การประชุมวิชาการทางวิศวกรรมไฟฟ้า ครั้งที่ 48
The 48th Electrical Engineering Conference (EECON-48)
วันที่ 19-21 พฤศจิกายน 2568 ณ โรงแรมฟูราม่า จังหวัดเชียงใหม่

SDR Based Anti-Drone System on 2.4-GHz ISM band

Raktanwan Poolsuwan[1], Arsit Boonyaprapasorn[2], and Pasu Kaewplung[3,*]

[1,3] Defense Engineering and Technology, Faculty of Engineering, Chulalongkorn University
Phayathai Rd., Pathumwam, Bangkok, Thailand, 10330
[2] Department of Mechanical Engineering, Chulachomklao Royal Military Academy (CRMA)
Suwansorn Rd., Muang, Nakhon-Nayok, 26001 Thailand
6670207921@student.chula.ac.th[1], arsit.bo@crma.ac.th[2], Pasu.K@Chula.ac.th[3,*]

Abstract

This research delineates the design and feasibility of a comprehensive, full-cycle counter-unmanned aerial vehicle (UAV) or drone multi-stage process system leveraging Software-Defined Radio (SDR) platforms. In first process, the detection employs a Frequency Modulated Continuous Wave (FMCW) radar on ISM as carrier frequency for the detection and tracking of aerial targets. This subsystem is designed to ascertain the distance and velocity of incoming objects. The second stage involves the classification of radio frequency (RF) signals. A Convolutional Neural Network (CNNs) is utilized to analyze the control and data transfer signals transmitted between the drone and its operator within the Industrial, Scientific, and Medical (ISM) band (2.4 GHz). The last stage is neutralization of confirmed threats achieved through two electronic countermeasure techniques. The first step is the deployment of a jamming signal to disrupt the command-and-control link in the ISM band (2.4 GHz), effectively isolating the drone from its operator. Concurrently, the system will engage in Global Positioning System (GPS) spoofing within the L1 band by transmitting simulated GPS L1 signal in 1.575-GHz band to confuse drone's position. The system tested with DJI Mini 4K drone with radar cross section of 0.01 m^2 has result as detection range of 20 m with jamming and spoofing range of 50 m in limited transmitted power of 20 dB according to ISM band limitation.

Keywords: Drone, UAV, Anti-drone, SDR, Radar, Jamming, RF-classification

1. Introduction

The rapid proliferation and the technological advancement of Unmanned Aerial Vehicles (UAVs), commonly known as drones, present a significant and evolving challenge to national security across multiple domains, including economic, social, political, and military sectors. The increasing accessibility and the affordability of UAV technology, available in various sizes and configurations, have democratized its use, extending its reach from state actors to non-state entities and individuals. This widespread availability complicates monitoring and control, creating a new threat vector that is difficult to mitigate comprehensively. Recent conflicts, such as those in Ukraine, Gaza, and Myanmar [1]-[3], have demonstrated the potent application of UAVs in modern warfare and asymmetric engagements, highlighting the urgent need for effective anti-drone system [4].

This paper outlines the design and feasibility of an integrated anti-drone system engineered for the surveillance, monitoring, and neutralization of unauthorized drones within high-security zones. The proposed system is intended for deployment by security agencies tasked for the protection of critical infrastructure and areas of national importance. The system's architecture is predicated on a multi-layered approach encompassing detection, classification, and interception. Initially, the system employs radar technology for the detection and localization of small drones. Upon identifying an anomalous object within its operational radius, after detected turn to a classification phase. This utilizes signature analysis to recognize the specific characteristics of the drone's control signal, thereby determining its type, manufacturer, or operational mode. The positional and classification data are then relayed to a central control system for threat assessment and decision-making. The system will execute a jamming by transmitting interference signals on the same frequency band as the drone's command and control link to sever communication with its operator. Subsequently, the system will engage in GPS spoofing, broadcasting counterfeit satellite navigation signals to deceive the drone's guidance system. This research can detect drone of size 0.01 m^2 in 20 m and disrupt all wireless communication both navigation and control in 50 m.

2. Principles and related works

2.1 Anti-drone System

An anti-drone system is engineered to detect, classify, and neutralize unauthorized drone activity within a designated area. Its functionality hinges on three interdependent requirements. Firstly, drone detection involves the acquisition of data, such as RF reflections, emitted RF signals, thermal signatures, or acoustic emissions, utilizing technologies like radar, thermal and visible cameras, or acoustic sensors, each optimized for specific environmental conditions. Secondly, drone classification and identification are critical to mitigate false positives from other aerial objects or environmental noise. This process typically employs advanced techniques like image processing or RF recognition, often integrated with neural networks, to ascertain the drone's type, manufacturer, and size, thereby enabling a comprehensive risk assessment. Finally, drone neutralization, primarily for non-military drones, is

*Corresponding Author

achieved through soft-kill methods. This involves the disruption the drone wireless communication signals, including both control and GPS links, effectively severing the operator's control and rendering the drone inert within the anti-drone system's operational range. [4]-[7]

2.2 Drone Detection with FMCW Radar

FMCW radar (Frequency-Modulated Continuous Wave) determines target range and relative velocity by analyzing the frequency and phase differences between a continuously transmitted, frequency-modulated signal and its reflections shown in Fig 1. This method's continuous monitoring and low power consumption make it well-suited for drone detection, as it provides simultaneous, high-resolution measurements of both parameters. After transmitting signal reflex with a delay t received back to the radar, the two signal mixed by multiplying conjugate within the time domain and the result is intermediate frequency (f_{IF})

$$f_{IF} = \frac{B}{T_c}t + f_0\left(\frac{B}{T_c}(t - \tau) + f_0\right) = \tau\left(\frac{B}{T_c}\right) \quad (1)$$

$$R = \tau\left(\frac{c}{2}\right) = T_c\left(\frac{f_{IF}}{2}\right)\left(\frac{c}{B}\right) \quad (2)$$

$$v = \frac{\lambda\Delta\phi}{(4\pi T_c)} \quad (3)$$

t is the time delay, d is the distance from the object to the detector, and c is the speed of light. and B is the frequency bandwidth used in the system. v is the speed of the object, λ is the wavelength, $\Delta\Phi$ is the angle difference of the received wave, f_{IF} is intermediate frequency and T_c is the time delay between the transmitted and received signal.

[9]-[13] have successfully demonstrated the efficiency of a drone detection system employing Frequency Modulated Continuous Wave (FMCW) radar implemented via SDR. This approach leverages the inherent advantages of SDR technology, including its compact form factor, wide operating frequency range, cost-effectiveness, and high sample rate, all of which are highly conducive to the stringent requirements of anti-drone applications. The programmability and the reconfigurability offered by SDR enables a flexible system design and a rapid adaptation to evolving drone threats and environmental conditions, representing a promising avenue for robust and scalable drone detection solutions.

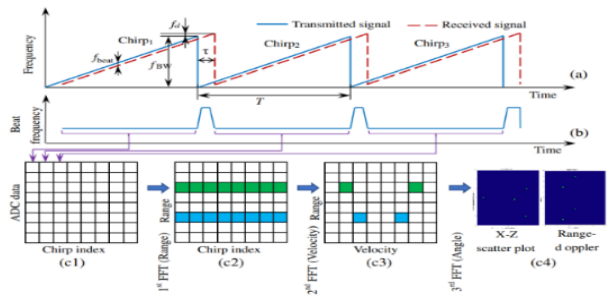

Fig. 1 The basic FMCW radar principle [8]

2.3 RF-Classification

Radio frequency (RF) signal classification for drone detection leverages the unique communication patterns between drones and their controllers. This is often achieved by employing SDRs due to their wide frequency band operation, cost-effectiveness, and high sample rates suitable for anti-drone. Upon signal reception via SDR, the raw RF data is transformed into spectrograms, visual representations of the signal's frequency content over time. These spectrogram images are then analyzed and categorized using CNNs, a deep learning architecture adept at image recognition. [14]-[17] has demonstrated high accuracy, with some research reporting up to 98% classification accuracy. This indicates that CNNs-based spectrogram analysis is reliable drone signal identification in noisy environments.

2.4 Jamming and GPS Spoofing

RF jamming systems are designed to disrupt drone operations by emitting interference signals across the specific frequency bands used for drone control and communication. Commercial drones predominantly utilize bands at 2.4 GHz and 5.6 GHz, although a broader range of 400 MHz to 6 GHz can be employed. There is indicated RF noise with a 10-MHz bandwidth that can effectively interfere with Wi-Fi channels and control communications.

In parallel, GPS spoofing offers another neutralization method. The public L1 channel (1.575 GHz) of GPS is susceptible to artificial signal injections. By transmitting a carefully crafted, more powerful artificial GPS L1 signal, a drone's onboard GPS receiver can be forced to compute an erroneous position, overriding the weak legitimate satellite signals. This manipulation effectively redirects or disorients the drone. Studies, often utilizing commercial Software-Defined Radios (SDRs), [18]-[25] have successfully demonstrated both RF jamming in the (2.4-2.5)-GHz ISM band with varying bandwidths to cover drone communication channels, and GPS jamming and spoofing at the L1 band. The effectiveness of these techniques can be quantitatively assessed through Free Space Path Loss (FSPL) and Received Power calculations.

$$L = 20\log_{10}(d) + 20\log_{10}(f) + 20\log_{10}\left(\frac{4\pi}{c}\right) - G_t - G_r \quad (4)$$

$$P_r = R_t + G_t + G_r - L - L_t - L_r \quad (5)$$

where d is the distance in m, f is the frequency used, c is the speed of light, G_t is the gain of the transmitting antenna, and G_r is the gain of the receiving antenna. P_r is the receiving power, P_t is the transmitting power, G is the antenna gain, L is the loss in the medium, and L_t , L_r are the losses in the transmitting and receiving circuits, respectively.

3. Implementation

3.1 Proposed SDR based anti-drone system

The proposed anti-drone system, centered on SDR technology, integrates three essential functions. Firstly, drone detection is achieved using an SDR, specifically the USRP B200, which serves as a versatile signal generator, transmitter, and receiver. Secondly, the drone identification is performed by processing spectrogram images of drone control signals through CNNs developed with the TensorFlow. This enables robust classification of drone types. Finally, the drone neutralization is accomplished through a combination of RF jamming within the ISM band to disrupt control signals and GPS L1 spoofing, as visually represented in Fig. 2.

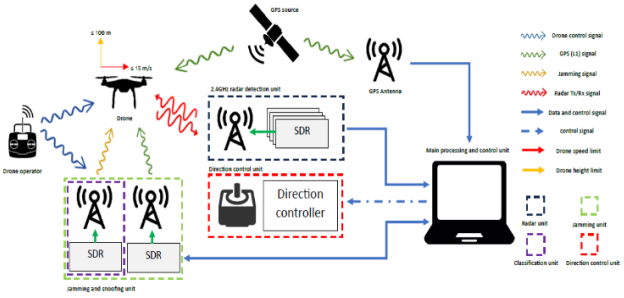

Fig. 2 Proposed anti-drone system concept [26]

3.2 Detection sub-system SDR base radar

[26] Simulations initially predicted a detection range of approximately 70 m for a radar cross-section (RCS) of 0.1 m^2 at a transmit power of 0.1 W. However, for field testing, we tested with a DJI Mini 4K drone, which has a smaller RCS of 0.01 m^2. Consequently, a revised simulation was necessary to reflect this smaller RCS while maintaining other parameters. This updated MATLAB simulation indicated a detection range of approximately 25 m. The simulation also incorporated an antenna gain of 10 dB, a triangular linear chirp signal with 1024 chirps per sweep, and a bandwidth of 14 MHz (ranging from −7 MHz to 7 MHz). The system demonstrated a velocity resolution of 0.5 m/s, as illustrated in Fig. 3 has simulated detection range of 26 m and gr-plasma implements and generated linear frequency-modulated waveform (LFM) to plot range-doppler map for visualize a detection [28].

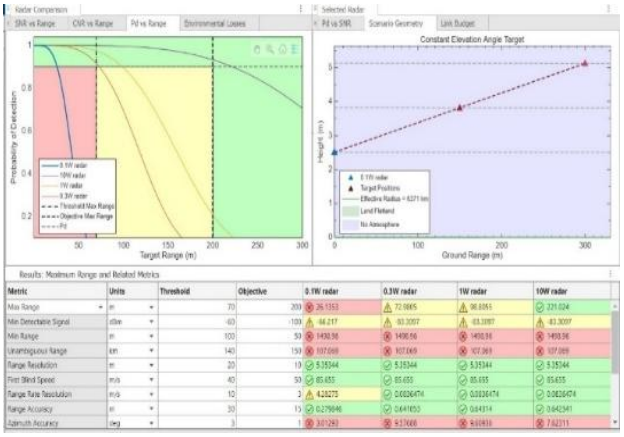

Fig. 3 MATLAB simulated radar with RCS of 0.01 m^2

3.3 SDR Base RF-Classification

This research employs the CNNs model, implemented in Python 3.12 with TensorFlow 2.19, for the classification of drone control radio frequency (RF) signals. CNNs is designed to recognize distinct patterns in power-based spectrograms, which exhibit clear variations across different drone models. The training dataset for the CNN dataset [28],[29] has a sampling rate of 100 MSps and a center frequency of 2.44 GHz shown in Fig. 4 and dataset for DJI Mini 4k captured by SDR shown in Fig. 5. This comprises control signals from various drone models, as well as environmental noise signals within the same frequency band. The objective is to enable the model to accurately differentiate between various types of received RF signals. Through the iterative fine-tuning of program parameters, the aim is to achieve a classification accuracy of at least 80%. The CNNs model is structured as a 1024 x 1221 matrix, representing 1024 frequency bins across 1221 time samples and layers shown in Table 1 .

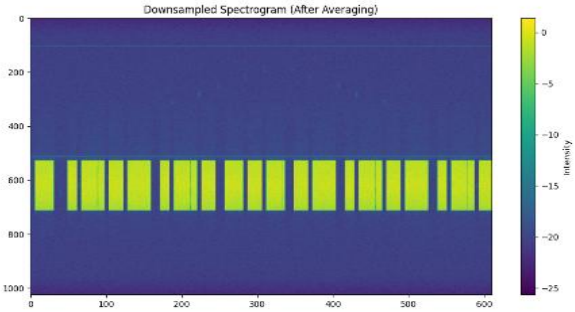

Fig. 4 Example of KU RDR dataset [29]

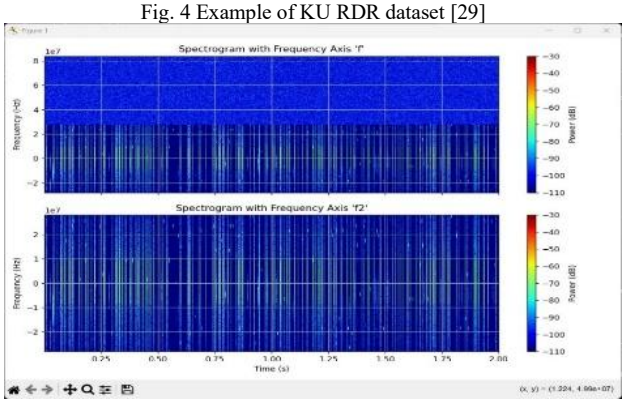

Fig. 5 Spectrogram of DJI Mini 4k RF signal

Table 1. CNNs model description

	Layer	Details
0	Input	spectrogram size 1024 x 1221
1	Conv2D1	32 filters 3 x 3, activation Relu
	Maxpool2D1	Pool size 2 x 2
2	Conv2D2	64 filters 3 x 3, activation Relu
	Maxpool2D2	Pool size 2 x 2
3	Conv2D3	128 filters 3 x 3, activation Relu
	Maxpool2D3	Pool size 2 x 2
Fc	Fully connected	Dense 128, dropout 0.4
		Dense 64, dropout 0.4
SoftMax		Number of classes = 0 - 6

3.4 SDR Base Jamming and GPS Spoofing

The control signal jamming system generates random amplitude and phase interference, mimicking Rayleigh noise to simulate rapid communication disruption. It combines Gaussian noise with random communication signals in Fig. 6 (16-28 MHz bandwidth) and transmits them via SDR using GNU Radio. The output features random signal intensity and frequency, with the combined signal ready for antenna transmission. For a reliable connection, a drone's RF signal-to-noise ratio (SNR) must exceed 0 dB. An SNR below -5 dB indicates a weak signal, resulting in an automatic loss of the connection. The dynamic range for a stable link is between 0 dB and -5 dB. In Fig. 7 show MATLAB simulated of range and SNR with both control and jamming transmitting power of 20 dB in 150 m range.

Satellite positioning signal simulation is performed by generating simulated signals from a The daily GPS broadcast ephemeris file (BRDC) file with GPS-SDR-SIM, which transmits satellite numbers, transmission angles, transmission duration, and power strength to closely resemble signals received from real positioning satellites. The transmitted signal compose of details, including the angular position of each satellite in the area. In Fig. 8 show received GPS simulated signal on GPS tester.

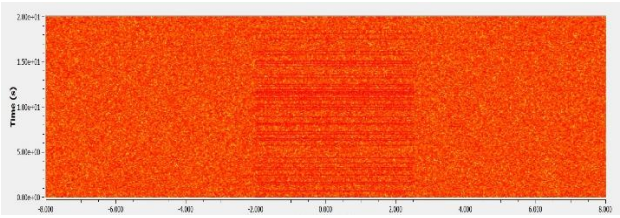

Fig. 6 Simulated signal with gaussian noise use in jamming

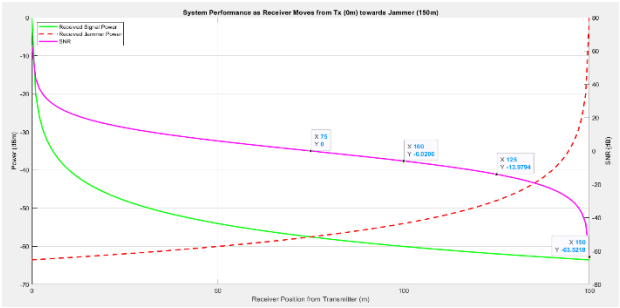

Fig. 7 SNR of received signal and jamming signal in 150 m

Fig. 8 Received GPS simulated signal with random location

3.5 Field test setup

Field tests were conducted on a two-lane road at least 200 m long to define the operational area and range for the prototype, which is expected to have a detection range of at least 20 m and a control jamming signal range of 50 m. The test setup included a main processor (MSI Katana GF76 11UG), an SDR (USRP B200), a radio frequency amplifier (ZX60-V62+, ZX60-33LNR-S), a band pass filter (TAOGLAS BPF.24.01), and antennas (MD24-12 (2.4 GHz) , ANT-20087EB56 (1.575 GHz)), as shown in Fig. 9. The transmitting and receiving antennas were positioned 70 cm above the ground and spaced 1 m apart to help reduce signal reflection from the transmitting antenna.

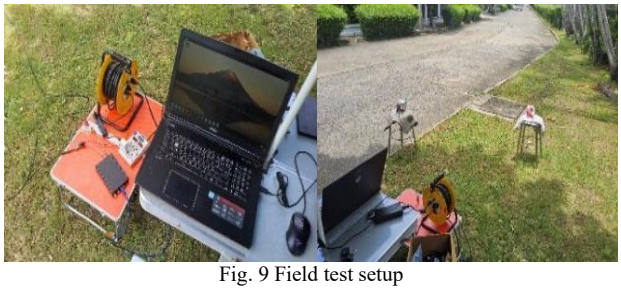

Fig. 9 Field test setup

4. Field test results

4.1 Radar sub-system

The UAV was positioned 50 m away from the prototype, flying at an altitude of 2 m from the ground. It then flew in and out within an area ranging from 1 to 50 m at speeds between 0 and 7.5 m/s. The detection map sets a range of 200 m and speeds from -15 (moving away) to 15 (approaching) m/s. The results were recorded based on the detection range of the drone in increments of 5 m, as shown in Fig 10. The red circles indicate the detectable range and signal intensity: 1 m (-25 dB), 5 m (-30 dB), 10 m (-40 dB), 15 m (-45 dB), and 20 m (-50 dB).

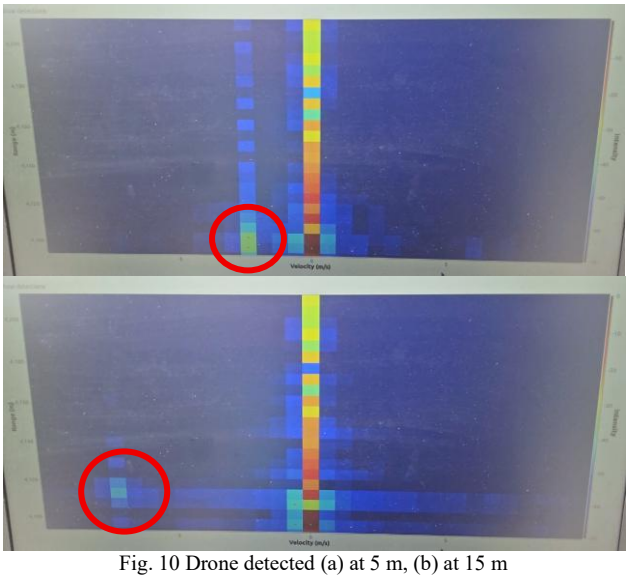

Fig. 10 Drone detected (a) at 5 m, (b) at 15 m

4.2 RF-Classification sub-system

The data was categorized into seven types, labeled 0 through 6, with each category containing 200 samples. These categories are: 0 (DJI Matrice 300), 1 (Frysky), 2 (DJI Mini 4K), 3 (DJI Inspire 2), 4 (DJI Mavic), 5 (DJI Mini 2), and 6 (Background signal), as illustrated by the training examples in Fig. 4. The dataset fed into the model was divided into three parts: 70% for training, 10% for validation, and 20% for testing. The model then classified the data into these seven categories, providing a probability percentage from 0 to 1 for each type, as shown in Fig 11. A probability exceeding 80% for a given category was used as the criterion for subsequent decision-making.

```
esc[1m1/1esc[0m esc[32m====================esc[0mesc[37mesc[0m esc[1m0sesc[0m 236ms/step
esc[1m1/1esc[0m esc[32m====================esc[0mesc[37mesc[0m esc[1m0sesc[0m 256ms/step
Sample 0 Prediction: [[4.2753168e-27 3.5029034e-22 3.7236363e-28 7.1430049e-11 9.9960560e-01
  2.6496823e-08 3.9438382e-04]]
Sample 0 Shape: (1, 1024, 1221, 1), Min: -15.0, Max: 17.775466918945312
Sample 0 Prediction (Percentages):
Class 0: 0.00%
Class 1: 0.00%
Class 2: 0.00%
Class 3: 0.00%
Class 4: 99.96%
Class 5: 0.00%
Class 6: 0.04%
Key of 1 = dict_keys(['__header__', '__version__', '__globals__', 'data_with_label'])
Keys: ('spectrogram', 'label')

esc[1m1/1esc[0m esc[32m====================esc[0mesc[37mesc[0m esc[1m0sesc[0m 140ms/step
esc[1m1/1esc[0m esc[32m====================esc[0mesc[37mesc[0m esc[1m0sesc[0m 160ms/step
Sample 1 Prediction: [[6.3499137e-08 1.1364733e-06 6.2682200e-04 9.4022274e-01 5.8856238e-02
  2.8036206e-04 1.2540402e-05]]
Sample 1 Shape: (1, 1024, 1221, 1), Min: -15.0, Max: 13.549842834472656
Sample 1 Prediction (Percentages):
Class 0: 0.00%
Class 1: 0.00%
Class 2: 0.06%
Class 3: 94.02%
Class 4: 5.89%
Class 5: 0.03%
Class 6: 0.00%
Key of 2 = dict_keys(['__header__', '__version__', '__globals__', 'data_with_label'])
Keys: ('spectrogram', 'label')
```

Fig. 11 RF-Classification testing with data samples

4.3 Jamming sub-system

After transmitting 2.45-GHz interference, the UAV operator, positioned at least 150 m away, flew the drone incrementally closer to the prototype, assessing control at 5-m intervals. The RC screen showed green signal from 75-200 m. Between 75-55 m, it turned yellow with a "Drone has interference" message (Fig. 12(a)) , causing delayed control. Below 55 m, the UAV completely lost control, the screen turned red with "Drone loses connected to remote" (Fig. 12(b)). This indicates the system's effective jamming range is at least 50 m.

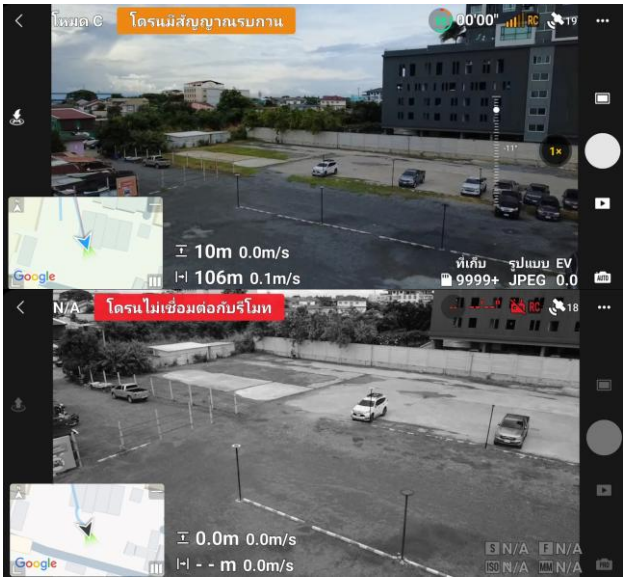

Fig. 12 Drone status (a) has interference, (b) loses connected to remote

4.4 GPS Spoofing sub-system

The GPS Spoofing system was tested with a drone flying in a circular path, starting 100 m from the prototype and incrementally moving 5 m closer and simulating GPS signal shown in Fig 13 (a) and received by GPS receiver in Fig 13 (b). Normally, the control screen would show reception from 16-20 satellites (top-right corner). However, as the drone approached 20-50 m, the number of satellites dropped to 6-8, and the UAV's position on the screen became static. After at least 3 seconds, the drone's position appeared as a large green circle, indicating an inability to accurately determine its location (Fig 14). When the UAV was less than 15 m from the prototype, the control screen showed no satellite signal reception at all (Fig 15).

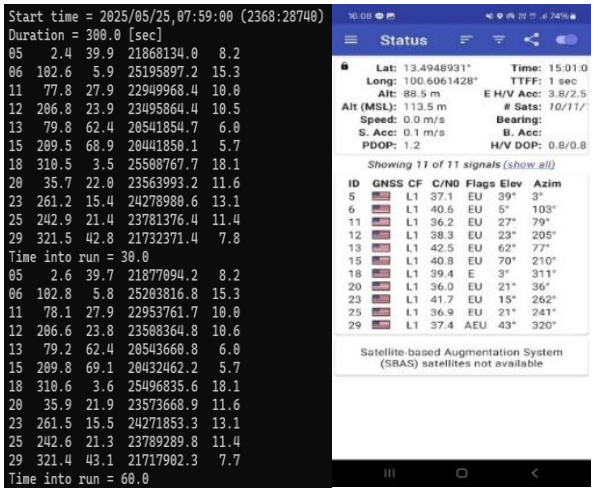

Fig. 13 GPS signal details of (a) Simulated GPS signal, (b) GPS spoofing in GPS receiver

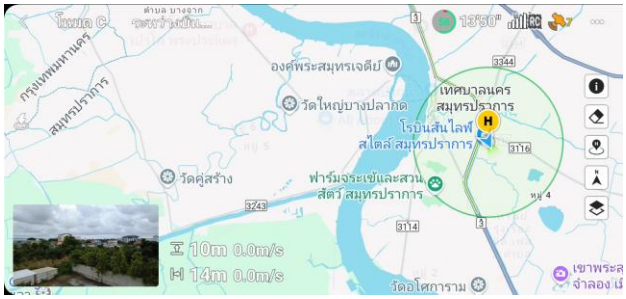

Fig. 14 Drone confusing on GPS signal

Fig. 15 . Drone lost GPS signal

4.5 Anti-drone system specification

When integrating all four sub-systems into a single prototype, the operational range of the overall system is limited by the sub-system with the shortest range. This constraint is specifically due to the radio detection system, which has an operational range of 20 m. Details regarding the operational ranges of each sub-system are provided in Table 2.

Table 2. Proposed anti-drone system specification

Functionality	Sub-system	Range (m)
Detection	Radar RCS (0.01 / 0.05 / 1.0 / >1.0)	20 / 30 / 90 / 200
Classification	RF classification	100
Neutralization	RF Jamming	50
	GPS spoofing	50
Anti-drone prototype		20

5. Conclusions

This research successfully presents the design, implementation, and testing of a prototype anti-drone system, leveraging a SDR USRP B200 as the primary transceiver across all subsystems. Developed using GNU Radio and Python. Field test results demonstrated the radar's ability to detect drones with a 0.01 RCS at 20 m, the classification system achieving 80% accuracy at a 100 m signal range, and both jamming and spoofing functionalities effectively disrupting drones communication and navigation at a minimum range of 50 m. Consequently, the prototype successfully demonstrated the operational capability of all four subsystems within a 20-m radius limited by detection sub-system, fulfilling the research objectives and establishing a foundation for future performance enhancements.

6. Future work

In the future, we will work on adding more drone RF data and including RF frequency range more than ISM band to increase prototype capacity to work with RC control drone (FPV drone) with realistic testing environment. We are going to test with multiple drone models, sizes and manufactures to verify the results then use the results to optimize and modify the system for better performance in the future requirements.

7. Acknowledgments

This research is part of the defense engineering and technology, Chulalongkorn university, Thailand. This research is funded by Ratchadapisek Somphot Fund for Center of Excellence in Artificial Intelligence, Machine Learning and Smart Grid Technology and funded by Defence Technology Institute.

References

[1] Bender and J. Staggs, "Leveling the Playing Field: Equipping Ukrainian Freedom Fighters with Low-Cost Drone Detection Capabilities," in 2023 15th International Conference on Cyber Conflict: Meeting Reality (CyCon), Tallinn, Estonia, 2023, pp. 287-312, doi: 10.23919/CyCon58705.2023.10181421.

[2] A. Kajander, "Russian Invasion of Ukraine 2022: Time to Reconsider Small Drones?," in 2023 15th International Conference on Cyber Conflict: Meeting Reality (CyCon), 30 May-2 June 2023 2023, pp. 313-327, doi: 10.23919/CyCon58705.2023.10181494.

[3] Kaniewski, "Hamas: Learning about drone warfare from the war in Ukraine," DW. [Online]. Available: https://www.dw.com/en/hamas- learning-about-drone-warfare-from-the-war-in-ukraine/a-67169578, Feb. 2024.

[4] S. Park, H. T. Kim, S. Lee, H. Joo, and H. Kim, "Survey on Anti-Drone Systems: Components, Designs, and Challenges," IEEE Access, vol. 9, pp. 42635-42659, 2021, doi: 10.1109/ACCESS.2021.3065926.

[5] S. Winkler, S. Zeadally, and K. Evans, "Privacy and Civilian Drone Use: The Need for Further Regulation," IEEE Security & Privacy, vol. 16, no. 5, pp. 72-80, 2018, doi: 10.1109/MSP.2018.3761721.

[6] S. Pisa et al., "Evaluating the radar cross section of the commercial IRIS drone for anti-drone passive radar source selection," in 2018 22nd International Microwave and Radar Conference (MIKON), 14-17 May 2018 2018, pp. 699-703, doi: 10.23919/MIKON.2018.8405330.

[7] Y. Mekdad et al., "Exploring Jamming and Hijacking Attacks for Micro Aerial Drones," ICC 2024 - IEEE International Conference on Communications, Denver, CO, USA, 2024, pp. 1939-1944, doi: 10.1109/ICC51166.2024.10623000.

[8] Long, Ningbo & Wang, Kaiwei & Cheng, Ruiqi & Yang, Kailun & Weijian, Hu & Bai, Jian. (2019). Assisting the visually impaired: Multitarget warning through millimeter wave radar and RGB-depth sensors. Journal of Electronic Imaging. 28. 1. 10.1117/1.JEI.28.1.013028.

[9] S. Deshmukh and K. J. Vinoy, "Design and Development of RADAR for detection of Drones and UAVs," in 2022 IEEE Microwaves, Antennas, and Propagation Conference (MAPCON), 12-16 Dec. 2022 2022, pp. 1714-1719, doi: 10.1109/MAPCON56011.2022.10047163.

[10] S. G. Gutierrez, et al, "Design of a low-cost continuous-wave Doppler RADAR operating at 2.4 GHz," in 2021 Argentine Conference on Electronics – CAE, pp. 19-24, 2021.

[11] D. Santos, P. Sebastião, and N. Souto, "Low-cost SDR based FMCW radar for UAV localization," in 2019 22nd International Symposium on Wireless Personal Multimedia Communications (WPMC), 24-27 Nov. 2019 2019, pp. 1-6, doi: 10.1109/WPMC48795.2019.9096117.

[12] Y. K. Kwag, I. S. Woo, H. Y. Kwak, and Y. H. Jung, "Multi-mode SDR radar platform for small air-vehicle Drone detection," in 2016

CIE International Conference on Radar (RADAR), 10-13 Oct. 2016 2016, pp. 1-4, doi: 10.1109/RADAR.2016.8059254.
[13] P. Janpangngern et al., "High-Resolution FMCW Radar for Small UAV Detection Using GNU Software-Defined Radio," IEEE Access, vol. 13, pp. 86396-86412, 2025, doi: 10.1109/ACCESS.2025.3570635.
[14] Garvanov, D. Kanev, M. Garvanova, and V. Ivanov, "Drone Detection Approach Based on Radio Frequency Detector," in 2023 International Conference Automatics and Informatics (ICAI), 5-7 Oct. 2023 2023, pp. 230-234, doi: 10.1109/ICAI58806.2023.10339072.
[15] K. Pärlin, T. Riihonen, G. Karm, and M. Turunen, "Jamming and Classification of Drones Using Full-Duplex Radios and Deep Learning," in 2020 IEEE 31st Annual International Symposium on Personal, Indoor and Mobile Radio Communications, 31 Aug.-3 Sept. 2020 2020, pp. 1-5, doi: 10.1109/PIMRC48278.2020.9217351.
[16] C. Xue, T. Li, Y. Li, Y. Ruan and R. Zhang, "Radio Frequency Identification for Drones Using Spectrogram and CNN," GLOBECOM 2022 - 2022 IEEE Global Communications Conference, Rio de Janeiro, Brazil, 2022, pp. 4564-4569, doi: 10.1109/GLOBECOM48099.2022. 10000823.
[17] D. I. Noh et al., "Signal Preprocessing Technique With Noise-Tolerant for RF-Based UAV Signal Classification," IEEE Access, vol. 10, pp. 134785-134798, 2022, doi: 10.1109/ACCESS.2022.3232036.
[18] T. Multerer et al., "Low-cost jamming system against small drones using a 3D MIMO radar based tracking," in 2017 European Radar Conference (EURAD), 11-13 Oct. 2017 2017, pp. 299-302, doi: 10.23919/EURAD.2017.8249206.
[19] J. Gordon, V. Kraj, J. H. Hwang and A. Raja, "A Security Assessment for Consumer WiFi Drones," 2019 IEEE International Conference on Industrial Internet (ICII), Orlando, FL, USA, 2019, pp. 1-5, doi: 10.1109/ICII.2019.00011.
[20] L. Chiper, A. Martian, D. I. Muscalu, C. Vladeanu, and I. Marghescu, "Aerial Drone Defense System based on Software Defined Radio Platforms," in 2022 14th International Conference on Communications (COMM), 16-18 June 2022 2022, pp. 1-4, doi: 10.1109/COMM54429.2022.9817314.
[21] R. Ferreira, J. Gaspar, P. Sebastião, and N. Souto, "A Software Defined Radio Based Anti-UAV Mobile System with Jamming and Spoofing Capabilities," Sensors, vol. 22, p. 1487, 02/15 2022, doi: 10.3390/s22041487.
[22] S. Deshmukh and V. Sharma, "An SDR-based anti-drone system with Detection, Tracking, Jamming, and Spoofing Capabilities," in 2022 IEEE Microwaves, Antennas, and Propagation Conference (MAPCON), 12-16 Dec. 2022, pp. 388-393, doi: 10.1109/MAPCON56011.2022. 10046968.
[23] R. Ferreira, J. Gaspar, P. Sebastião, and N. Souto, "A Software Defined Radio Based Anti-UAV Mobile System with Jamming and Spoofing Capabilities," Sensors, vol. 22, p. 1487, 02/15 2022, doi: 10.3390/s22041487.
[24] M. Ezuma, F. Erden, C. K. Anjinappa, O. Ozdemir, and I. Guvenc, ``Drone remote controller RF signal dataset," Tech. Rep., 2020, doi: 10.21227/ss99-8d56.
[25] B. W. Parkinson, P. Enge, P. Axelrad, and J. J. Spilker, Jr., Global Positioning System: Theory and Applications, vol. 2. Reston, VI, USA: Amer. Inst. Aeronaut. Astronaut., 1996.
[26] R. Poolsuwan, A. Boonyaprapasorn and P. Kaewplung, "SDR Based Anti-Drone System with 2.4GHz," 2025 27th International Conference on Advanced Communications Technology (ICACT), Pyeong Chang, Korea, Republic of, 2025, pp. 31-35, doi: 10.23919/ICACT63878.2025.10936779.
[27] S. Flandermeyer, R. Mattingly, and J. Metcalf, "gr-plasma: A New GNU Radio-based Tool for Software-defined Radar," Proceedings of the GNU Radio Conference, vol. 7, no. 1, 2022-09-25 2022. [Online]. Available: https://pubs.gnuradio.org/index.php/grcon/article/view/121.
[28] M. Mokhtari, J. Bajčetić, B. Sazdić-Jotić and B. Pavlović, "RF-based drone detection and classification system using convolutional neural network," 2021 29th Telecommunications Forum (TELFOR), Belgrade, Serbia, 2021, pp. 1-4, doi: 10.1109/TELFOR52709.2021.9653332.
[29] S. Basak, S. Pollin, and B. Scheers, "Drone Detection and Classification using Artificial Intelligence based RF Sensing," Detectie en classificatie van drones met behulp van kunstmatige intelligentie op basis van RF-detectie, 2023.

Raktawan Poolsuwan received B.S. degree in the electrical energy engineering, KMITL, Thailand in 2020 and currently pursuing an M.S. degree in defense engineering and technology with Chulalongkorn University, Thailand. His current research interest includes the design and application of RF integrated circuit, wireless communication, drone, and anti-drone technology.

ARSIT BOONYAPRAPASORN received the B.S. degree in mechanical engineering from the King Mongkut's University of Technology (KMUTT), Thailand, in 1998, and the M.S. degree in systems and control engineering and the Ph.D. degree in mechanical engineering from Case Western Reserve University, Cleveland, OH, USA, in 2003 and 2009, respectively. Since then, he has been a Lecturer with the Chulachomklao Royal Military Academy, Nakhon Nayok, Thailand. His research interests include nonlinear control and robotics, with a specific focus on nonlinear feedback control and its application in biological systems, lab-on-chips, and climbing robots

PASU KAEWPLUNG was born in Bangkok, Thailand, in December 1971. He received the B.S. and M.S. degrees in electrical engineering from Yokohama National University, Yokohama, Japan, in 1996 and 1998, respectively, and the Ph.D. degree in electrical engineering from Chulalongkorn University, in 2003. From April 1998 to March 2000, he has conducted research with the Research Center for Advanced Science and Technology (RCAST), The University of Tokyo, Japan. He is currently an Associate Professor with the Department of Electrical Engineering, Faculty of Engineering, Chulalongkorn University. His research activities have been devoted to optical access technology, optical fiber transmission systems, dispersion management, and the applications ofnonlinear optical effects.