ARID ZONE JOURNAL OF ENGINEERING, TECHNOLOGY & ENVIRONMENT
AZOJETE June 2025. Vol.21(2):637-645
Published by the Faculty of Engineering, University of Maiduguri, Maiduguri, Nigeria.
Print ISSN: 1596-2490, Electronic ISSN: 2545-5818
https://doi.org/10.63958/AZOJETE/2025/21/02/028
www.azojete.com.ng

ORIGINAL RESEARCH ARTICLE

DRONE EQUIPMENT AND CONFIGURATION FOR DETECTING THEFT IN TELECOMMUNICATION INFRASTRUCTURE

C. O.Njoku[1], A. V.Gambo[2*], and Y. Bello[3]

[1]Department of Mechanical Engineering, Air Force Institute of Technology, Kaduna
[2]Department of Mechanical Engineering, Ahmadu Bello University, Zaria
[3]Department of Mechatronics Engineering, Air Force Institute of Technology, Kaduna
**Corresponding authors' email: gambo.anthony@yahoo.com*

ARTICLE INFORMATION

Received: 19th February 2025
Revised: 31st April 2025
Accepted: 1st May 2025

Keywords:
UAV
Drones
Telecommunication
infrastructureSensor

ABSTRACT

Drone aircrafts, also known as an Unmanned Aerial Vehicle (UAV) or Unmanned Aircraft Systems (UAS) has gained more importance in environmental monitoring as well as in telecommunication infrastructure theft response around the world. The study aims at identifying the type of sensors that can be mounted on drones for effective telecommunication infrastructure theft detection and prevention. The various parts of drone and configuration were tested. Sensors capable of detecting telecommunication infrastructures in the visible, infra-red, near infra-red, laser fluoro-sensor were all evaluated. The ability of the UAV to continuously and successfully patrol along or beside telecommunication infrastructure reveals that it takes about 5 minutes for the UAV to complete a programmed 150m autonomous patrol. During power test, result showed that for every 150m programmed patrol, 15 minutes of solar charging is required to restore the battery back to its initial voltage. It was concluded that a drone can properly be used for telecommunication infrastructure theft response operations. Appropriate sensors mounted on the drone can detect telecommunication infrastructure theft and can also access locations which are not readily accessible and other aerial patrol platform. The limitation of drones is the payload capability and its inability to operate well in windy weather since data collection with drone are faster, cheaper and easier during telecommunication infrastructure theft response operations. It is highly recommended to mount the suitable sensor capable of detecting telecommunication theft and vandalization even during nighttime operations.

1.0 Introduction

A drone can be defined as "a land, sea or air vehicle that is remotely or automatically controlled (Domaille and Campion, 2018). Drone aircrafts, also known as an Unmanned Aerial Vehicle (UAV) or Unmanned Aircraft Systems (UAS) has gained more importance in environmental monitoring as well as in telecommunication infrastructure theft response around the world. The operations that require the use of a drone are both for simple freight transport and for dealing with natural disasters such as an earth quake, fires, floods, tsunamis and similar emergencies (Michail *et al*., 2019).

Drone aircrafts have the potential to deliver information quickly and economically in areas with access difficulties and have the ability to fill an important gap in surveillance capability (Joshi, 2019). UAV are able to fly with high altitudes above clouds which minimizes the cloud effects in imaging and targeted object appreciation. They are able to overcome some of the limitations encountered by other means of aerial and in situ observations. For instance, satellite observations can be constrained by the sensor's spatial and spectral resolutions, atmospheric conditions, revisit time and cost (Domaille and Campion, 2018). For the drone to achieve this there are some auxiliary equipment and configuration needed to ensure it has the capability of performing the effective function of surveillance and detection.

The incorporation of infra-red/night vision technology can aid in its visibility in unlit areas or at night. Such human surveillance activities have been performed for some time by the military and by civilian police forces and the technology is now crossing over into commercial use. According to Guarnera (2023), applications such as "Drone in a box" are becoming available (where surveillance drones are flown and charged autonomously as an alternative to patrolling sites). Drone technology is already in limited use with many network operators and tower owners although its applications are far from ubiquitous (Passifiume, 2017). To date, the use of drones in telecommunication industries has focused on the "drone technology" itself. Focus is now being shifted to how the output from drone surveillance can be better utilized in telecomm infrastructure theft detection. This is so because drones have now become more accurate, reliable, self-aware (in respect of their surroundings) and better at capturing images (Bleiberg, 2014). Such drones can be used to obtain reliable and real time information by triggering signals about physical objects through the process of recording, measuring and interpreting photographic images. Both drone technology and photogrammetric software modeling technology have evolved sufficiently which has made it possible to create accurate representations of three dimensional structures (such as towers, communication masts) from the image and positioning data collected by drones. The images are post processed (usually as a service-triggering alarm) and the output is then made available to decision makers (Chris, 2023).

The telecommunications industry plays a vital role in keeping us connected, and the integration of drones into this field is revolutionizing how we maintain and expand these networks. As drones in telecommunications industry become increasingly prevalent, they are transforming the way companies approach tower inspections, network expansions and emergency response time.

With benefits such as efficient tower inspections, improved network planning and cost savings, the use of drones in the telecommunications industry has grown rapidly.

According to Rejeb (2023), the use of drones with smart intrusion detection and alarm systems to curb theft and vandalism of Telecomm infrastructures has helped to eliminate the following challenges associated with the traditional human-based methods:

i. Cost Savings: Drones offer significant cost savings in the telecommunications industry by reducing the need for manual labour and expensive equipment. They can quickly perform tasks that would otherwise require specialized equipment or teams of technicians, such as tower inspections, mapping and network planning. Additionally, drones can minimize downtime by identifying issues before they cause network outages thereby reducing maintenance costs,

ii. Improved Safety: The use of drones in telecommunications greatly enhances worker safety. Climbing towers for inspections and maintenance can be dangerous and accidents can result in injuries or even fatalities. Drones eliminate the need for technicians to climb towers in many cases, reducing the risk of accident and promoting a safer work environment,

iii. Increased Efficiency: Drones can perform tasks more quickly and accurately than humans, increasing efficiency in the telecommunications industry. They can inspect towers, map terrain and test signal strength in a fraction of the time it would take a team of technicians. This improved efficiency allows companies to better allocate resources and focus on other critical aspects of their operations,

iv. Better Data Collection: Drones equipped with advanced sensors and cameras can collect valuable data that can be used to optimize networks, monitor infrastructure and plan future expansions. High-resolution imagery, 3D models and signal strength data provide companies with the information they need to make data-driven decisions and improve their operations.

The disabling of critical communications networks due to vandalism and theft has a significant impact on essential public services like emergency response, health care, energy grids and public transportation which can lead to broader societal costs and potential risks to public safety. The vandalization of these public infrastructures can lead to service disruptions, increased service charges, revenue decline, increased expenditure on security measures and erosion of public trust (Schwung, 2022).

2. Materials and Method

2.1 Materials

The materials used for this research includes:

Corresponding author's email address: gambo.anthony@yahoo.com

2.1.1 UAV system

UAVs are particularly useful in areas where landing and take-off runs are impossible and they are also portable. The high power consumption for hovering flights relatesto their flight durations (typically to one hour based on electric motors and rechargeable batteries), although the largest platforms can accommodate larger fuel capacity. Control is typically via line-of-sight and for a quick analysis. They are readily deployable using a one or two-man crew for the programmed intrusion/vandalism detection mission. The modeled and dimensioned 3-D structure of the UAV system is as shown in Figure 1.

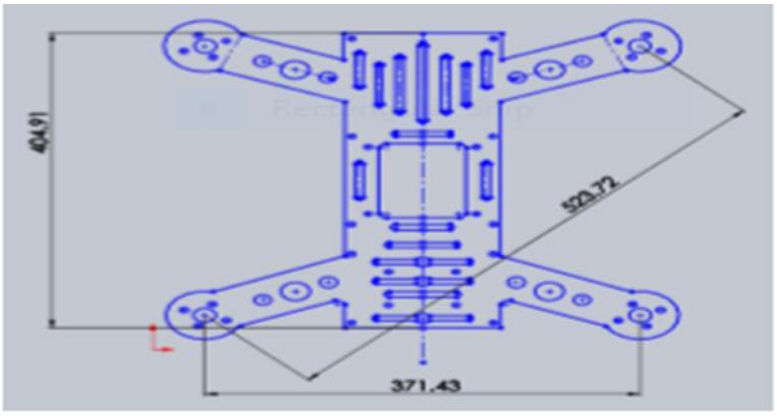

Figure 1: 3-D Modeling and dimensioning of the UAV System

2.1.2 Development board

The development board used in the UAV system to perform autonomous intrusion/vandalism detection was the Arduino Uno Rev.

2.1.3 Global positioning system

The Arduino GPS shield is a GPS module breakout board designed for Global Positioning System tracking as shown in Plate 1. It requires a supply voltage of 5V and operates at a baud rate of 38,400 bps. It has an onboard SD card slit for data storage and often stacked on top of the Arduino board placed on the UAV system.

Plate 1: GPS shield and Antenna mounted on Arduino Uno Rev

2.1.4 Xbee

A pair of Xbee Pro 900 HP wireless modules is used to establish wireless communication between the UAV unit and the Host PC at the remote base station. The basic parameters of the module are shown in Table 1.

Corresponding author's email address: gambo.anthony@yahoo.com

Table 1: Relevant parameters of the Xbee Pro HP module

PARAMETERS	SPECIFICATIONS
RF Band Rate	900MHz
RF Data Rate	10 kpbs 0r 200 kbps
Indoor Urban Range (2.1 Db Antenna)	10 kpbs up to 2,000 ft (610 m) 200 kpbs up to 1,000 ft (305m)
Outdoor LOS Range (2.1 Db Antenna)	10 kpbs up to 9 miles (15.5km) 200 kpbs up to 4 miles (6.5km)
Supply Voltage	2.1V – 3.6V
Transmit Voltage	215Ma
Receive Voltage	29Ma

2.1.5 Motor shield

A Mega motor shield for Arduino was used to connect the 12V motors to the 12V lead acid battery. The motor shield draws its power supply from the 12V lead acid battery and feeds that to motors 'A' and 'B' of the UAV system depending on the logic signal it receives from the program uploaded into the Arduino Uno Rev as shown in Plate 2.

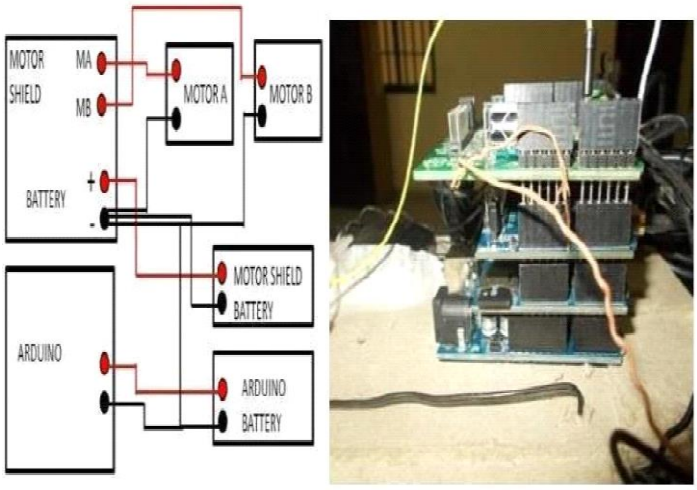

Plate 2: Connections for mega motor shield and mega motor shield stacked on arduino uno rev

2.1.6 Magnetometer

Plate 3 depicts a magnetometer which used to ensure an accurate 180 degrees turn in the opposite direction after the completion of the patrol so that the UAV system can patrol in the opposite direction.

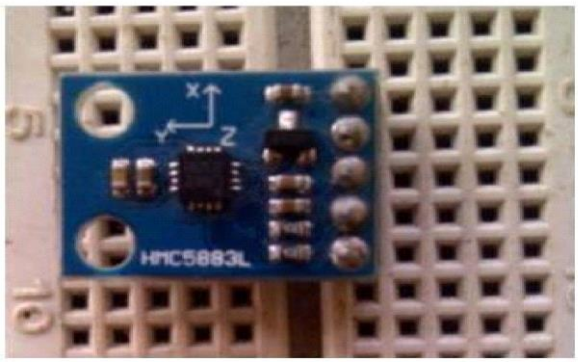

Plate 3: Magnetometer

2.1.7 Ultrasound sensor

The HC-SR04 as depicted in Plates 4(a) and 4(b) are ultrasound sensors which are capable of transmitting and receiving ultrasound waves. During patrol, using the HC-SR04 Sensor, if the UAV system detects an obstacle

less than 35cm in front of it, it takes a detour route to avoid the object before continuing along its patrol route.

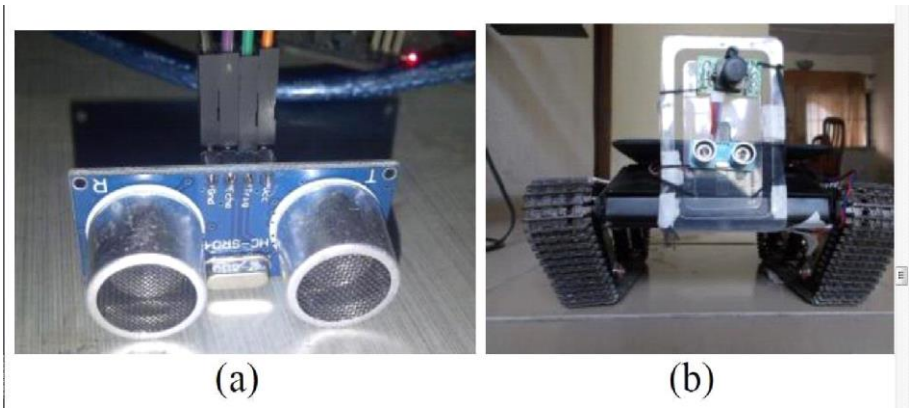

Plate 4: HC-SR04 Sensor

2.1.8 Camera

The LS-Y201-Infrared camera as shown in Plates **5**(a) and **5**(b) captures high resolution pictures using serial port. The infrared feature has a built-in sensor to sense the ambient light and will automatically turn on infrared LEDs when light intensity is low. It requires a power supply of 3.3V or 5V, a current consumption rate of 80 – 200MA and a serial baud rate of 38,400 bps and the image resolution is set to 320×240 pixels (Yin, 2013).

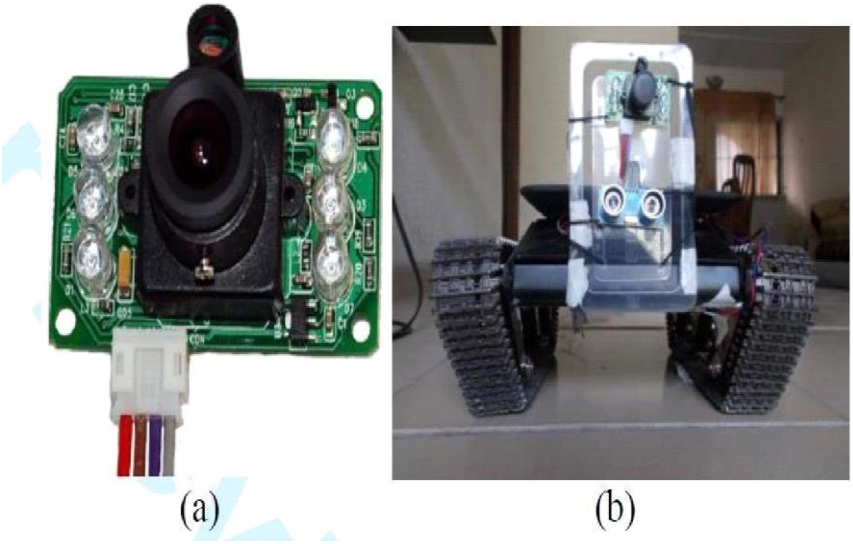

Plate 5: LS-Y201-Infrared Camera

2.1.9 Solar panel

In other to maintain continuous power supply to the UAV system, a solar panel was incorporated into the system. The solar panel has an output power of 8W, an output voltage of over 18V and an output current of 450 mA. It is made from polycrystalline cell and keeps batteries charged for optimum performance.

2.2 Method

The schedule of the research methodology for this research work ranged from the feasibility study on drone surveillance application, UAV configuration, sensor integration and testing procedures.

2.2.1 UAV System requirements

The hierarchical decomposition of the UAV system which ranges from power, propulsion, structures, Guidance, Navigation and Control (GNC), payload, battery, Inertial Measurement Unit (IMU), flight computer, radar, motors, Global Positioning System (GPS), body, arms and landing gear is as outlined in Figure 2.

Corresponding author's email address: gambo.anthony@yahoo.com

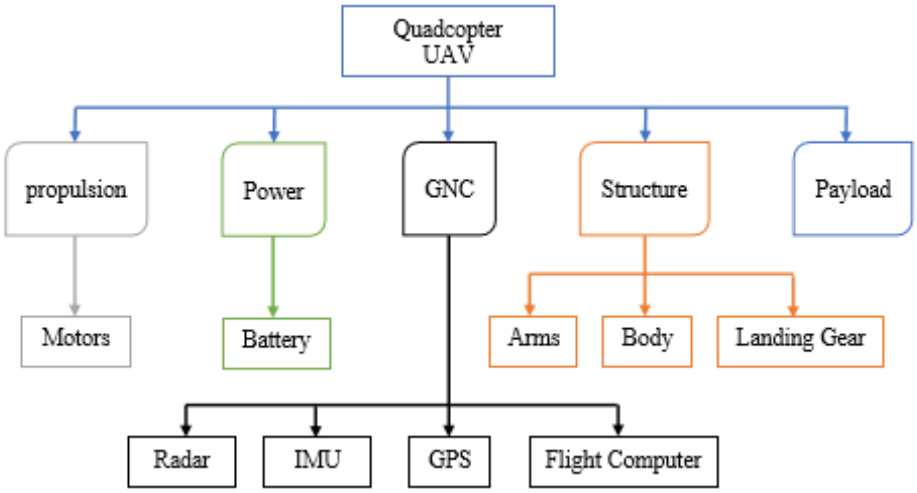

Fig. 2: Hierarchical decomposition of the UAV System

2.2.2 *Technical specifications*

The set of key performance indicators which are capable of describing the performance competence of the UAV system is as outlined below in Table 2.

Table 2: Design Specifications of the UAV System

Specifications	**Values**
Dimensions	405mm X 371mm X 70mm
Weight	1000g
Power	200W
Rotors	4
Propellers	10" X 4.5" (10" in diameter and 4.5" in pitch)
Battery	3300mAh (C) 3S LiPo 35C (Max)
Controller	Arduino Uno Rev 3
Payload Mass	150g
Diagonal Size (Propellers excluded)	520mm
Motors (for medium size UAV of 500mm)	A2212 brushless out runner dc motor, 1000Kv. No load current @ 10V:0.5A. Thrust @ 3S with 1045 propeller 800gms approx..
Current Capacity	12A/60s
Motor Dimensions	27.5 X 30mm
ESC Specification	18A (30A Recommended)
Propellers RPM	7536 RPM
Input Voltage	11.1V
Pitch Speed	32.1 MPH (51KMH)
Efficiency	80%
Weight to be lifted by the UAV	2Kg or more
Flight Time	Up to 15 minutes

2.2.3 *Flight dynamics*

Figure 3 depicts the UAV flight dynamics that was taken into cognizance as defined by the inertial frame. UAV's position with respect to the ground al**o**ng with the gravity pointing in the negative Z-direction and the body frame which was defined by the UAV's different orientations. We also considered six degrees of freedom which described any time space motion of a rigid body in motion. It was made up of three translational motions that made the UAV move longitudinally (forward and backward), vertically (upward and downward) and laterally (right and left). In addition, there were three rotational motions along three axes which made the UAV move rotationally among each axis to produce roll, pitch and yaw movements.

Corresponding author's email address: gambo.anthony@yahoo.com

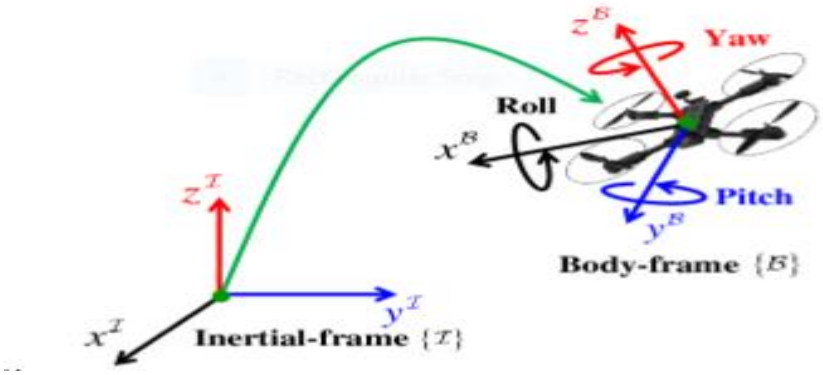

Figure 3: The relative orientation between inertial frame and body frame of a UAV in 3D Space

2.2.4 Testing procedures

The experimentation was carried out in accordance with the procedures of Dmitry*et al.*, (2018). As the UAV system moves towards the telecommunication intrusion/vandalized site, it simultaneously checks for any intrusion using the HC-SR04 sensor mounted in front of the UAV. On detection of any intrusion/vandalism, it stops and takes pictures of such intrusion/vandalism via the LS-Y201-Infrared camera which captures high resolution pictures using serial port. Images and GPS location of the intrusion site are sent wirelessly to the host PC at the base station via the Xbee modules and such intrusion can be verified from the acquired images. Similarly, during patrol, the unit constantly checks to ensure that it was travelling in the correct direction using the onboard magnetometer and if the unit drifts away from its original direction, a path adjustment algorithm was employed to return it to the correct direction. Furthermore, the UAV system was programmed to autonomously detect and avoid obstacles along its surveillance path using HC-SR04 sensor. In the event of obstacle detection less than 35cm away from the UAV system, it takes a detour route to go around the obstacle before resuming its patrol. Upon arriving at the end location, the UAV system turns 180 degrees using information provided by the onboard magnetometer. After turning, the system waits at a preset time interval of 30minutesbefore patrolling the intrusion site again on a return mission. The GPS data for the end and start locations were interchanged so that the unit can patrol in the opposite direction. In every one hour, the UAV system patrolled the 150m stretch of the intrusion site for approximately 5 minutes. The UAV system will be able to detect any intrusion/vandalism, capture 320 × 240 pixel images of the intrusion/vandalism site and transmits the intrusion/vandalism GPS location and images to a PC at a remote base station, 100m away from the intrusion/vandalism site within 10 seconds.

The GPS latitude of the surveillance route ranges from 5.53986°–5.53977°. When the UAV system detects an intrusion or physical tampering of the infrastructure, its GPS longitude may range from 5.82597°–5.82525°. The variation from its pre-set range signals an intrusion or physical tampering will automatically make the UAV system to wirelessly issue an alarm message to the host PC at the remote base station, signaling the surveillance team that an intrusion or physical tampering has been detected. After alerting the surveillance team to the presence of an intrusion, the UAV system will continue its patrol of assigned surveillance route. In addition to the GPS location of the intrusion, the system will also capture 320 × 240-pixel image of the intrusion and then transmit a picture of the vandalization or intrusion taken by its onboard camera module within the 10 seconds. So not only does the surveillance team know that an intrusion has occurred and its location, they are also to visually see the vandalized or intruded section of the infrastructure. The base station was located approximately 100m away from the surveillance route and the remote PC with the receiving Xbee module was at the base station.

The decision-making model of the UAV system that can be commercialized is shown in Figure 4. When the UAV system is initialized, it obtains its current location using Global Positioning System (GPS). It also obtains the GPS location of the Start and End points of the intrusion/vandalization it is assigned to detect as well as its orientation using the onboard Magnetometer. North, South, East and West orientation information was also acquired by Magnetometer, which assures that the UAV system is travelling in the correct direction.

Corresponding author's email address: gambo.anthony@yahoo.com

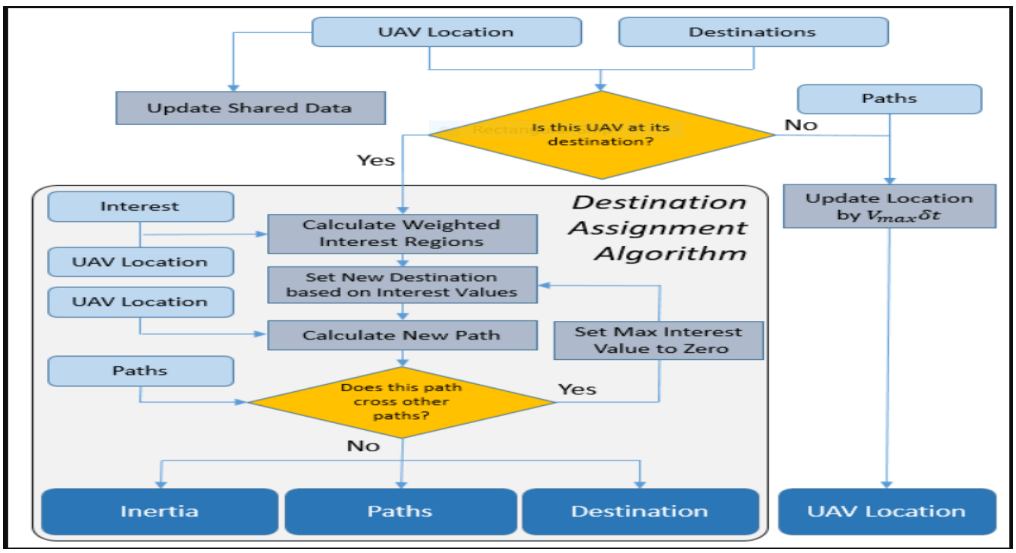

Figure 4: Decision-making model of the UAV

3. Results and Discussions

The ability of the UAV System to proffer short-, medium- and long-term solutions was evaluated under the following criteria:

3.1 Surveillance Patrol

The ability of the UAV to continuously and successfully patrol along or beside telecommunication infrastructure reveals that it takes about 5 minutes for the UAV to complete a programmed 150m autonomous patrol. This result is in agreement with the works ofJoshi (2019) in their study they stated that once the unit completes its surveillance patrol, it stops and turns 180 degrees to face the opposite direction within 5 minutes.

3.2 Power Test

The 12V battery of the UAV system was measured before and after the completion of the 150m patrol. During time intervals between patrols, an 18V solar panel will charge the 12V battery to ensure continuous availability of power supply between patrols. For every 150m programmed patrol, 15 minutes of solar charging is required to restore the battery back to its initial voltage as stated elsewhere (Bleiberg, 2014). Table 2 gives the result of the battery test for the UAV during the surveillance patrol.

Table 2: Battery test for UAV system during and in-between surveillance patrol

Initial Battery Voltage (V)	Patrol Time (m)	Patrol Distance (m)	Battery Voltage after Patrol	Solar Charging Time (m)	Final Battery Voltage (V)
12.92	5	150	12.65	15	12.92
12.92	5	150	12.65	30	12.98

3.3 Obstacle Avoidance

The HC-SR04 ultrasonic sensor on the UAV system was programmed to automatically alert the unit in case of an obstacle in front of it. A detour route to avoid the obstacle was taken by the UAV when the sensor detects any obstacle less than 35cm in front of the UAV system. This is in agreement with previous works by Stewart, (2018).

4. Conclusion

The research has delved into the many ways drones are revolutionizing the telecommunication industry. A survey of current drone detection and classification techniques indicates a fast-expanding area characterized by considerable technological advances and novel approaches. The fast development in the usage of UAVs has prompted serious issues about privacy, security and safety. As a result, developing effective UAV detection algorithms has become critical. The paper has offered an overview of several UAV detection approaches, such as radar-based, acoustic-based, RF-based and visual-based approaches. However, the discussion also emphasized the inherent challenges that persist. The size and speed diversity of drones, their dynamic behavior

Corresponding author's email address: gambo.anthony@yahoo.com

and similarity to other flying objects and their limited battery life make the detection task more challenging. Additionally, different interference factors in real-world scenarios, including adverse weather and lighting conditions, urban locations with plenty of obstructions such as buildings and trees, ambient and background noise, wind, the presence of wireless communication signals from Wi-Fi and Bluetooth sources, bird echoes, etc, present unique challenges for each detection modality. It is believed that this review article will be a helpful resource for academics, engineers and policymakers working in UAV detection and classification.

References

Bleiberg, J. 2014. New innovations that could change the world. Availability in https://www.brookings.edu/blog/techtank/2014/06/10/10-new-innovations-that-could-change-the-world/ accessed on 30 October, 2024.

Chris G. 2023. Connecting the world: How Drones are Revolutionizing the Telecommunications industry. https://www.bluefalconaerial.com/home/contact/. accessed on 5 May, 2023.

Dmitry Y. Tyugin, AA. Kurkin, VD. Kuzin, DV. Zeziulin, VS. and Makarov, RV. 2018. The Exploration of Autonomous Mobile Robot Movement": Characteristics in Difficult off-road conditions of a Coastal Zone. *International journal of Imaging and Robotics*, 18(1).

Domaille, S. and Campion, D. 2018: Droning On: A review of UAV use in recent surveillance attended by ITOPF and considerations for the future.Available in https://www.itopf.org accessed on 20 January, 2025.

Guarnera, F. 2023: Drone in a box: An overview of use and applications of UAV for Telecommunications infrastructure surveillance patrol.*International Journal of Imaging and Robotics,* 11(4).

Joshi, D. 2019. Drone Technology: Uses and Applications for Commercial, Industrial and Military Drones in 2020 and the Future. Availability in https://www.businessinsider.com/drone-technology-uses-applications accessed on 30 October, 2024.

Michail, P., Avraam, C. and Dimitrios, P. 2019. UAV flight control based on Arduino board implementations.*International Journal of Engineering Applied Sciences and Technology*, (4)5: 438-443.

Passifiume, B. 2017. University of Calgary Professor Developing New Drone Technology. Availability inhttps://calgaryherald.com/technology/science/vision-based-navigation-is-just-like-in-humans-calgary-professor-developing-new-drone-technologyaccessed on 7 January, 2025.

Rejeb, A., Rejeb, K., Simske, S.J. and Treiblmaier, H. 2023. Drones for supply chain management and logistics: A review and research agenda. *Int, J. Logist. Res. Appl.* 26: 708 – 731

Schwung, M., Lunze, J. 2022. Cooperative Control of UAVs Over an Unreliable Communication Network. *IEEE Aerosp. Electron. Syst. Mag.* 37: 20 -34

Stewart, D. 2018. The use of drones in telecoms. Availability in befutureready@techmahindra.comaccessed on 17 November, 2024.

Yin MM. 2013. Development of Process Control with Obstacle Avoidance Behavior in Autonomous Mobile Model. *International Journal of Imaging and Robotics,* 10(2).

Corresponding author's email address: gambo.anthony@yahoo.com