Budget Concerned Anti-drone System with Wifi Connectivity

Krunal Intwala[1] , Kishor Kolhe[2]
***Corresponding Author**:- Krunal Intwala
Address: [1]School of Computer Engineering and Technology Dr. Vishwanath Karad MIT World Peace University,Pune ,India , E-mail:1032200117@mitwpu.edu.in
[2]School of Computer Engineering and Technology Dr. Vishwanath Karad MIT World Peace University
Pune ,India , E-mail:kishor.kolhe@mitwpu.edu.in

Abstract
The Internet of Things (IoT) has recently emerged as one of the most significant technological advancements of the twenty-first century. Internet-connected physical objects that are often seen are referred to as IoT. All physical devices, including sensors, that may be utilized to incorporate software are referred to as things in the IoT. An unmanned aerial vehicle is a drone. As the name implies, there is no human pilot present on the board. Because of its small size and light weight mechanism, it has a lot of potential to do jobs that can ease our daily life. Different frequency signals may be used to operate the drones. Drones with wifi connectivity may also be controlled by wifi-enabled devices, such as smartphones, unlike radio frequency drones, which are typically flown via a remote control. Due to their advantages, drones are being used more often for both legal and illegal activities, including the transfer of illegal goods over international boundaries and the monitoring of security. Anti-drone technologies are being developed as a result since they might be crucial in the development of smart cities in the future. But citizens can no longer deploy anti-drone equipment due of their high cost. We have proposed a proposal for an IoT-based anti-drone system as a result in this study. Building a WiFi-Pineapple and Raspberry Pi anti-drone system is the article's main goal. Drones with wifi capabilities may be brought down or even taken over because of their vulnerability to wireless attacks, requiring them to land in a safe or emergency mode. The drone that was near to the system was our target in this paper's attempt to employ wireless attacks with the following components. Wireless attack elements include packet spoofing, deauthentication attack, DOS attack, wireless password cracking, and unauthorised root access attack. This study has described its findings and attack success rate. The DJI Tello drone that was used in this experiment has WiFi capabilities, and the system was automated so that it could decide how to carry out the assaults on its own.

Keywords— Anti-drone System, IoT, Wireless Attacks, Automation

DOI Number: 10.14704/nq.2022.20.9.NQ44626 **Neuro Quantology 2022; 20(9):5380-5387**

I. INTRODUCTION

An unmanned aircraft is a drone. Unmanned aerial vehicles (UAVs) or unmanned aircraft systems are more official names for drones. A drone is essentially a flying robot that can be remotely controlled or fly on its own using flight plans that are controlled by software and onboard sensors and a global positioning system (GPS). Light composite materials are typically used in unmanned aircraft to save weight and improve agility. Military drones can fly at exceptionally high altitudes thanks to the strength of the composite material.

UAV drones are outfitted with a variety of cutting-edge technologies, including infrared cameras, GPS, and lasers. UAVs were frequently linked to the military. They were first employed as platforms for weaponry, which was more contentious, anti-aircraft target practice, and information collection. Today, drones are employed in a variety of civilian capacities, such as search and rescue, surveillance, traffic monitoring, weather monitoring, firefighting, personal use, photography, videography, agriculture, delivery services[1], emergency rescue[2], wildlife and historical conservation and medicine. DJI, Parrot, Yuneec, Kespry, Autel Robotics, Skydio, Insitu, Delair, EHang, Aerialtronics are a few well-known manufacturers of drones and drone components.

Drones require a power source, such as a battery, in order to fly. The drone itself plus the control system make up an unmanned aerial vehicle system. Drones need a controller, which enables the user to launch, steer, and land the aircraft via remote controls. Radio waves, such as Wi-Fi, are used by controllers to connect with the drone.

Table 1. Different Type of Drones

Type	Weight
Nano	Not more than 250 grams.
Micro	More than 250 grams but not more than 2 kg.
Small	More than 2 kg but not more than 25 kg.
Medium	More than 25 kg but not more than 150 kg.
Large	More than 150 kg.

Over wireless connections, commercial drones are controlled and transmit data, typically video. The drones may employ a variety of wireless connections. Others employ more commercially available techniques while some use proprietary protocols.

Fig 1. Types of Drones

Many commercial drones employed 802.11 or WiFi, in the 2.4 GHz frequency range, as the technology for sent data, including those from early versions of DJI and Parrot. Even today, the majority of low-cost commercial drones use WiFi for control. Since commercial WiFi chips are affordable, widely accessible, and enable users to effortlessly manage and receive data from their smartphone, it is handy for manufacturers. Drone and center are using communication module such as RF (radio frequency), Bluetooth and Wi-Fi(Wireless Fidelity)[3]. The remote-control system of a drone is typically based on wireless communications, such as 2.4 GHz, 5.8 GHz, or Wi-Fi (IEEE 802.11 a/b/g/n)[2].

WiFi does, however, have drawbacks. It has a naturally restricted range, and the signal quality may suffer while flying over locations with other WiFi networks. This further reduces the range or results in poor video quality. However, utilizing adapters to extend the wifi range might be able to fix this issue.

In either the 2.4 GHz or 5.8 GHz range, common 802.11 frames contain both control and data packets. To prevent interference, the drones frequently automatically transition between the 2.4 GHz and 5.8 GHz bands dependent on the wireless environment. Wi-Fi may be utilized at quite close ranges. A Wi-Fi signal's range can vary from 300 to 2000 meters, depending on the setup and environmental factors. Due to less interference in that band in urban areas, 5GHz Wifi networks are preferred. There are already tens of thousands of drone businesses with products on the market. Many don't have Wi-Fi, although some do. For instance, only for its drone devices, DJI has three different unique communication methods. These protocols have a wider transmission range and are less susceptible to interference.

Fig 2. Drone from different manufacturers

UAV laws have been created in several nations. Laws are constantly changing as drone use becomes more widespread. drones in open airspace must stay below 150 meters and keep at a distance of at least 30 meters from people, properties on the ground, and vehicles[4]. Pilots of personal and commercial drones must review the rules of the nation and the area in which they are using the equipment. In India, never fly a micro Drone higher than 200 feet (60 meters) in the air or a nano Drone higher than 50 feet (15 meters). Keep drones away from heliports and airports, without prior authorization, do not fly a drone over or close to any no-drone zones, public events, or packed stadiums. Do not fly a drone over or close to any government or military bases. Unmanned vehicles may be used to spy[5] and fly over areas in public capturing footages of people and breach their privacy and may also use them for personal intentions or even crash into houses and private spaces.

Neuro Quantology | September 2022 | Volume 20 | Issue 9 | Page 5380-5387 | doi: 10.14704/nq.2022.20.9.NQ44626
Krunal Intwala , Kishor Kolhe ,/ Budget Concerned Anti-drone System with Wifi Connectivity

It is important that these privacy physical security concerns are addressed and ensure protection of drones, users, wireless connections and other safety controls. These anti drone technologies use various detection techniques which are being developed to detect audio, video, motions using different methods. There is an integration of technologies into these anti drone systems which encompasses a wide range that help to identify and track aerial vehicles. Radar systems, RF communications are some of the important techniques used for these purposes to counter the threats[5]. These technologies are developed so that they can cover distances up to several miles for detection and target and identify drones which may be of various types, sizes.

II. Literature Review

The study offered an architecture in which the drone would be found by the anti-drone system using radar, camera, or radio frequency. The drone would then be identified in the Identification phase, where more data about the drone, such as image recognition and RFID tag, would be obtained. The drone is then neutralized by employing various tools and procedures, including as jamming, hijacking, and capture. Then, a proposal for an anti-drone system was made, in which the choice would be made by a model for classifying airspace priorities based on risk assessment of the most recent data[1].

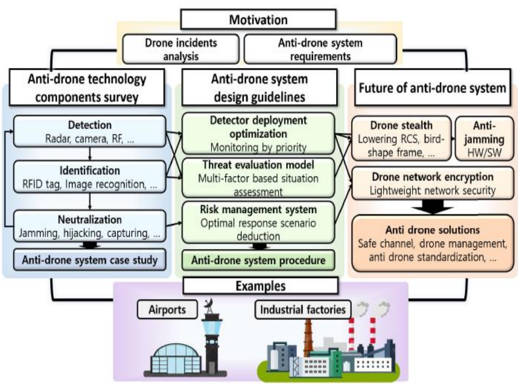

Fig 3. Drone incident analysis and system requirements for anti-drone system

Wi-Fi drone capture may also be accomplished utilizing the XBee 868LP connection. The drone will be equipped with a GPS receiver, will be connected to the ground through a 2.4 GHz remote control connection, and will communicate via a Telemetry Box made up of an XBEE 868LP link and a video link. The data that is received can be tampered with and sent to a different device that is connected through an 802.11 WEP link[6].

Fig 4. Drone capturing using XBee 868LP link

Here, it was suggested that the user provide a set of four waypoints that represent the location's extreme bounds and are necessary for the RSSI scan. GPS coordinates will be used to represent the waypoints. The drone will fly to the specified locations while conducting a thorough RSSI scan of the surrounding region. As soon as the drone reaches a height of 20 meters, it stabilizes. The RSSi values obtained at various places will be grouped by the clustering algorithm according to whether the signal strength is "Very Good," "Good," or "Poor." Additionally, the drone will halt its RSSI scan and head back to the base station once the last waypoint has been reached[7].

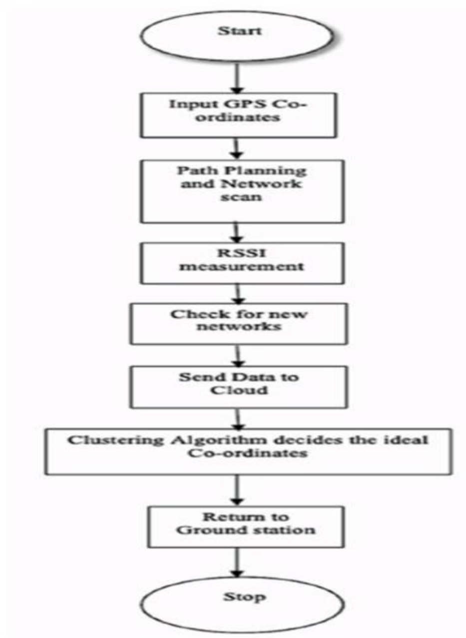

Fig 5. Flow chart to RSSI scan and return to home

III.Proposed Anti-Drone System

We have created an automated system that will perform certain steps of attacks to capture the wifi-based drone. The system setup is ready, it will start looking for any wireless signals found in the vicinity. If found any, it will check if the drone is government registered or not. The

Neuro Quantology | September 2022 | Volume 20 | Issue 9 | Page 5380-5387 | doi: 10.14704/nq.2022.20.9.NQ44626

government registered drones might be used by Police or Military for security reasons. Thus, once confirmed the drone is illegal, the system will start its functionality and try to capture the drone in good condition so we could investigate over it using memory card used for capturing the data and other information. If not, unfortunately the drone will be crash landed in the vicinity for security aspects.

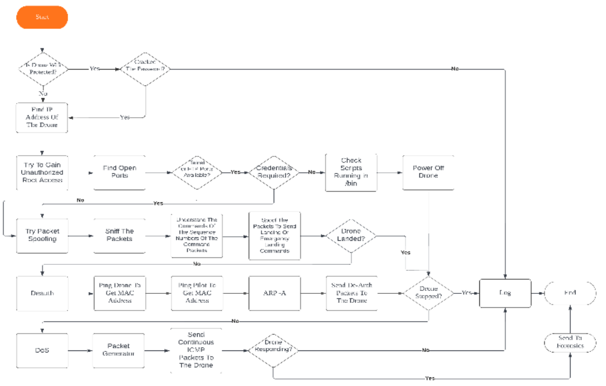

Fig 6. Flow diagram for anti-drone system

Therefore, the drone will do a reconnaissance anytime it comes within range of the system in order to learn whether it is a wifi-enabled drone. If so, it will attempt to determine whether the drone's wifi is password-protected. The use of a brute force attack will help break the password. Once the password has been obtained, an attempt will be made to identify the drone's IP address in an effort to get unauthorised root access to the drone.

To perform the unauthorized root access attack, the system has to cross verify if the telnet or FTP ports are open on the drone. It will also check if the credentials are required incase the ports are open. Incase the system gets Telnet or FTP ports with anonymous login, it will check the /bin folder for the running scripts and try to power off the drone. However, if the ports are closed or credentials are enabled then the system will look for spoofing the packets.

To try packet spoofing, first the system will try to sniff some of the packages. The sniffed packages will analyzed and system will try to learn based upon the sequence number of the packages. Using the information of the sequence, the system will try to send 'Safe Landing' or 'Emergency Landing' commands to the drone. If the attack is successfil, the drone will make an emergency landing right on the spot. If not, the system will try to perform the deauthentication attack.

We have now exhausted all the option to live-capture the drone in this situation. Unfortunately, the system will now switch to an offensive mode and attempt to capture the drone at any costs using Deauthentication or DoS attacks.

In order to launch the Deauthentication Attack, the system should be aware about the MAC addresses of the drone and the pilot's controller. As a result, it will send both devices a straightforward ICMP message and store the responses. To put it simply, the system has just ping'd the devices, revealing their MAC addresses. The de-auth packets will be sent to the drone using Address Resolution Protocol that use the MAC addresses of both devices up until the drone is forced to perform a crash landing or safe landing relying on the manufacturer's features. 5383

Even though the drone is still in the air, it will now carry out the last attack, a Denial-Of-Service attack (also known as a DoS attack), under the pilot's direction. The system has already gathered a lot of information about the drone up to this point, including its MAC address and IP address, which are necessary for the DoS attack.

Sending packets to the device repeatedly until it is unable to provide service is how the DoS attack is carried out. Thus, a packet generator will be useful in this situation to constantly deliver the drone a large number of ICMP packets until it is forced to conduct the crash landing over the same spot immediately.

Even if this attack is ultimately unsuccessful, there will be enough logs and data about the drone to pass on to the forensics team for more research.

The setup of all the hardware is as shown in the below diagram:

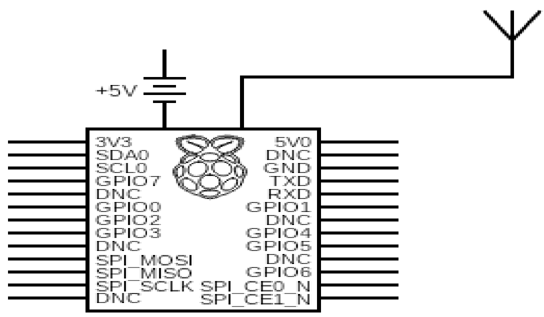

Fig 7. Hardware setup

The Raspberry Pi 4 is connected to the 5V power and Wifi Pineapple to the USB of the Raspberry. The memory card in the Raspberry Pi 4 will already be flashed with Kali Linux ARM image. And the program should also be pre-downloaded in the Kali Linux ARM OS.
The Wifi Pineapple should be connected to the Raspberry Pi such that it can share the data between them. One way is to connect Raspberry Pi to the Wifi Pineapple's Wifi. And another way is to use USB cable that has the capability to transfer cable. Either of the solution would work. And cross verifying if the Raspberry Pi is able to communicate with Wifi Pineapple by hitting the IP address of the WiFi Pineapple in the browser would lead us to the dashboard after entering the credentials.

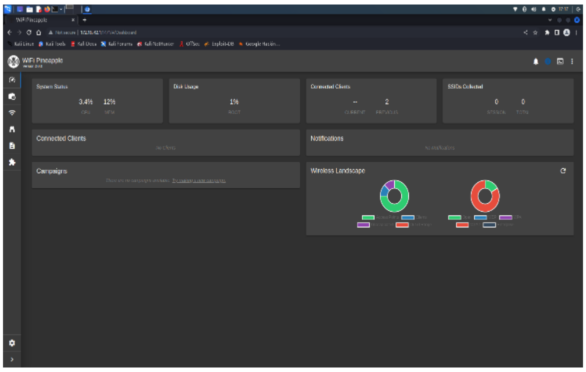

Fig 8. Wifi Pineapple Dashboard

The program when started will continuously look for the available networks in the surroundings. As soon as the DJI Tello Drone is bought in the radar of the system, it will try to bring it down as it does not contain any kind of RFID attached to it.
The estimated cost of construction for this anti-drone device is about ₹22,000 (around $277). Comparing the price of this device to the conventional anti-drone systems now on the market worldwide, it is far more affordable. Given that it has very high attack success rates, as will be discussed later in this paper, this product can also be used in the creation of smart cities in the future.

IV. Hardwares Used

To perform the above experiment, we have used the following hardware:

- Raspberry Pi 4 Model B

Fig 9. Raspberry Pi 4 Model B

- RAM Memory: 8 GB
- Brand: Raspberry Pi
- CPU Manufacturer: ARM
- RAM Memory Maximum Size: 8 GB
- Resolution: 3840 x 2160
- Wireless Communication Technology: Bluetooth
- Wireless Communication Standard: Bluetooth, 801.11ac
- Hard Disk Interface: USB 3.0

- Hak5's Wifi Pineapple

Fig 10. Wifi Pineapple

- 2.4 GHz 802.11 b/g/n (5 GHz/ac with module)
- Single Core MIPS Network SoC
- Three Dedicated Role-based Radios
- With three high gain antennas
- USB-C Power/Ethernet Port, USB 2.0 Host Port,
- Single RGB LED Indicator
- 256 MB RAM, 2 GB EMMC
- Power via USB-C

- DJI Tello Drone

Fig 11. DJI Tello Drone

○ Aircraft Weight: Approximately 80 g (Propellers and Battery Included)
○ Dimensions: 98×92.5×41 mm
○ Propeller: 3 inches
○ Built-in Functions: Range Finder, Barometer, LED, Vision System, 2.4 GHz 802.11n Wi-Fi, 720p Live View
○ Port: Micro USB Charging Port
○ Battery Detachable Battery: 1.1Ah/3.8V
○ Camera: 5MP (2592x1936)
○ FOV: 82.6°
○ Video: HD720P30
○ Format: JPG(Photo); MP4(Video)
○ EIS: Yes

- Other hardware included like a memory card flashed with Kali Linux ARM image, a smart phone as controller for DJI Tello Drone.

V. Experiment And Testing

The results of individual attacks on DJI Tello are mentioned below in detail.

A. Unauthorized Root Access Attack

DJI Tello does not have Telnet or FTP ports open, hence Unauthorized Root Access Attacks was not successful on this drone. As the system could not find the required ports, it further went on to perform the next attack. Thus, this system passed through this attack.

B. Packet Spoofing

While testing of the packet spoofing attack, the system successfully captured 108 packets and their sequence numbers. But the data being transmitted between the drone and pilot was using encryption which restricted the system to do the analysis. But the drone is equipped with custom commands that uses python scripts. Thus, if the commands were directly fed into the system, the landing signals were transmitted successfully and the drone successfully made the safe landing.

C. DeAuthentication Attack

When performed the deauthentication attack on DJI Tello, it deauthenticated the communication between the Pilot and the Drone. Thus, the drone was no more under the control of the pilot. Thus, this attack was also successful.

D. DoS Attack

The DoS attack forced the drone to make a crash landing on the spot when the attack was performed.
We have also included a feature that allows logs to be kept so that future investigations into any reported incidents will be simple.

```
SSID: Pine_AP
MAC: 00:13:37:A8:D1:A9
Channel: 11
Security: Open
Clients: 0
Signal: -33 dBm

SSID: Pineapple_Hak5
MAC: 02:13:37:A8:D1:A9
Channel: 11
Security: WPA2 (PSK)
Clients: 1
Signal: -31 dBm

```

Fig 12. Logs Sample

The above attacks were performed several times to measure the accuracy of the system. The observations are as mentions below:

A. Wifi Cracking

The wifi-enabled drones could set a password to their wifi for protection. However, we tried different combinations here to check the time required in order to crack the password. The observations of the timings it took to crack the passwords are as shown in the below table:

Table 2. Wifi Cracking Time

Sr. No.	Password Examples	Avg. Time
1.	1234567890	1-5 seconds
2.	Abc12345	30 seconds
3.	Abcd12345678	1 Minute
4.	abcdefgh	1 Minute
5.	Abcd#789$	15 Minutes

We observed the numeric passwords were easy to crack with common passwords being cracked in less than 5 seconds. Passwords containing alphabets or alphanumeric characters took maximum of 60 seconds to crack. While alphanumeric password when combined with special characters took the maximum amount of time of approximately 15 minutes. Thus, drones with easier passwords were soon to get under control as the attacks were started earlier compared to the passwords with alphanumeric and special characters combination.

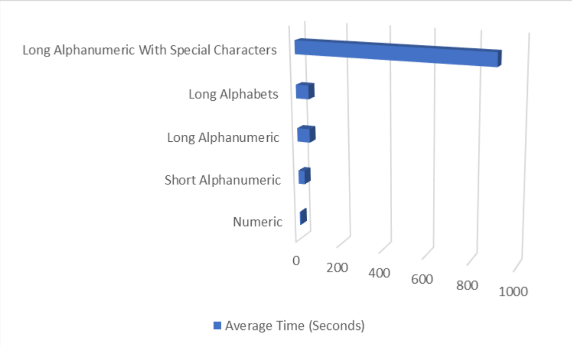

Fig 13. Wifi Cracking

A. Wireless Attacks On Drones

The highest success ratio of all the systems were found over Unauthorized Root Access Attack and Packet Spoofing Attack consisting of not a single failure attempt. As the attacks were a negative scenario testing where the ports were not open and packets were encrypted, still we tried the attack multiple time to check if the system reports the ports as open by consideration of the odds. But the system only extracted the open ports and resulting in to the highest success ratio of the attacks on the drone by this system.

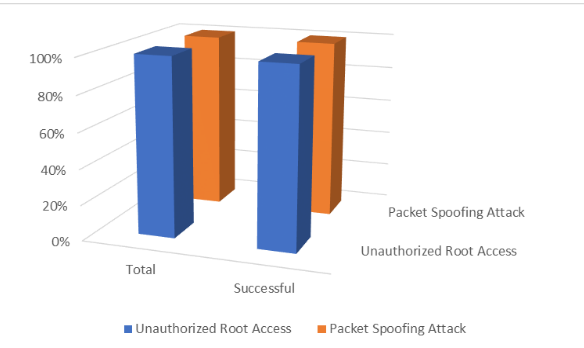

Fig 14. Wireless Attacks Comparison

The least success ratio was observed over the deauthentication attack, where the drone was designed to change the channel automatically to the one with the least latency for better user experience. Despite low success ratio, this attack was also successful wherein the drone was found to be no more in control of the pilot. The drone was designed to fly for a minute in the air and search for the pilot to reconnect in 60 seconds. If not, the drone would make a safe landing. As the system was already sending the deauthentication packages for more than 1 minute, the drone had to forcefully perform the safe landing as the pilot won't be able to reconnect to the drone and take control over it.

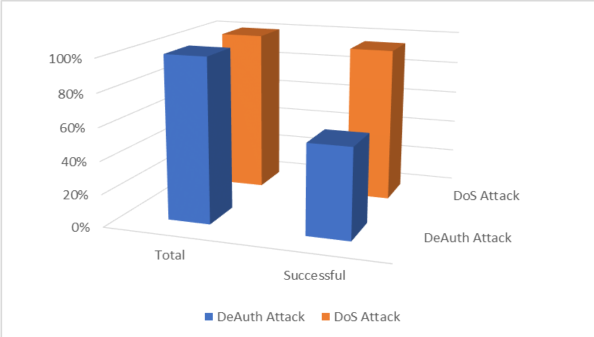

Fig 15. Wireless Attacks Comparison

The DoS attack also showed promising results, only one unsuccessful attempt where an error was observed in the system due to library files.

VI. Conclusion

We were able to successfully make a low-budget anti-drone system using Internet of Things (IoT). The system was also made and tested using different attacks on a DJI Tello Drone. After carrying out a deauthentication attack on a drone secured by wifi, we were able to stop communication between the drone's pilot and the drone by sending deauth packets. Furthermore, we explored why the success rate was low and determined that it was due to the channel-switching design of the drone. We also compared the time it took to hack the wireless password. The drone was subjected to an unauthorized root access attack and packet spoofing attack, which, while being the negative testing scenarios, showed the best success rate. Despite one unsuccessful effort in which the library was unable to retrieve the functions in the code, DoS attacks also generated encouraging results. As a result, a fully functional anti-drone system was successfully developed and well tested with good amount of success rate.

The project's future work will involve integrating more wireless attacks and testing on various wifi-based drones from different manufacturers.

References

Park, S., Kim, H., Lee, S., Joo, H. and Kim, H., 2021. Survey on Anti-Drone Systems: Components, Designs, and Challenges. 2021 IEEE Access (Volume: 9)

Abdularahman Hasan Abunada, Ahmed Yousif Osman, Amith Khandakar, Muhammad Enamul Hoque

Chowdhury, Tamer Khattab, Farid Touati; Design and Implementation of a RF Based Anti-Drone System; 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)

Seyit Alperen CELTEK; Akif DURDU; Ender KURNAZ; Design and Simulation of the Hierarchical Tree Topology Based Wireless Drone Networks; 2018 International Conference on Artificial Intelligence and Data Processing (IDAP)

Nappaphol Siriphun, Shigeru Kashihara, Doudou Fall, Assadarat Khurat; Distinguishing Drone Types Based on Acoustic Wave by IoT Device; 2018 22nd International Computer Science and Engineering Conference (ICSEC)

Edwin Vattapparamban, ˙Ismail G¨uvenc, , Ali ˙I. Yurekli, Kemal Akkaya, and Selc , uk Ulua˘gac; Drones for Smart Cities: Issues in Cybersecurity, Privacy, and Public Safety; 2016 International Wireless Communications and Mobile Computing Conference (IWCMC)

Petar Čisar, Robert Pinter, Sanja Maravić Čisar, Milan Gligorijević;Principles of Anti-Drone Defense; 2020 11th IEEE International Conference on Cognitive Infocommunications (CogInfoCom)

Mir Faisal Ahmed, Emad M. Naveed, Pratham Nar, Sumit Kumar Jindal; Design of an Autonomous drone for IoT deployment analysis; 2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN)

Xiufang Shi, Chaoqun Yang, Weige Xie, Chao Liang, Zhiguo Shi, and Jiming Chen; Anti-Drone System with Multiple Surveillance Technologies: Architecture, Implementation, and Challenges; IEEE Communications Magazine (Volume: 56, Issue: 4, April 2018)

Ottilia Westerlund and Rameez Asif; Drone Hacking with Raspberry-Pi 3 and WiFi Pineapple: Security and Privacy Threats for the Internet-of-Things; 2019 1st International Conference on Unmanned Vehicle Systems-Oman (UVS)

Przemysław Flak; Drone Detection Sensor With Continuous 2.4 GHz ISM Band Coverage Based on Cost-Effective SDR Platform; IEEE Access (Volume: 9)

Vijay A. Kanade; Securing Drone-based Ad Hoc Network Using Blockchain; 2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS)

Jeremy Straub; Anti-Drone and Anti-Autonomy: Achieving Drone Control via System Logic Analysis; 2019 IEEE Aerospace Conference

Sawsen Abdulhadi Mahmood; Anti-Drone System: Threats and Challenges; 2019 First International Conference of Computer and Applied Sciences (CAS)

Thomas Multerer, Alexander Ganis, Ulrich Prechtel, Enric Miralles, Askold Meusling, Jan Mietzner, Martin Vossiek, Mirko Loghi and Volker Ziegler; Low-cost Jamming System Against Small Drones Using a 3D MIMO Radar Based Tracking; 2017 European Radar Conference (EURAD)

Majed Alwateer; Seng W. Loke; Niroshinie Fernando; Enabling Drone Services: Drone Crowdsourcing and Drone Scripting; IEEE Access(Volume:7))

Nikhil Bhomia, Kishor Kolhe, "Anti-Theft Hybrid Solution for Tracking & Locating Mobile Devices with Data Security", International Journal of Recent Technology and Engineering (IJRTE), ISSN: 2277-3878, Volume 8, Issue 2S3, pp. 696-699,
DOI: 10.35940/ijrte.B1129.0782S319, July 2019.

Samiksha Nakashe, Dr. Kishor Kolhe, "Smart Approach to crawl Web Interfaces with Personalized Search and Domain Classification Concept", International Journal of Computer Engineering and Applications (IJCEA), ISSN (Online): 2321-3469, Volume XII, Special Issue, pp. 1-8, May 2018