x,y,z coordinates)
of the malicious_drone is calculated
        }
}
```

# 4 Experimental Results

A PC with Intel(R) Core i7-12700 CPU @ 3.60GHz plus 16 GB DDR4 RAM was used for running the experiments. Results and comparisons were simulated using R 4.3.2. For the following calculations $P_{tr}$ is assumed to be 0.1 Watt (30 dBm), since: (a) the antenna of a small drone does not have to transmit high-power signals and (b) in this way less energy is used for malicious drone detection. On the other hand, $g_{tr}$ for $fr_{low}$ is assumed to be 5 dBi, $g_{rv}^1$ is assumed to be 5 dBi and $g_{rv}^2$ is assumed to be 3 dBi. Additionally, $g_{tar,t}^1 = g_{tar,r}^1 = g_{tar,t}^2 = g_{tar,r}^2 = 1\ dBi$, since it is considered that the gain of the malicious drone does not resemble the gain of real antennas, but it is significantly less. Furthermore, $fr_{low}$ is set to 900 MHz ($\lambda_1 \equiv \lambda_{lF} = 0.33\ m$) with its first harmonic at 1,800 MHz ($\lambda_2 = 0.165\ m$). Finally, $fa_1$=1, $fa_2$= 0.5, $\pi \approx 3.14$ and $c \approx 299{,}792{,}458$ m/sec. Here it should be mentioned that the most common parameters have been selected for the problem under consideration, but even if other parameters are selected, they will lead to similar results.

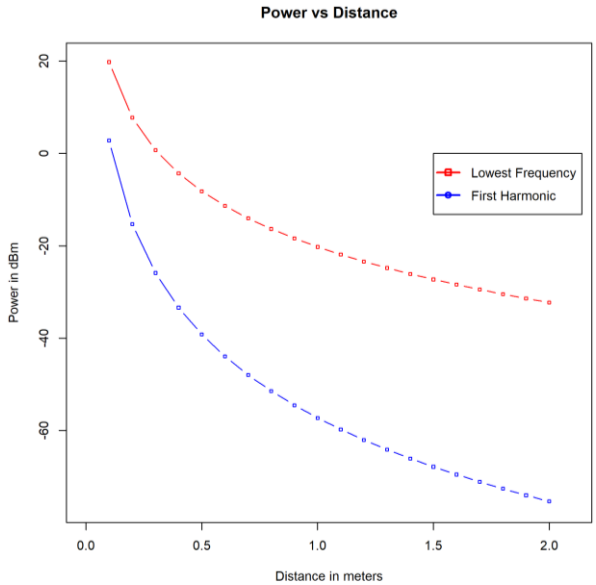



Fig. 4: Power received by the antenna of the mini-drone for the lowest frequency and its first harmonic

Based on the aforementioned parameters, $P_{4,in}^1$ and $P_{4,in}^2$ (Eq. 18) are calculated and visualized in Figure 4. As it can be observed, the received power at a distance of 0.1m is 19.77 dBm and 2.76 dBm for the lowest frequency and the first harmonic, while, in the case of 2m it falls to -32.27 dBm and -75.3 dBm respectively. Here it should be mentioned that each receiver has a sensitivity. If the strength of the received signal is less than the sensitivity threshold, then the receiver will not be able to receive the signal. According to [27], the common 802.11g products have a sensitivity of -85 dBm, many wireless market products offer a sensitivity of -105 dBm, while professional devices provide a receiver sensitivity of almost -120 dBm. Thus, the proposed scheme with its specific parameters enables the mini-drone to detect the malicious drone, even if its antenna is a common market product and not a highly specialized and specifically designed antenna. Reliable detection of the malicious drone can be achieved even at a distance of 2 meters.


(a) (b)

Fig. 5: (a) Hand-held scanning device (b) Passive infrared sensor

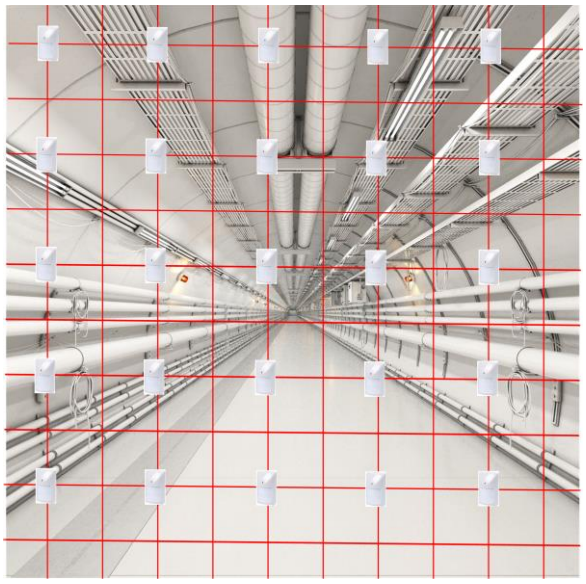


Fig. 6: Foldable grid of sensors

## 4.1 Comparison to State-of-the-Art Approaches

Sensors emitting laser beams could somehow confront the problem of tiny malicious drones, but

such a solution would need a huge number of laser sensors to cover the whole space and possibly produce many false alarms (due to bugs, insects, etc.). For this reason, in this paper, two common approaches are considered and compared to the proposed scheme. The first, traditional approach is based on a human guard who holds a scanning device (Figure 5(a)) and inspects the whole CI. The second approach is based on passive infrared sensors (Figure 5(b)), e.g. and without loss of generality, Panasonic's PaPIRs passive infrared sensors [28], [29]. Additionally, let us assume that the CI resembles a rectangular tank with a length equal to 100 m, a width equal to 4 m, and a height equal to 4 m. In this case, the volume of the CI is estimated to be 1,600 $m^3$. According to [28], [29] PaPIRs can detect an area of 70×25 cm (1,750 $cm^2$) at a distance of 12 m. Assuming that the tiny spy-drone has a size of 7.5×7.5 cm (56.25 $cm^2$) and considering that PaPIRs exhibit a linear behavior regarding the distance – detectable area relation, then PaPIRs sensors should be placed about every 0.8m in order to be able to detect the tiny malicious drone, in a foldable grid (Figure 6). The grid of sensors could be unfolded on non-working hours and folded on working hours.

On the other hand, it is assumed that the human guard can raise the hand-held scanning device to a height of 2 – 2.2 meters. In this case, the malicious drone's maximum distance could be 1.8 – 2 meters. Considering similar to the mini-drone's receiver sensitivity, the human guard can effectively scan the whole CI, using the hand-held scanning device.

Next, the three approaches are compared quantitatively and qualitatively. In particular, the quantitative comparisons include the time to scan the CI and the cost of scanning, while the qualitative comparisons include false alarms and parameters such as sensitivity, human mistakes, preparation time, and ease of installing/uninstalling.

Regarding the time to scan the CI, let us consider that the CI is cut into slices and the distance between slices is 1 m. Let us also consider that the human guard moves at a speed of 1.4 m/sec and spends 5 seconds to scan each slice. Let us also consider that the mini drone passes through the center of the slices (following the axis of the grid), transmits a signal every 0.01 seconds, and moves at a speed of 1 m/sec. In order to scan the CI under consideration, the human guard needs 571.4 sec, the passive infrared sensors approach needs 0 sec and the proposed approach needs 100 sec. Figure 7 provides the scan time per CI's cubic meter for the three approaches. Volume is provided in the log10 scale. As it can be observed, the passive infrared sensors approach needs zero time, since the grid of sensors covers the whole volume of the CI. Additionally, the human scanning approach provides the worst performance (in case of 50,000 $m^3$, scanning takes 17,856.25 sec), while the proposed approach provides a time reduction of 82.5% compared to the human scanning approach (e.g. in the case of 50,000 $m^3$, scanning takes 3,125 sec).

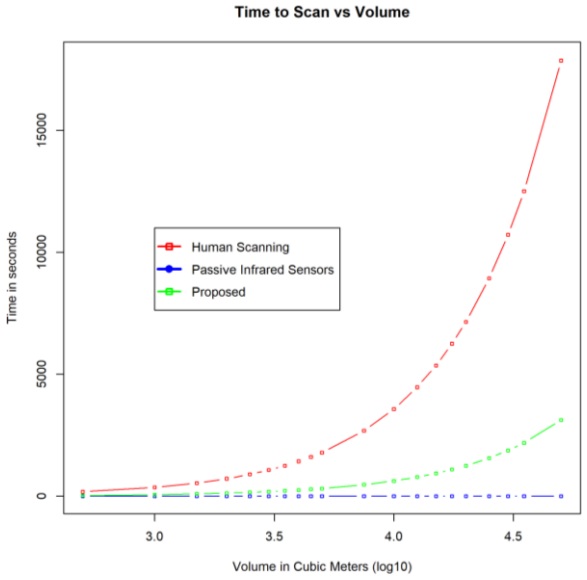
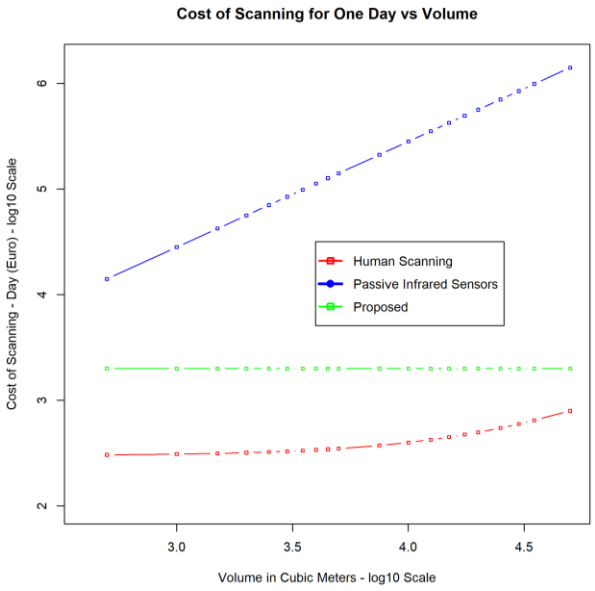



Fig. 7: Time to scan CI versus CI's volume (in cubic meters – log10 scale)

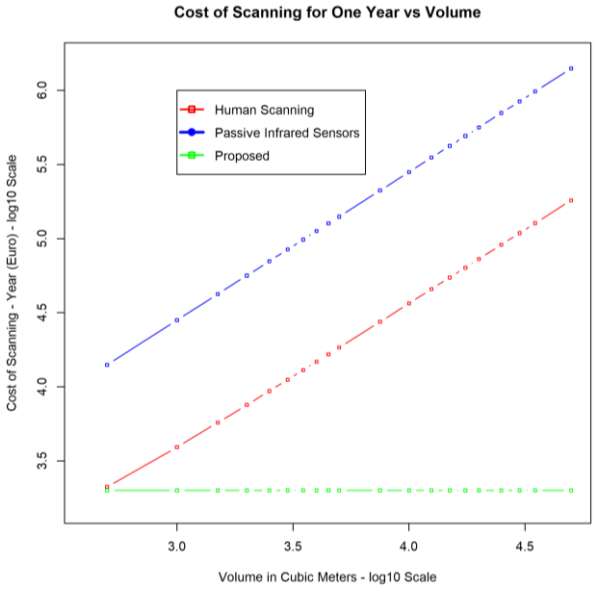
Now, regarding the cost of scanning, let us assume that a human guard has a total cost (daily rate, insurance, etc.) of 80 Euros per 8 hours and the hand-held scanning device costs 300 Euros. Let us also assume that each passive infrared sensor costs on average 10 Euros [30] (depending on the number of purchased sensors). In order to cover the whole CI, each slice (foldable grid of passive infrared sensors) should contain 36 sensors (one every 0.8 meters), while the total number of slices is 125 (each slice every 0.8 meters). As a result, the whole CI is covered by 4,500 sensors. On the other hand, the cost of buying an autonomous mini drone like e.g. Pegasus mini [31] and making all necessary adaptations (e.g. addition of transmitter, receiver, signal analyzer, etc.) may reach 2,000 Euros. It is also assumed that in one day, the CI should be scanned 10 times. This is reasonable, since the malicious drone may move at any time from its position. Then the overall cost for one day and for one year are visualized in Figures 8(a) and 8(b) respectively.

Table 1. Qualitative comparison of the three approaches

| | False Alarms | Sensitivity | Human Mistakes | Preparation Time | Ease of Installing / Uninstalling |
|---|---|---|---|---|---|
| **Human Scanning** | Very Low | Very Low | Yes | No | Easy |
| **Passive Infrared Sensors** | Moderate | Moderate | No | Moderate | Difficult |
| **Proposed** | Very Low | Very Low | No | No | Easy |




(a)




(b)

Fig. 8: (a) Cost in Euro (log10 scale) of One-Day Scanning versus CI's volume (in cubic meters – log10 scale) (b) Cost in Euro (log10 scale) of One-Year Scanning versus CI's volume (in cubic meters – log10 scale)

As it can be observed, the minimum cost for one day is provided by the human scanning approach (304.96 Euro for a CI of 500 $m^3$ and 796 Euro for a CI of 50,000 $m^3$). This is expected in the short term since the cost of the hand-held device is much lower (300 Euro) than the cost of the modified mini-drone (2,000 Euro). However, in the long term, the proposed approach provides much lower operational costs compared to the other two approaches. In particular (Figure 8(b)), the minimum cost for one year is provided by the proposed scanning approach (2,000 Euro for a CI of any volume), while the human scanning approach requires 2,110.43 Euro for a CI of 500 $m^3$ and 181,342.54 Euro for a CI of 50,000 $m^3$ and the passive infrared sensors approach requires 14,062.5 Euro for a CI of 500 $m^3$ and 1,406,250 Euro for a CI of 50,000 $m^3$.

Thus, (a) compared to the human scanning approach, the proposed approach reduces the scanning cost from 5.23% to 98.9% (b) compared to the passive infrared sensors approach, the proposed approach reduces the scanning cost from 85.78% to 99.86 %. Here it should be mentioned that the cost of recharging the mini-drone's batteries is neglected since it is low. Even if it is considered, the costs of the other two approaches (especially for large CIs) are still orders of magnitude greater.

Finally, a qualitative comparison of the three approaches is provided in Table 1. In particular, regarding false alarms, the passive infrared sensors approach may be vulnerable to insects, swarms of bugs, etc. Regarding sensitivity, the passive infrared sensors approach may be more sensitive to temperature and for this reason, it is recommended that sensors are 3 to 5 meters away from heat sources. Additionally, the passive infrared sensors approach cannot detect malicious drones if they are not moving. The proposed approach and the human scanning approach can detect malicious drones if a ground truth 3D location map is available. If there is not a ground truth 3D location map and the malicious drone does not move it cannot be located. In this case, a malicious worker (maybe a staff member of the CI) could pick up the malicious drone and leave the CI.

Furthermore, the human scanning approach may be vulnerable to human mistakes (e.g. if the human guard does not properly scan the CI). On the other hand, the passive infrared sensors approach may need some time for preparation, especially in order to unfold (and fold) the grid of sensors. Finally, the passive infrared sensors approach takes much time to install/uninstall and it is a solution of low portability, compared to the other two approaches. For reproducing the simulated results, datasets are provided in Table 2, Table 3, Table 4 and Table 5 of the appendix.

## 5 Conclusion

Critical infrastructures face a significant risk of rapid destruction or becoming targets of various cyber-attacks at minimal cost, if not adequately defended against tiny malicious drones. This study concentrated on countering autonomous tiny malicious drones, by incorporating mini-drones equipped with harmonic radar and a novel algorithm that creates 3D non-linear device location maps of indoor areas. Extensive comparisons to state-of-the-art methods revealed both the advantages and limitations of the proposed approach.

Future research can address various unresolved issues. For instance, the scenario where the malicious drone does not move, the case of very large CIs or the case of CIs that combine indoor and outdoor sensitive areas. Further research initiatives might also involve creating a more extensive simulation framework that incorporates practical challenges such as dynamic obstacles and various drone speeds, thus enhancing the evaluation of the algorithm's efficacy in complex scenarios. Lastly, there is potential for implementing security plans optimized for specific critical infrastructures, taking into account their unique characteristics.

*Acknowledgement:*
The authors would like to thank Dr. Dimitrios Kouremenos, Mr. Vasilios Yfantis, Mr. Andreas Kener† and Mr. Konstantinos Psaraftis for their support, ideas, comments and remarks regarding the experimentation phase.

*References:*

[1] A. Skraparlis, K. S. Ntalianis and N. E. Mastorakis, "Real Time Threat Assessment of Truck Cargos Carrying Dangerous Goods for Preventing Terrorism Attacks on Neighboring Critical Infrastructures," *IEEE Access*, vol. 10, pp. 76547-76562, 2022, doi: 10.1109/ACCESS.2022.3189674.

[2] A. Skraparlis, K. Ntalianis, D. Kouremenos and N. Mastorakis, "An innovative security screening architecture for detecting illicit goods and threats," *International Journal of Mathematics and Computers in Simulation*, vol. 15, pp. 153-160, 2021, doi: 10.46300/9102.2021.15.28

[3] M. Teng, C. Gao, Z. Wang, and X. Li, "A communication-based identification of critical drones in malicious drone swarm networks," *Complex Intell. Syst.*, vol. 10(3) , pp. 1-15, Jan. 2024, https://doi.org/10.1007/s40747-023-01316-9

[4] F. Slimeni, T. Delleji, Z. Chtourou, "RF-Based Mini-Drone Detection, Identification & Jamming in No Fly Zones Using Software Defined Radio," In: Nguyen, N.T., Manolopoulos, Y., Chbeir, R., Kozierkiewicz, A., Trawiński, B. (eds) Computational Collective Intelligence. ICCCI 2022. Hammamet, Tunisia. *Lecture Notes in Computer Science*, vol. 13501, pp. 791-798, Springer, Cham. https://doi.org/10.1007/978-3-031-16014-1_62

[5] M.S. Bressler and L. Bressler, "Beware the unfriendly skies: how drones are being used as the latest weapon in cybercrime", *Journal of Technology Research,* vol. 7, pp. 1-12, 2017, [Online]. https://www.aabri.com/manuscripts/172584.pdf (Accessed Date: July 6, 2024).

[6] S.K. Bhoi, K.K. Jena, K.D. Naik, C. Mallick, R. P. Nayak, "Detection of Malicious Unmanned Aerial Vehicle Carrying Unnecessary Load Using Supervised Machine Intelligence Model with SqueezeNet Deep Neural Network Image Embedder," In: Jacob, I.J., Kolandapalayam Shanmugam, S., Izonin, I. (eds) Data Intelligence and Cognitive Informatics. *Algorithms for Intelligent Systems,* pp. 349-361, Springer, Singapore, 2023, https://doi.org/10.1007/978-981-19-6004-8_28.

[7] S. V. R. V. Prasad and P. M. Khilar, "SVM-SFL based malicious UAV detection in wireless sensor networks," *Concurrency Computat Pract Exper.*, vol. 36(13):e8049, 2024, doi: 10.1002/cpe.8049.

[8] M. Keizer, S. Sciancalepore and G. Oligeri, "GhostBuster: Detecting Misbehaving Remote ID-enabled Drones," 2024 *IEEE 21st Consumer Communications & Networking Conference (CCNC)*, Las Vegas, NV, USA,

pp. 324-332, 2024, doi: 10.1109/CCNC51664.2024.10454860.

[9] A. Feyzioglu, and Y. S. Taspinar, "Malicious UAVs Classification Using Various CNN Architectures Features and Machine Learning Algorithms," *International Journal of 3D Printing Technologies and Digital Industry*, vol. 7(2), pp. 277-285, 2023, https://doi.org/10.46519/ij3dptdi.1268605

[10] M. A. Sayeed, R. Kumar and V. Sharma, "Safeguarding unmanned aerial systems: an approach for identifying malicious aerial nodes," *IET Communications*, vol. 14(17), pp. 3000-3012,2020, https://doi.org/10.1049/iet-com.2020.0073.

[11] S. Al-Dharrab, "Detection Performance of Malicious UAV using Massive IoT Networks," *2023 IEEE 97th Vehicular Technology Conference*, Florence, Italy, pp. 1-5, 2023, doi: 10.1109/VTC2023-Spring57618.2023.10200462

[12] S. Birnbach, R. Baker, S. Eberz and I. Martinovic, "#PrettyFlyForAWiFi: Real-world Detection of Privacy Invasion Attacks by Drones," *ACM Transactions on Privacy and Security*, vol. 24(4) pp. 1–34, 2021, https://doi.org/10.1145/3473672.

[13] E. Unlu, E. Zenou, N. Riviere and P.-E. Dupouy, "Deep learning-based strategies for the detection and tracking of drones using several cameras". *IPSJ Transactions on Computer Vision and Applications*, vol. 11(7), 2019, https://doi.org/10.1186/s41074-019-0059-x.

[14] P. Zhu, L. Wen, D. Du, X. Bian, H. Fan, Q. Hu and H. Ling, "Detection and Tracking Meet Drones Challenge," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 44(11), , pp. 7380-7399, 2022, doi: 10.1109/TPAMI.2021.3119563.

[15] R. Hamatapa and C. Vongchumyen, "Image Processing for Drones Detection," *2019 5th International Conference on Engineering, Applied Sciences and Technology (ICEAST)*, Luang Prabang, Laos, 2019, pp. 1-4, doi: 10.1109/ICEAST.2019.8802578.

[16] A. Carrio, J. Tordesillas, S. Vemprala, S. Saripalli, P. Campoy and J. P. How, "Onboard Detection and Localization of Drones Using Depth Maps," *IEEE Access*, vol. 8, pp. 30480 – 30490, 2020, doi: 10.1109/ACCESS.2020.2971938.

[17] M. W. Ashraf, W. Sultani and M. Shah, "Dogfight: Detecting Drones from Drones Videos," *2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, Nashville, TN, USA, 2021, pp. 7063-7072, doi: 10.1109/CVPR46437.2021.00699.

[18] K. Abbasi, A. Batool, F. M. A. Asghar, A. Saeed, M. J. Khan and M. U. Rehman, "A Vision-Based Amateur Drone Detection Algorithm for Public Safety Applications," *2019 UK/ China Emerging Technologies (UCET)*, Glasgow, UK, 2019, pp. 1-5, doi: 10.1109/UCET.2019.8881879.

[19] S. Scholes, A. Ruget, G. Mora-Martín, F. Zhu, I. Gyongy and J. Leach, "DroneSense: The Identification, Segmentation, and Orientation Detection of Drones via Neural Networks," *IEEE Access*, vol. 10, pp. 38154-38164, 2022, doi: 10.1109/ACCESS.2022.3162866.

[20] S. Luesutthiviboon, G. C. H. E. de Croon, A. V. N. Altena, M. Snellen and M. Voskuijl, "Bio-inspired enhancement for optical detection of drones using convolutional neural networks," *Proc. SPIE vol. 12742, Artificial Intelligence for Security and Defence Applications*, Amsterdam, Netherlands, 127420F (17 October 2023); https://doi.org/10.1117/12.2673788.

[21] R. Tiwari and A. K. Dubey, "Detection of Camouflaged Drones using Computer Vision and Deep Learning Techniques," *2022 12th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*, Noida, India, 2022, pp. 380-383, doi: 10.1109/Confluence52989.2022.9734191.

[22] C. J. Swinney and J. C. Woods, "A Review of Security Incidents and Defence Techniques Relating to the Malicious Use of Small Unmanned Aerial Systems," *IEEE Aerospace and Electronic Systems Magazine,* vol. 37(5), pp. 14-28, 2022, doi: 10.1109/MAES.2022.3151308.

[23] P. Crippa, *"Cyber Security and Drones,"* In: Masys, A.J. (eds) Handbook of Security Science, pp. 619-633, Springer, Cham, 2022, https://doi.org/10.1007/978-3-319-91875-4_60.

[24] M. Elsayed, M. Reda, A. S. Mashaly and A. S. Amein, "Review on Real-Time Drone Detection Based on Visual Band Electro-Optical (EO) Sensor," *2021 Tenth International Conference on Intelligent Computing and Information Systems (ICICIS)*, Cairo, Egypt, 2021, pp. 57-65, doi: 10.1109/ICICIS52592.2021.9694151.

[25] K. A. Gallagher, *"Harmonic Radar: Theory and Applications to Non-Linear Target*

*Detection, Tracking, Imaging and Classification,"* Ph.D Thesis. The Pennsylvania State University, 2015, [Online]. https://etda.libraries.psu.edu/catalog/27417 (Accessed Date: July 6, 2024).

[26] A. F. Martone, "Forensic Characterization of RF Circuits," Ph.D Thesis, Purdue University, 2007, [Online]. https://engineering.purdue.edu/~ace/thesis/martone/thesis.pdf (Accessed Date: July 6, 2024).

[27] HUAWEI, WLAN Antenna Quick Start, Receiver Sensitivity, Document ID: EDOC1000077015, [Online]. https://support.huawei.com/enterprise/en/doc/EDOC1000077015/bc2e25db/receiver-sensitivity (Accessed Date: July 6, 2024).

[28] Panasonic Industry, PIR Motion Sensor PaPIRs, [Online]. https://industrial.panasonic.com/ww/products/pt/papirs (Accessed Date: July 6, 2024).

[29] Panasonic, PIR Motion Sensor PaPIRs, [Online]. https://www.tme.eu/Document/52c180ac33c503d43640c8b77161fa7d/bltn_eng_papirs.pdf (Accessed Date: July 6, 2024).

[30] DigiKey, Panasonic Electric Works EKMC4607111K, [Online]. https://www.digikey.be/en/products/detail/panasonic-electric-works/EKMC4607111K/10222330 (Accessed Date: July 6, 2024).

[31] M. McNabbon (2020, Jan. 13), *Transformables: Check Out the Pegasus Mini, a Football-Sized Drone that Flies or Drives*, [Online]. https://dronelife.com/2020/01/13/transformables-check-out-the-pegasus-mini-a-football-sized-drone-that-flies-or-drives/ (Accessed Date: July 6, 2024).

# APPENDIX

Table 2. Power received by the antenna of the mini-drone for the lowest frequency and its first harmonic (Figure 4)

| Distance in meters | $P^1_{4,in}$ (dBm) | $P^2_{4,in}$ (dBm) |
|---|---|---|
| 0.1 | 19.7708684 | 2.760176 |
| 0.2 | 7.7296686 | -15.301624 |
| 0.3 | 0.6860182 | -25.867100 |
| 0.4 | -4.3115312 | -33.363424 |
| 0.5 | -8.1879318 | -39.178025 |
| 0.6 | -11.3551816 | -43.928899 |
| 0.7 | -14.0330532 | -47.945707 |
| 0.8 | -16.3527311 | -51.425223 |
| 0.9 | -18.3988320 | -54.494375 |
| 1 | -20.2291316 | -57.239824 |
| 1.1 | -21.8848390 | -59.723385 |
| 1.2 | -23.3963814 | -61.990699 |
| 1.3 | -24.7868657 | -64.076425 |
| 1.4 | -26.0742530 | -66.007506 |
| 1.5 | -27.2727819 | -67.805300 |
| 1.6 | -28.3939309 | -69.487023 |
| 1.7 | -29.4470884 | -71.066760 |
| 1.8 | -30.4400318 | -72.556175 |
| 1.9 | -31.3792756 | -73.965040 |
| 2 | -32.2703314 | -75.301624 |

Table 3. Time to scan CI versus CI's volume (in cubic meters – log10 scale) (Figure 7)

| Volume in $m^3$ (log10) | Human Scanning (sec) | Passive Infrared Sensors (sec) | Proposed (sec) |
|---|---|---|---|
| 2.698970 | 178.5625 | 0 | 31.25 |
| 3.000000 | 357.1250 | 0 | 62.50 |
| 3.176091 | 535.6875 | 0 | 93.75 |
| 3.301030 | 714.2500 | 0 | 125.00 |
| 3.397940 | 892.8125 | 0 | 156.25 |
| 3.477121 | 1071.3750 | 0 | 187.50 |
| 3.544068 | 1249.9375 | 0 | 218.75 |
| 3.602060 | 1428.5000 | 0 | 250.00 |
| 3.653213 | 1607.0625 | 0 | 281.25 |
| 3.698970 | 1785.6250 | 0 | 312.50 |
| 3.875061 | 2678.4375 | 0 | 468.75 |
| 4.000000 | 3571.2500 | 0 | 625.00 |
| 4.096910 | 4464.0625 | 0 | 781.25 |
| 4.176091 | 5356.8750 | 0 | 937.50 |
| 4.243038 | 6249.6875 | 0 | 1093.75 |
| 4.301030 | 7142.5000 | 0 | 1250.00 |
| 4.397940 | 8928.1250 | 0 | 1562.50 |
| 4.477121 | 10713.7500 | 0 | 1875.00 |
| 4.544068 | 12499.3750 | 0 | 2187.50 |
| 4.698970 | 17856.2500 | 0 | 3125.00 |

Table 4. Cost in Euro (log10 scale) of One-Day Scanning versus CI's volume (in cubic meters – log10 scale) (Figure 8(a))

| Volume in $m^3$ (log10) | Human Scanning in Euro (log10) | Passive Infrared Sensors in Euro (log10) | Proposed in Euro (log10) |
|---|---|---|---|
| 2.698970 | 2.484243 | 4.148063 | 3.30103 |
| 3.000000 | 2.491250 | 4.449093 | 3.30103 |
| 3.176091 | 2.498145 | 4.625184 | 3.30103 |
| 3.301030 | 2.504933 | 4.750123 | 3.30103 |
| 3.397940 | 2.511616 | 4.847033 | 3.30103 |
| 3.477121 | 2.518199 | 4.926214 | 3.30103 |
| 3.544068 | 2.524682 | 4.993161 | 3.30103 |
| 3.602060 | 2.531071 | 5.051153 | 3.30103 |
| 3.653213 | 2.537366 | 5.102305 | 3.30103 |
| 3.698970 | 2.543572 | 5.148063 | 3.30103 |
| 3.875061 | 2.573337 | 5.324154 | 3.30103 |
| 4.000000 | 2.601192 | 5.449093 | 3.30103 |
| 4.096910 | 2.627368 | 5.546003 | 3.30103 |
| 4.176091 | 2.652055 | 5.625184 | 3.30103 |
| 4.243038 | 2.675414 | 5.692131 | 3.30103 |
| 4.301030 | 2.697580 | 5.750123 | 3.30103 |
| 4.397940 | 2.738783 | 5.847033 | 3.30103 |
| 4.477121 | 2.776414 | 5.926214 | 3.30103 |
| 4.544068 | 2.811042 | 5.993161 | 3.30103 |
| 4.698970 | 2.900917 | 6.148063 | 3.30103 |

Table 5. Cost in Euro (log10 scale) of One-Year Scanning versus CI's volume (in cubic meters – log10 scale) (Figure 8(b))

| Volume in $m^3$ (log10) | Human Scanning in Euro (log10) | Passive Infrared Sensors in Euro (log10) | Proposed in Euro (log10) |
|---|---|---|---|
| 2.698970 | 3.324370 | 4.148063 | 3.30103 |
| 3.000000 | 3.593380 | 4.449093 | 3.30103 |
| 3.176091 | 3.758251 | 4.625184 | 3.30103 |
| 3.301030 | 3.877469 | 4.750123 | 3.30103 |
| 3.397940 | 3.970910 | 4.847033 | 3.30103 |
| 3.477121 | 4.047763 | 4.926214 | 3.30103 |
| 3.544068 | 4.113040 | 4.993161 | 3.30103 |
| 3.602060 | 4.169774 | 5.051153 | 3.30103 |
| 3.653213 | 4.219947 | 5.102305 | 3.30103 |
| 3.698970 | 4.264918 | 5.148063 | 3.30103 |
| 3.875061 | 4.438643 | 5.324154 | 3.30103 |
| 4.000000 | 4.562394 | 5.449093 | 3.30103 |
| 4.096910 | 4.658590 | 5.546003 | 3.30103 |
| 4.176091 | 4.737294 | 5.625184 | 3.30103 |
| 4.243038 | 4.803900 | 5.692131 | 3.30103 |
| 4.301030 | 4.861636 | 5.750123 | 3.30103 |
| 4.397940 | 4.958188 | 5.847033 | 3.30103 |
| 4.477121 | 5.037130 | 5.926214 | 3.30103 |
| 4.544068 | 5.103906 | 5.993161 | 3.30103 |
| 4.698970 | 5.258500 | 6.148063 | 3.30103 |

**Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)**

The authors equally contributed in the present research, at all stages from the formulation of the problem to the final findings and solution.

**Sources of Funding for Research Presented in a Scientific Article or Scientific Article Itself**

No funding was received for conducting this study.

**Conflict of Interest**

The authors have no conflicts of interest to declare.