

SDR Based Anti-Drone System with 2.4GHz

Raktanwan Poolsuwan*, Arsit Boonyaprapasorn**, Pasu Kaewplung ***

*, *** Defense Engineering and Technology, Faculty of Engineering, Chulalongkorn University
Phayathai Rd., Pathumwam, Bangkok, Thailand, 10330

** Department of Mechanical Engineering, Chulachomklao Royal Military Academy (CRMA)
Suwansorn Rd., Muang, Nakhon-Nayok, 26001 Thailand

6670207921@student.chula.ac.th*, arsit.bo@crma.ac.th**, Pasu.K@Chula.ac.th***

Abstract— This paper studied the feasibility of an anti-drone system with a full cycle of operation based on commercial Software Defined Radio (SDR). This proposed system will consist of a detection system with Frequency Modulated Continuous Wave (FMCW) used for drone detection by measuring position, direction, and speed to identify incoming objects. The second process is Radio Frequency classification (RF-classification) using Convolutional Neural Networks (CNNs) on the control signal emitted by both the drone and its operator to classify the type of received signal in the ISM band widely used in commercial drones. The last process is Jamming the ISM band control signal using a highly transmitted power jamming signal to prevent a drone from being recognized and controlled by its operator and spoofing the Global Positioning System (GPS) in the L1 band commonly used in a non-military application for drone neutralization. In the future, the proposed system design will be tested in various possible environments and situations so that the test results can be used for further improvements and corrections.

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

I. INTRODUCTION

Nowadays, rapid changes in technology have a negative effect on many sectors around the globe such as economic, social, political, and military sectors. The impact of technological change may pose a new type of threat to national security that many countries should be aware of. A kind of technology threatening national security is to use of an unmanned aerial vehicle (UAV), commonly known as a drone. It has been found that unmanned aerial vehicles or drone technology can be used in a wider variety of activities and applications. such as events that occurred in The Russian-Ukrainian war, the Gaza conflict, and the fighting in Myanmar [1]-[3]. Along with this technology has a reduced price. There are many types and sizes of unmanned aerial vehicles to choose from. It is accessible to both the public and small organizations. This makes controlling and monitoring risks arising from this type of technology difficult. Currently, risks that may arise from a drone are still difficult to take care of and prevent thoroughly [4].

The goal of this paper is to design and evaluate the feasibility of an anti-drone system that can be used to oversee, monitor, and prevent dangers from drones in high-security areas or locations. To be appropriate in development and use for security agencies. which is responsible for taking care of and

protecting the areas or places that are important to national security This system will be developed to have the ability to detect small, unmanned aircraft by using detection and location technology with radio waves or radar. After determining the location of the abnormality within the radius of the system radio wave aircraft control signal pattern recognition technology. So that the system can recognize the type, manufacturer, or mode of operation of the unmanned aircraft and take the information from the location and classification of the aircraft to be processed in the central control system. to decide on the next step of dealing with but if the central control system decides to intercept and restrain the unmanned aircraft The system will command interference in the same frequency range as the frequency used to control the air operator's aircraft. to stop commands from owner-controller Then command a satellite or artificial GPS positioning signal to make this system capable of deceiving and controlling this unmanned aerial vehicle in the desired direction.

II. PRINCIPLE AND RELATED WORKS

A. Drone

Drones are valuable tools due to their multi-functionality with advanced sensors and cameras with the potential to present security threats such as surveillance, smuggling, and risk with important infrastructure. we can use to specification as a baseline for commercial drones that we expect to detect in a real situation with a height limit of 122 meters and a speed that does not exceed 44.7 meters per second following the regulation with ISM band (2.4/5.6GHz) [5]. [6] showed an average size drone has a Radar Cross Section (RCS) between 0.1 – 1 sqm. measured by radar with frequency of 2 - 4 GHz. The drone specification used in this research is shown below.

- Height <100m
- Speed 10-30 m/s
- Radar Cross section minimum 0.1 sqm.
- Weight <30 kg

B. Anti-drone System

Anti-drone system is a system that is designed to detect, monitor, and prevent any drone from unauthorized activity in its responsible area. It has 3 main requirements shown in the figure. 1. First is drone detection by collects data that is visible or emitted by a drone via RF reflection, RF signal, heat, sound,

etc. This can be done with many methods like radar, thermos and visible cameras, and acoustic sensors but each method has its suitable scenario. Second, drone classification and identification are crucial because the detection process can give fault data with other flying objects or environment noise. Therefore, the system needs to be able to classify drones and give a confirmation. Currently, most of this process uses image processing or RF recognition with a neural network that gives an estimated possibility of drone type, manufacturer, and size. These data can be used to estimate the risk from that drone and determination for the last process. Third is drone neutralization which can separate in 2 ways hard and soft kills that are suitable for non-military drones by interrupting wireless communication signals for both controlling and GPS communication hence preventing drone operators from further interacting with the drone making that drone no longer a threat to the area within anti-drone system coverage. [4], [7]

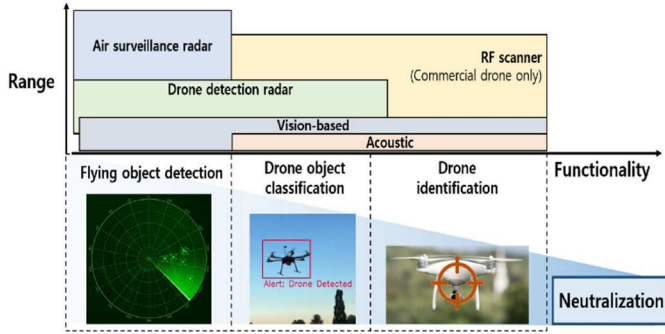


Figure 1. Anti-drone methods with functionality and range [4]

C. Drone Detection with FMCW Radar

FMCW radar (Frequency-Modulated Continuous Wave) works by transmitting continuous modulated frequency signal and comparing different in receive signals that reflex from a target in the antenna coverage to measure its range and relative velocity as shown in the figure 2. This type of radar can measure and monitor its target continuously with lower transmitted power. Therefore, FMCW is reasonable to use for drone detection. FMCW signal can measure for target range and relative velocity in relation below.

$$f(t) = f_0 + \left(\frac{B}{T_c}\right)t \quad (1)$$

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})

$$f_{IF} = \frac{B}{T_c}t + f_0 \left(\frac{B}{T_c}(t - \tau) + f_0\right) = \tau \left(\frac{B}{T_c}\right) \quad (2)$$

$$R = \tau \left(\frac{c}{2}\right) = T_c \left(\frac{f_{IF}}{2}\right) \left(\frac{c}{B}\right) \quad (3)$$

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

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.

Angle of arrival (AOA) is measured by using multiple receive antennas at least 2 and compare time and phase different of receive signal in each antenna by relation show below.

$$\Delta \phi = \frac{2\pi \Delta d}{\lambda} \quad (5)$$

$$\theta = \arcsin\left(\frac{\lambda \Delta \phi}{2\pi l}\right) \quad (6)$$

$\Delta \phi$ is the angular difference of the received waves, Δd is the distance between the receiving antennas, θ is the direction angle of the object with respect to the back beam of the system, and λ is the wavelength.

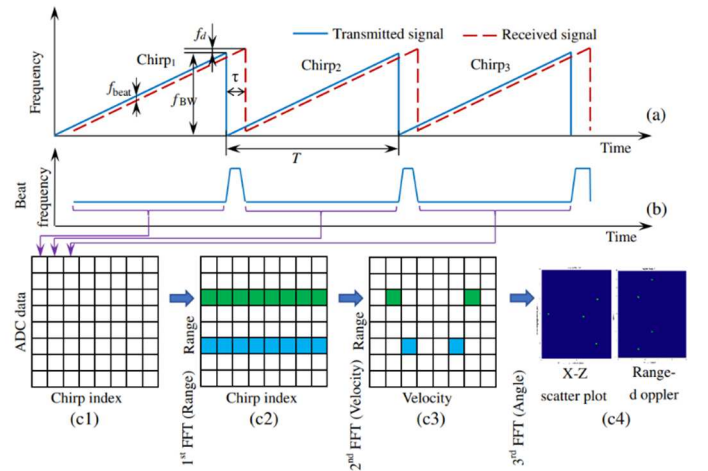
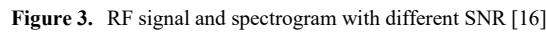


Figure 2. The basic FMCW radar principle [8]

[9]-[12] proposed and tested a drone detection system with FMCW radar based on SDR and showed promising results. SDR is a compact programable radio transceiver with operates in a wide range of frequencies, has low cost, and high sample rate that matches anti-drone requirements.

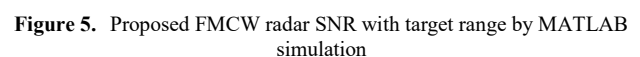
D. RF-Classification

Radio signals classification using RF signals between the drone and the controller to process and analyse with SDR that it allows a wide range of frequency bands. After receiving the signal, the signals will be processed to spectrogram and utilizing CNN to recognize and categorize spectrogram image data shown in figure 3. [1],[13]-[15] using commercial SDR to perform signal processing and detection and [16] research and develop a drone signal classification with CNN and power-base spectrogram with an accuracy of 98% with signal to noise ratio (SNR) of -15 dB



The proposed anti-drone system must fulfill all 3 requirements to efficiently prevent unauthorized drones from it intend target. This can be done by combining sub-systems of FMCW radar for drone detection based on SDR (USRP B210), RF-classification using CNN neural network, and

The radio equipment proposed in this research uses an SDR (USRP B210) as the source of the radar signal that generated and modulated the signal with GNU radio (public signal processing software) so that it can be separated from the external radio signal in the same frequency range. In this research, the 2.4 GHz ISM band was selected as FMCW chirp carrier frequency with bandwidth 28 MHz, the pulse repetition frequency (PRF) is 1400, transmit and receive antenna gain of 8, 6 dBi with total system loss of 12 dB used to detect objects with RCS 0.1 sqm. This parameter is used to calculate the feasibility of FMCW in MATLAB (software for numeric computing and implementation of algorithms) simulation and is shown in Figure 5 and 6. From the simulation, the maximum range of this configuration is 70 meters in an ideal environment. Since the SDR, cannot transmit at high power. Therefore, on the transmission side, an additional power amplifier is required and an antenna with high gain and a wide angle of wave propagation is selected, where the main beam is directional.



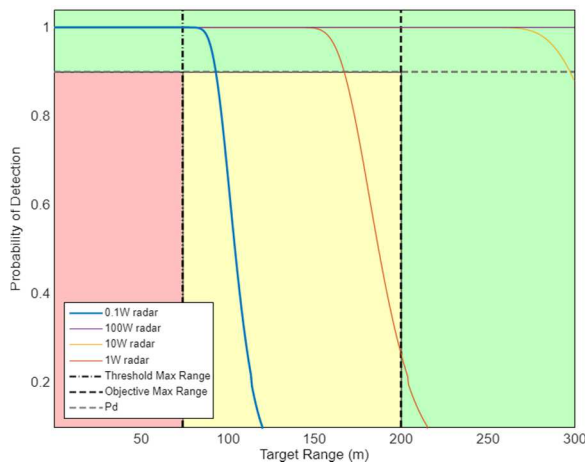


Figure 6. Proposed FMCW radar probability of detection with MATLAB simulation

B. SDR Base RF-Classification

The radio signal classification system is an application of CNNs artificial intelligence network to arrange layers of networks together to train and memorize the power-based spectrogram pattern of control signals used for controlling drones. The RF classification is trained on a data set of drone control signals from different manufacturers and sizes [21] as shown in Figure 7. It helps sort out the types of detected objects. The program of this system receives the controlling radio signal of drones by receiving RF signal with SDR installed with the ISM band antenna to receive the control signals and through the frequency filter. After receiving, it is recorded and sent to generate power-based spectrograms to use in CNNs network for drone evaluation and classification. The system processes and provides the estimated possibility for each type of drone. The possibility values obtained from this sub-system will be used in decision-making for Jamming and GPS Spoofing sub-system.

Description	Value
Number of drone controllers	15
Sampling frequency	20 GHz
Center frequency	2.4 GHz
Number of signals/drone RC	1000
Number of samples/signal	5 million
Time duration/signal	0.25 ms
Average data size/signal	7 MB
Dataset size	124 GB
Data format	.mat

Figure 7. Drone signal dataset [16][21]

C. SDR Base Jamming and GPS Spoofing

This sub-system combined a Jamming system that generated and transmitted interference noise signals on a 2.4GHz ISM band with (Amplitude modulation) AM modulation of 10-20MHz bandwidth that is sufficient for jamming a channel of a drone's control communication and GPS spoofing system. Artificial GPS signals are generated with GPS data from the daily GPS broadcast ephemeris file (brdc) and are publicized by NASA's Global Navigation Satellite System (GNSS) data. This sub-system used SDR (Adam Pluto) for each signal

transmitted and received programmed by GNU radio and python to work on the signal processing process. Jamming and spoofing succession is dependent on an interference signal to overpower the original signal source that the drone receiver antenna received. This can be calculated by formulas (7) and (8) show relation of received power with range from jamming unit in Figure 8. Within 200 meters from the system, generated jamming and GPS spoofing signals have outpowered the drone original signal (GPS required a minimum -130 dB for acquisition) at -45 dB for 2.4GHz ISM band and -120 dB for GPS L1 communication.

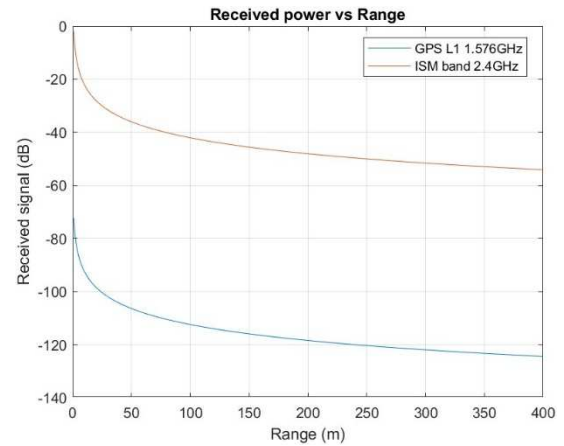


Figure 8. GPS L1 and 2.4GHz signals received power with a range from jamming and GPS spoofing sub-systems.

TABLE 1. PROPOSED ANTI-DRONE SPECIFICATION

Sub-systems	Equipment	Details	Range (m)
FMCW radar	SDR (USRP B210) 2.4GHz antenna	Antennas - Tx gain 8 dB - Rx gain 6 dB	70 (ideal)
Classification	SDR (Adam Pluto) 2.4GHz antenna	CNNs with Power-based spectrogram	> 200 (FSPL)
Jamming	SDR (Adam Pluto) 2.4GHz antenna	Jamming at 2.4GHz, AM, 10-20MHz BW	>200 (Tx 20 dB)
GPS Spoofing	SDR (Adam Pluto) GPS L1 antenna	Spoofing at 1575.42MHz, GPS L1	>200 (Tx 20 dB)

IV. CONCLUSIONS AND FUTURE WORK

The simulation and calculations show this proposed SDR base anti-drone has the potential to monitor and prevent unauthorized drones' activity in the 70 meters coverage area with FMCW radar operate by SDR USRP B210. The classification and neutralization sub-systems operate with SDR Adam Pluto transmitted power of 20 dB is sufficient for a minimum of 200 meters that has more range than the detection sub-system hence this anti-drone is capable of interrupting unauthorized drones that incoming and outgoing from the detect coverage area to increase a probability of successful

intercept them. The specification of this proposed system is shown in Table 1. In the future, we will work on field tests with the proposed configuration and verify the results to optimize and modify the system for better performance in multiple scenarios and configuration.

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.JEL.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] 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.
- [14] K. Pärilä, 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.
- [15] 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.
- [16] 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.
- [17] 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.
- [18] 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.
- [19] L. Chiper, A. Martian, D. I. Muscalu, C. Vlădeanu, 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.
- [20] 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.
- [21] 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.
- [22] 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.



Raktawan Poolsuwan received B.S. degree in the electrical energy engineering, King Mongkut's Institute of Technology Ladkrabang, 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 (RCAT), 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 of nonlinear optical effects.