Journal of
Advancements in Robotics

ISSN: 2455-1872
Volume 11, Issue 2, 2024
May–August
DOI (Journal): 10.37591/JoARB

STM JOURNALS

https://journals.stmjournals.com/joarb

Review JoARB

Guardian of the Sky: Drone Detection and Jamming Technology

Pradyumna Krishna Chopade[1,*], Anuja Gopal Bhate[1], Himanshu Ganesh Mhade[1], Hemangi Navare[2]

Abstract

India has reported remarkable growth in drones in the past ten years for both commercial and defense uses that led to extremely intricate problems. Systems operate as the major onset of the risks involved that might be associated with drone operations. This article provides a comprehensive evaluation of counter-drone systems, with a particular focus on two fundamental aspects: radar targeting, tracking, and other technologies. The main objective of the study is to examine the specific features and worth of radar detection as well as radio frequency jamming warrants. In the layout of drone detection, it is impossible to have a better instrument than radar-based detection systems to spot and track a drone. Such systems artfully exploit modern technologies to detect drones via their size, speed, and altitude, so being able to have real-time data is helpful in proper intervention. The present article focuses on the most frequently applied radar systems to gain a deeper insight into their principles of operation and their performance under the different conditions. Furthermore, a combination of radar systems with other detection methods like acoustic and optical sensors is scrutinized to improve the precision and cogency of detection. As opposed to this, radio frequency jamming is a method of preventing drones from transmitting and receiving signals. The performances of these instruments against the particular frequencies that drones exploit for their employment, such as Wi-Fi and radio frequencies are measured. Through the blending of radar-based detection with radio frequency jamming, this write-up proposes the strategic tips for producing effective anti-drone techniques. Concisely, the presented research gives evidence that helps authorities make decisions that protect the country and also cultivate the enable use of drones for lawful purposes.

Keywords: Radar, radiofrequency, low-cost vs. high-cost drones, rf jamming, security threats, regulatory and legal considerations, counter drone systems, security and public safety, low-cost UAV countermeasures

***Author for Correspondence**
Pradyumna Krishna Chopade
E-mail: pradyumnachopade@gmail.com

[1]Student, Department of Electronics and Telecommunication, Sinhgad College of Engineering (affiliated to Savitribai Phule Pune University), Pune, Maharashtra, India
[2]Professor, Department of Electronics and Telecommunication, Sinhgad College of Engineering (affiliated to Savitribai Phule Pune University), Pune, Maharashtra, India

Received Date: April 24, 2024
Accepted Date: May 24, 2024
Published Date: July 10, 2024

Citation: Pradyumna Krishna Chopade, Anuja Gopal Bhate, Himanshu Ganesh Mhade, Hemangi Navare. Guardian of the Sky: Drone Detection and Jamming Technology. Journal of Advancements in Robotics. 2024; 11(2): 19–25p.

INTRODUCTION

The use of unmanned aerial vehicles (UAVs), also known as drones, has seen a remarkable surge in recent years. These aircraft are engineered to function autonomously, dispensing with the necessity for a human pilot aboard. The term "Unmanned Aerial System" (UAS) is often used interchangeably with UAV, but it encompasses a wider range of components beyond just the drone itself. A UAS includes the ground control station where the pilot operates the drone remotely, the communication channels for sending commands and receiving data, and all the necessary hardware and equipment that enable the drone to function properly.

Drones come in various designs and configurations. While some resemble traditional airplanes, the more common types are multicopters, such as quadcopters, hexacopters, and octocopters. These multirotor configurations provide enhanced versatility and maneuvering capabilities, rendering them appropriate for a diverse array of applications [1].

Currently, there is a growing trend towards smaller UAVs that can operate at lower speeds and navigate through urban environments more effectively. Drones have proven to be incredibly valuable in numerous fields, including aerial photography, traffic monitoring, disaster response, precision agriculture, and industrial inspections. Their ability to access hard-to-reach areas and provide real-time data has made them an indispensable tool in many industries [2].

However, alongside the beneficial applications of drones, there has been an increase in their use for malicious purposes. Drones can pose significant risks in sensitive locations such as airports, stadiums, and urban areas, where they can cause considerable damage. They can be used for espionage, smuggling illegal goods across borders, or even delivering contraband into prisons. Other potential targets include private properties, government facilities, important events, and commercial and industrial sites, with nuclear power plants being of particular concern [3].

The rising threat of malicious drone activities has become a major motivation for developing countermeasures. The increasing prevalence of drones has transformed them into a potent tool wielded by adversaries. Detecting and countering hostile drone operations is a complex and challenging task, involving two key stages: drone detection and drone jamming [4].

COMPONENTS USED

Arduino Uno R3

The Arduino UNO is a feature-rich microcontroller board powered by the ATmega328P processor [5]. This device offers users a range of interfaces, comprising 14 digital I/O pins, with the flexibility for 6 of them to serve as PWM outputs, enabling control over analog devices. The board also includes 6 analog input pins, a 16 MHz ceramic resonator for reliable clock speed, a USB interface for connecting to a computer, a power input jack, an ICSP header for advanced programming, and a handy reset button. Starting with the Arduino UNO is effortless due to its integrated components supporting the microcontroller. Just plug it into a computer using USB or power it with an AC adapter or battery, and you're all set to begin your project exploration. The UNO's user-friendly design encourages experimentation and learning, allowing you to explore its features and capabilities with confidence, even if you're new to electronics [6].

RF Transceiver Module

The CC1101 is an economical transceiver crafted for low-power wireless tasks in the sub-1 GHz frequency spectrum. Although its main focus lies in the Industrial, Scientific, and Medical (ISM) and Short-Range Device (SRD) bands at 315, 433, 868, and 915 MHz, it boasts versatility, effortlessly adapting to frequencies spanning 300-348 MHz, 387-464 MHz, and 779-928 MHz. One of the key features of the CC1101 is its integration with a highly customizable baseband modem, which supports various modulation schemes and data rates up to 600 kbps. This adaptability enables the transceiver to adjust to varying application needs and enhance its performance [7].

The CC1101 offers robust hardware assistance across a range of functions, including packet management, data storage, burst transmissions, channel assessment, indication of link quality, and wake-on-radio capability. These features help to streamline the implementation of wireless communication protocols and improve the overall efficiency of the system [8].

Managing the primary operational settings and the 64-byte transmit/receive FIFOs of the CC1101 is straightforward via an SPI interface. Typically, the CC1101 is paired with a microcontroller and a handful of passive components to craft a comprehensive wireless communication solution. For long-range applications, the CC1101 can be paired with the CC1190 range extender, which operates in the 850-950 MHz band. This combination enhances the sensitivity and output power of the system, enabling reliable communication over greater distances [9].

Wi-Fi Module

The NodeMCU is an open-source platform that combines software and hardware development tools to create a powerful and affordable System-on-a-Chip (SoC) solution based on the ESP8266 chip. Developed by Espressif Systems, the ESP8266 integrates all the essential components of a computer, including a CPU, RAM, Wi-Fi connectivity, and a modern operating system with a software development kit (SDK) [10].

The ESP8266EX stands out for its capability to offer a complete and self-sufficient solution for Wi-Fi networking. It can be used either as a standalone application processor or to offload Wi-Fi networking functions from another processor. When used as the main application processor, the ESP8266EX boots directly from an external flash memory and utilizes its integrated cache to enhance system performance. Alternatively, when serving as a Wi-Fi add-on, the ESP8266EX can easily provide wireless internet connectivity to any microcontroller-based design through common interfaces such as SPI, SDIO, I2C, or UART.

The ESP8266EX stands out as one of the most integrated Wi-Fi chips available in the market. It integrates antenna switches, RF baluns, power amplifiers, low-noise amplifiers, filters, and power management modules, needing only minimal external circuitry. The whole solution, along with the front-end module, is crafted to occupy a small PCB footprint, making it perfect for applications with limited space.

Ultrasonic Sensor

The HC-SR04 Ultrasonic Sensor is a cost-effective solution for measuring proximity and distance, widely used in various robotics projects for object avoidance. Its applications extend beyond robotics, finding use in turret systems, water level monitoring, and even parking sensors.

The second iteration of the widely-used HC-SR04 Low-Cost Ultrasonic Sensor extends its compatibility by accommodating a broader input voltage range, enabling smooth integration with controllers operating at 3.3V. Utilizing sonar technology, the HC-SR04 provides a straightforward and cost-effective solution for distance measurement. It emits an ultrasonic pulse at around 40 kHz, which is well above the range of human hearing, and calculates the distance to the target by measuring the time taken for the echo to return.

The distance to an object can be determined using the formula: Distance = ((speed of sound in air) * time) / 2, where the speed of sound in air at 20°C (68°F) is approximately 343 m/s.

This sensor distinguishes itself with remarkable precision and reliability in range measurements, all within an easily accessible module. The sensor includes a 2.54mm pitch pin header, which allows for easy integration into solderless breadboards, making prototyping a breeze.

METHODOLOGY

Various strategies exist for detecting drones, each with its own advantages and disadvantages, making them suitable for different situations. As a result, it is common practice to employ a combination of different detection methods to achieve optimal results.

The most used techniques for drone detection include radar, radio frequency (RF), acoustic, optical, and thermal (infrared) sensing. Utilizing a variety of detection systems is advisable as opposed to relying on a singular method for detection. The selection of which systems to integrate should be based on the particular location and needs of the secured area. Once a drone is successfully detected, the next step is to implement jamming measures. While jamming is not the only countermeasure available, it is considered one of the most effective methods for combating drones, alongside other approaches such as drone destruction.

RF jamming of drone communication links can be implemented in either a directional or omnidirectional manner. Directional jamming offers a longer range compared to omnidirectional jamming. However, omnidirectional jamming is more reliable since it does not rely on the success of drone detection. The main drawback of omnidirectional jamming, apart from its shorter range, is that it can cause disruption to other devices in the area that operate on the same frequency being jammed. The objective of jamming is to manipulate the signal to a degree where the receiver cannot discern it, or alternatively, to disrupt specific components of the system, leading to either complete or partial denial of service.

Drone Detection

Radar systems, although widely used, face challenges in detecting small drones due to their size, speed, and maneuverability. Despite limited robust solutions, radar detection offers advantages such as long-range capabilities in obstacle-free environments, detection of autonomous drones, and performance in adverse conditions. However, it also has drawbacks, including varying reflectivity of materials, limitations in urban areas, and potential harm from high-emission power.

Several radar realization concepts can be applied to drone detection, each with its own pros and cons. Securing large areas can be achieved using a single surface movement radar or multiple smaller radars. Monostatic pulse radar excels at distinguishing drones from birds using micro-Doppler signatures but requires careful consideration of radar characteristics.

Light Detection and Ranging (LIDAR), combining light and radar, shows potential for drone detection but is limited by insufficient resolution and small drone laser radar cross-sections. LIDAR benefits include easy object separation, independence from weather, and precise position determination. Higher-resolution LIDARs are possible but currently expensive, although costs are expected to decrease.

Drone Jamming

The objective of jamming is to interfere with the signal to such an extent that the receiver is unable to differentiate it or to induce disruptions within the system, leading to either complete or partial denial of service. Drones typically use remote control (RC) links for commands, telemetry for flight data, video links for images, and Global Positioning Systems (GPS/GLONASS). Effective GPS jamming is the most potent way to impair a drone, causing it to crash. If other critical frequencies are jammed but GPS is not, the drone may land itself or return to its starting point.

Spoofing, a process of taking control of the drone’s flight and operation, is a more sophisticated form of disabling drones. Jammers come in various forms, such as weapons, portable devices, desktops, or specialized vehicles. As the commonly used frequencies for drone operation are well-known, jammer implementation is simplified compared to RCIED actuation jamming. Frequencies used for drone communication, video, and telemetry include 433MHz, 868MHz, 915MHz, 1.2GHz, 2.4GHz, 5.8GHz, and GPS/GLONASS frequencies.

Previous generations of drone systems utilized frequencies such as 27 MHz, 35 MHz, 49 MHz, 72 MHz, or 75 MHz. Jamming can be performed on frequencies other than the nominal ones, but the signal level must be higher. GPS signals have a very low level at the receiver (typically below –120 dBm), so effective jamming can be achieved by out-of-band signals, side-lobes, or intermodulation products. Tests show that a jamming-to-signal ratio of 25 dB causes maximum position errors and affects GPS receivers up to 2 km away.

Two modes of operation can occur during drone jamming. In the first mode, the jamming signal level is high, making GPS localization impossible and affecting other devices in the area. In the second mode, the jamming signal is lower, allowing GPS localization but with incorrect positions. The impacted region has reduced in size, with jamming effects being less pronounced. For drone jamming, it is not necessary to jam the entire frequency range but rather the regions around the specific frequencies used by drones, using established jamming techniques.

PROPOSED SYSTEM DESIGN AND METHODOLOGY

The proposed system for drone detection and jamming employs an Arduino microcontroller board as the central processing unit, coordinating an ultrasonic sensor mounted on a servo motor for wide-area scanning, and RF transceiver and Wi-Fi Deauthor modules for jamming. The ultrasonic sensor detects objects within a 400 cm range, triggering the activation of the jamming modules. The RF transceiver disrupts the drone's radio link at 433 MHz, while the Wi-Fi Deauthor sends deauthentication packets to disconnect the drone from its Wi-Fi network. The modular design facilitates seamless integration and customization, while stringent testing and calibration guarantee peak performance. The compact and portable system can be deployed in various locations, providing a robust solution to counter unauthorized drone activities.

Connections

The ultrasonic sensor is securely attached to the servo motor using custom-designed mounting hardware. This setup allows for precise and stable positioning of the sensor, ensuring accurate distance measurements. The Arduino board is connected to both the ultrasonic sensor and the servo motor, with the ultrasonic sensor using pin 8 and the servo motor using pin 9. Pin 8 is configured as an output to send trigger signals to the ultrasonic sensor, while pin 9 is set up as an input to receive the echo signals from the sensor. This configuration enables the Arduino to control the ultrasonic sensor and retrieve distance data effectively.

The servo motor is programmed to rotate 180 degrees in a sweeping motion, moving back and forth continuously. This oscillating movement enables the ultrasonic sensor to cover a wider area, spanning from –90 degrees to +90 degrees relative to its central position. By mounting the ultrasonic sensor on the servo motor and implementing this sweeping motion, the system can detect objects within a larger field of view, enhancing its spatial coverage. Additionally, the ultrasonic sensor is capable of measuring distances up to 400 cm from its location, providing a substantial range for object detection.

When the ultrasonic sensor identifies an object within its detection range, it sends a signal to the Arduino board. On receiving this signal, the Arduino generates a command to activate the RF Transceiver and the Wi-Fi Deauthor modules. These modules are connected to the Arduino board on pins 10 and 12, respectively. Pin 10 is designated as an output to control the RF transceiver, while pin 12 is set up as an output to manage the Wi-Fi Deauthor. Once the command is issued, the RF transceiver and the Wi-Fi Deauthor are turned ON, initiating their respective jamming functionalities.

The RF transceiver is specifically configured to jam radio frequencies in the 433 MHz band, which is commonly used by drones for communication and control. By transmitting strong interference signals at this frequency, the RF transceiver disrupts the communication link between the drone and its controller, effectively hindering its operation. Simultaneously, the Wi-Fi Deauthor targets the Wi-Fi signal that the drone may rely on for additional functionality or video transmission. The Wi-Fi Deauthor generates deauthentication packets, which are designed to disconnect the drone from its associated Wi-Fi network, further disrupting its communication capabilities.

By integrating the ultrasonic sensor, servo motor, RF transceiver, and Wi-Fi Deauthor, this system creates a comprehensive drone detection and jamming solution. The ultrasonic sensor actively scans the surroundings, identifying potential drone threats, while the servo motor enables wide-area coverage. On detection, the RF transceiver and Wi-Fi Deauthor work in tandem to jam the drone’s radio and Wi-Fi signals, effectively neutralizing its ability to operate or communicate with its controller. This comprehensive strategy boosts the system's efficacy in thwarting unauthorized drone activities and safeguarding sensitive areas against potential threats.

PROPOSED RESULTS

The proposed drone detection and jamming system is expected to deliver effective and reliable performance in countering unauthorized drone activities. By integrating an ultrasonic sensor mounted on a servo motor, the system should achieve accurate detection of drones within a 400 cm range, providing a wide area scanning capability. The continuous rotation of the servo motor will ensure comprehensive coverage, minimizing any blind spots and enhancing the system's ability to identify potential threats.

On successful detection of a drone, the system is anticipated to trigger the activation of the RF transceiver and Wi-Fi Deauthor modules promptly. The RF Transceiver, operating at 433 MHz, is expected to generate strong interference signals that will effectively jam the drone’s radio link. This jamming will disrupt the communication between the drone and its operator, preventing the transmission of commands and hindering the drone's ability to maintain controlled flight.

Simultaneously, the Wi-Fi Deauthor module is expected to send out deauthentication packets, targeting the drone's Wi-Fi connection. These packets will force the drone to disconnect from its associated Wi-Fi network, disrupting any video transmission or data exchange that may be occurring over the Wi-Fi link. The combined jamming of both the radio and Wi-Fi signals is anticipated to significantly impair the drone's overall functionality and render it inoperable.

The modular design of the system is expected to provide flexibility and adaptability, allowing for easy integration of additional sensors or jamming modules based on specific requirements. This modularity will enable the system to be customized and optimized for different deployment scenarios, ensuring its effectiveness across a range of drone models and communication protocols.

Thorough testing and calibration procedures will be undertaken to verify the precision and dependability of the system. The ultrasonic sensor’s performance will be thoroughly evaluated to ensure precise distance measurements and minimize false positives. The RF transceiver and Wi-Fi Deauthor modules will undergo extensive testing to verify their jamming capabilities and determine their effective range.

The compact and portable nature of the system is expected to facilitate easy deployment in various locations, such as critical infrastructure, public events, or sensitive areas. The Arduino board and connected modules will be housed in a rugged enclosure, providing protection against environmental factors and ensuring durability in different operating conditions.

Overall, the proposed drone detection and jamming system is expected to deliver a robust and efficient solution for countering unauthorized drone activities. By leveraging the capabilities of the ultrasonic sensor, servo motor, RF transceiver, and Wi-Fi Deauthor modules, the system is anticipated to provide real-time detection and effective jamming of drones, enhancing security measures, and protecting against potential threats posed by unauthorized drone operations. The system's modular design and adaptability will allow for future enhancements and integration with other security systems, ensuring its continued effectiveness in the face of evolving drone technologies.

CONCLUSION

In this venture, we investigated the feasibility of utilizing ultrasonic and RF modules for drone detection. The aim was to create a system capable of identifying the presence of drones in a given zone, giving important data for security and safety applications. The ultrasonic sensor was employed for distance measurement through the emission of high-frequency sound waves and subsequent calculation of the time it took for the echo to rebound. This permitted us to appraise the separation of objects inside its range. Be that as it may, it is imperative to note that ultrasonic sensors have restrictions in terms of range and may not be reasonable for recognizing drones at high heights.

The RF module played a significant part in this project by providing a means of communication and following. By utilizing RF innovation, we were able to set up a remote interface between the drone and our detection system. This empowered us to get signals and assemble basic information for analysis.

Through experimentation and testing, we observed that the combined utilization of ultrasonic and RF modules appeared promising for identifying drones within a direct range. Be that as it may, it's essential to recognize that this system may have restrictions when managing fast-moving or small-sized drones.

Moreover, natural components such as wind, impedances, and impediments can influence the precision and unwavering quality of the detection system. Further research and improvement is prescribed to optimize the system's execution under changing conditions.

In conclusion, this extend serves as a profitable establishment for drone discovery utilizing ultrasonic and RF innovation. It illustrates the potential for making successful and reasonable arrangements for security and safety applications. Future iterations of this project may benefit from joining additional sensors, refining calculations, and conducting comprehensive field tests to further upgrade the system's capabilities.

REFERENCES

1. Basarikatti S, Dhumal S, Datir S, Mishra S, Koyale S. Auto billing system using Arduino. Int J Res Appl Sci Eng Technol. 2022.[Online] Available at https://www.ijraset.com/research-paper/auto-billing-system-using-arduino.
2. ESP8266: the black magic boxes. Blackmagicboxes.com. 2024. [Online] Available at https://www.blackmagicboxes.com/?page_id=258
3. Matić V, Kosjer V, Lebl A, Pavić B, Radivojević J. Methods for drone detection and jamming. In Proceedings of the 10th International Conference on Information Society and Technology (ICIST) 2020 Mar 8. [Online] Available at https://www.eventiotic.com/eventiotic/files/Papers/URL/f07e8f39-5c16-420e-b0e3-5eb5b5ab1ba0.pdf
4. Laxmi Power Solutions. (2019). LPS earthing pit covers. [Online] Available at https://www.laxmipowersolutions.com/earthing-pit-cover.html
5. FasterCapital. (2024). Improving accuracy and reliability. [Online] Available at https://fastercapital.com/topics/improving-accuracy-and-reliability.html
6. Internet of Things. (2024). An ultrasonic range sensor. [Online] Available at https://bdavison.napier.ac.uk/iot/Tutorials/Arduino/ultrasonic/
7. Praveenchandar J, Navaneetha C, Bharathi RJ, Jainish GR, Thenappan S, Karthikeyan R. Development of an artificial intelligence-based railway crack detection and monitoring system using internet of things. Int J Recent Innov Trends Comput Commun. 2023; 11(9): 2463–2468.
8. Hwang SP, Kim DH. A study on the establishment of anti-drone system for the protection of national important facilities. J Digit Converg. 2020; 18(11): 247–257.
9. Yasmine G, Maha G, Hicham M. Survey on current anti-drone systems: process, technologies, and algorithms. Int J Syst Syst Eng. 2022; 12(3): 235–270.
10. Gautam T, Johari R. Drone: A systematic review of UAV technologies. In: International Conference on Computing, Communications, and Cyber-Security; 2022 Oct 21; Singapore: Springer Nature Singapore; 147–158 p.

