ISSN: 2321-2152

IJMECE

International Journal of modern electronics and communication engineering

E-Mail
editor.ijmece@gmail.com
editor@ijmece.com

www.ijmece.com

ISSN 2321-2152
www.ijmece.com
Vol 13, Issue 1, 2025

AUTONOMOUS SURVEILLANCE DRONE WITH IOT AND AI

CHERUKURI SAI JAYANTH [1] , GOLLA PARTHA SARADHI [2] , GUVVALA ARUN [3] , KOTRA SAKETH RAM [4] , SHAIK AFROZ [5] , S. IMRAN BASHA [6]

[12345]UG STUDENTS, DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING, DR.K.V.SUBBA REDDY INSTITUTE OF TECHNOLOGY, KURNOOL,AP, INDIA.

[6]ASSISTANT PROFESSOR, DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING, DR.K.V.SUBBA REDDY INSTITUTE OF TECHNOLOGY, KURNOOL,AP, INDIA

Abstract: This project leverages an FPV (First Person View) drone to monitor a college campus and detect individuals and vehicles in restricted areas using a live video feed. The drone streams video to a laptop, where a YOLO (You Only Look Once) deep learning algorithm processes the feed to detect persons and cars. If unauthorized activity, such as roaming outside classrooms or parking in undesignated areas, is detected, the system captures images and sends alerts with snapshots to authorities via a Telegram bot. This system enhances campus security and ensures compliance with rules in real-time.

1. INTRODUCTION

Monitoring and maintaining discipline in a large college campus can be challenging. Drones offer an efficient solution for surveillance, and when coupled with advanced AI algorithms like YOLO, they can identify specific objects in real-time. This project aims to automate campus monitoring by using a drone to detect individuals and vehicles in prohibited areas and notify authorities with actionable alerts, reducing the need for manual monitoring and enabling swift intervention.

Drones, also known as Unmanned Aerial Vehicles (UAVs), are aircrafts that can fly without the need for apilot. They are now used in a wide range of industries, including agriculture, economics, military, and many otherfacets of life [1]. Among them, security and surveillancehave proven to be one of the most essential uses for UAVs[2]. They have the potential to enhance security systems by performing high-risk activities, emergency response to various circumstances, and capturing and giving real-time video and photographs from the accident scene. This potential can even be expanded to new horizons with the help of Internet of Things (IoT).In 2017; University Technology Malaysia (UTM) launched a project called Comprehensive IoT Based Security solutions aimed to provide advanced and comprehensive security solutions to UTM campus. Figure1 shows the scheme of Future Campus Security bySecurity Division. Some of these systems such as Guard Touring System (GTS), Radio Frequency Identification (RFID) Vehicle Sticker and IoT-based Office Access Solutions have been successfully implemented while, others including Smart Barrier, Internet Protocol (IP) Walkie Talkie, Body Cam, Vehicle Enforcement System and Guard Analytics are currently underway. The IoT based ground patrolling system hassignificantly improved the conventional UTM securitysystem. However, UTM Johor Bahru campus comprises a steep terrain, oil plantations, woodlands and several buildings, all of which must be constantly monitored bythe UTM Security Division. Several areas aren't accessible by security guards due to possible hazards posed by the terrain itself, intruders or wild animals. In addition, fast response to emergencies is absent which may exacerbate the problem.

Another disadvantage shared by the majority of similar solutions and projects is a limited communication range. The radio frequency-

based telemetry that is typically utilized to communicate between the drone and groundcontrol stations has a range of a few kilometers and becomes significantly shorter when obstacles such as buildings are present. It is also prone to interference as the frequency allocated occupies the unlicensed spectrum. In addition, the existing drone solutions for aerial patrol in the market are offered in silo and detached from the ground Patrol systems Therefore, in this paper, we introduce a novel design of an autonomous drone for campus security, named JAG Drone, that uses cellular communication for its control, telemetry and data transfer. Furthermore, the drone utilizes Internet-of-Things (IoT) computing infrastructure to facilitate real-time data management and also scalable application such as integration with existing UTM's IoTbased Guard Touring System. The remainder of this paper is structured as follows. Section 2 contains the project background. Section 3 and Section 4 contain the methodology for the drone design and results, respectively. Section 5 concludes the paper.

Drones or unmanned aerial vehicles (UAVs) are aircrafts that can operate without onboard pilots. A typical unmanned aerial system consists of vehicle, ground control station (GTS) and communication system that links the two. UAVs can be operated remotely by human or autonomously by onboard computers [3]. UAVs are used in a wide range of applications, including security [4] and surveillance [5], detection of harmful gases, medicinal reasons, agricultural, and deliveries. Drones can be generally classified into two types, fixed wing and rotary wing. These two classifications can be further subdivided or even merged to create additional aircraft types such as vertical take-off and landing (VTOL) aircraft.

Drone kit python library is used to control the Pixhawkflight controller by sending MAVLink commands through the serial port between the Raspberry Pi microprocessor and the flight controller. This communication is bi-directional where Raspberry Pi can send and receive data. For example, Raspberry Pi can send commands such as takeoff, land, change mode, go to location and many more, while simultaneously receiving flight status such as altitude, position, speed and etc.

As mentioned in the methodology, the eCalc simulator issued to estimate the drone performance and important parameters such as flight time, speed, current and excitable 2 summarizes the performance comparison between the simulated results with the ones obtained from actual flight tests. As can be seen, the actual results are surprisingly close to the simulation results. This justifies the use of simulation tools to assist in the drone design as the simulated outcomes can be used as a baseline to achieve the desired result.

Autonomous response to emergencies is tested severalties, and the results shows that the drone is capable to autonomously navigate in the incident location. Figure 12shows one of the tests in which the security guard pressed the panic button, and hence the drone took off and flew to the incident spot. Once the drone reaches the emergency site, it can follow.

2. LITERATURE SURVEY

In recent years, drone technology has gained popularity across the world because of its numerous applications, particularly insecurity and surveillance. This technology can be further revolutionized with the deployment of Industrial Revolution 4.0 Technology. This paper discusses the development of an IoT-based autonomous drone for more comprehensive campus security and surveillance system. The drone is featured with the capability of conducting a fully autonomous aerial surveillance, being the first responder in emergencies, streaming

video while flying, avoiding obstacles, following a target and communicating with the current IoT based UTM's security patrolling system for data transfer and drone control. This has been accomplished by using the open source ArduPilot software, Pixhawk flight controller along with Drone kit python library installed on a Raspberry Pi 4. The findings show that the actual performance of the designed drone is fairlysimilar to the simulation results. The drone has successfully performed autonomous navigation to incident location with 1 to 2 meter accuracy as well as follow-me mode. The cellular technology utilized for drone communication also is more robust and provides promising solution to overcome short operation range and interference.

People counting and tracking systems are increasingly in demand for surveillance applications. However, current systems suffer from several limitations. They are often centralized, which makes them vulnerable to disruption and difficult to mobilize. This paper presents a cutting-edge smart security system prototype that addresses these limitations. The system is decentralized, by using lightweight algorithms to process images locally on smart cameras. This makes it more reliable and scalable, and it also enables new features such as crowd recognition, noise detection, intruder identification, and people counting. The system is also integrated with the Internet of Things (IoT), Artificial Intelligence (AI), and Unmanned Aerial Vehicle (UAV) technologies to improve further its performance and user experience. For example, the system can use drones to deploy cameras to remote or difficult-to-access locations, and it can use AI to analyze camera data in real time to identify potential threats. The proposed system has been tested on the Hashemite University campus, with cameras placed throughout the campus and a drone station located at the faculty of engineering. The test results have been encouraging, indicating that the system has great potential for improving security in a variety of settings. The paper also investigates and analyzes critical observations made throughout the implementation and testing phases. These observations can be used to guide the development of future security systems.

People counting and tracking systems are increasingly in demand for surveillance applications. However, current systems suffer from several limitations. They are often centralized, which makes them vulnerable to disruption and difficult to mobilize. This paper presents a cutting-edge smart security system prototype that addresses these limitations. The system is decentralized, by using lightweight algorithms to process images locally on smart cameras. This makes it more reliable and scalable, and it also enables new features such as crowd recognition, noise detection, intruder identification, and people counting. The system is also integrated with the Internet of Things (IoT), Artificial Intelligence (AI), and Unmanned Aerial Vehicle (UAV) technologies to improve further its performance and user experience. For example, the system can use drones to deploy cameras to remote or difficult-to-access locations, and it can use AI to analyze camera data in real time to identify potential threats. The proposed system has been tested on the Hashemite University campus, with cameras placed throughout the campus and a drone station located at the faculty of engineering. The test results have been encouraging, indicating that the system has great potential for improving security in a variety of settings. The paper also investigates and analyzes critical observations made throughout the implementation and testing phases. These

observations can be used to guide the development of future security systems.

We present Autonomous Surveillance Drone, a new approach to serve purpose of UAV surveillance. Instead, just sending video stream from drone to display device at user's side we have developed complete system to get insights from video stream. Our system architecture is extremely simple and biggest reason for this is platforms provided by Nvidia and Microsoft, throughout this paper we are demonstrating all results/outputs using services and hardware provided by Nvidia and Microsoft. We are using the Nvidia's Jetson Development board to compile our inference part(object detection using YOLO-V3) along with stream and metadata fetch at remote terminal, Jetson nano is our IoT edge device, to connect edge device and the remote terminal we are using Microsoft Azure IoT hub (Cloud Service

The integration of drone technology, IoT, and AI can revolutionize smart town surveillance systems by reducing costs and improving response times to crime. The development of human-friendly drones and IoT technology enables automated city supervision, while the integration of AI allows for immediate reports and actions, overcoming human limitations. Drones can continuously monitor different areas, detecting crime hotspots and providing a substitute for city policies. This smart surveillance system can improve emergency management and ensure a regulated and competent surveillance management approach. Ultimately, this technology can enhance the safety and security of smart towns, making them more effective, efficient, and reliable. The framework of the suggested intelligent surveillance system relies on the utilization of real-time data collection and analysis, integrating drone technology, IoT devices, and AI. The research showcases the system's efficacy in identifying and addressing criminal activities, making it an invaluable resource for law enforcement agencies. By combining these technologies, surveillance management can become more dependable and effective, ultimately contributing to the advancement of safer and smarter cities. The paper presents a comprehensive outline of the framework and its execution, providing a blueprint for future researchers and stakeholders to replicate and expand upon this endeavor. In this study, we present a superior surveillance system framework that is also implementable.

3. EXISTING SYSTEM

Drones or mini-unmanned aerial vehicles, have becoming an emerging trends due to their boundless applications in surveillance, military and numerous public services. Nowadays, deployment of surveillance drone for monitoring or security application remains challenging and

ongoing research. As Internet of Things (IoT) becomes more commercialized, various concept of IoT have been integrated with the drones due to efficient usage. Therefore, this paper proposed the development of surveillance drone system based on IoT for industrial monitoring-security applications. The rationale of integrating IoT with surveillance drone is that it allows authenticated users to login from any device, anywhere, and view video or images from surveillance drones in real-time for security awareness. In this work, the surveillance drone consists of mechanical system, electrical and electronic interfacing and IoT platform (mobile application system). In electronic system, power module, communication module, sensor and actuator as well as user interface module have been adopted and integrated into the systems. Besides, in software development system, user interface configuration was developed through mobile application to serve as IoT platform. A series of

ISSN 2321-2152
www.ijmece.com
Vol 13, Issue 1, 2025

experiments shows that the surveillance drone based IoT able to operate with a promising flying distance with surveillance camera as the “eyes” of the drone system.
Unauthorized activities, such as students loitering outside classrooms or vehicles parking in restricted zones, disrupt the campus environment and pose safety concerns. Manual surveillance is labor-intensive and often ineffective over large areas. An automated system using drones and AI can provide a real-time, efficient, and scalable solution for monitoring campus activity

4. PROPOSED SYSTEM

Drone Video Capture
The FPV drone, equipped with a high-definition camera, captures live video footage of the campus.
The video feed is transmitted wirelessly to a laptop or computer in real time via an FPV system or Wi-Fi module.
Video Streaming and Preprocessing
The laptop receives the video feed and processes it using Python libraries such as OpenCV.
Frames are extracted from the live feed and prepared for object detection.
Object Detection Using YOLO
The YOLO (You Only Look Once) deep learning model processes each frame to detect objects such as persons and cars.
Detected objects are highlighted with bounding boxes, and their class labels (e.g., "Person," "Car") are assigned.
Violation Identification
Logic is applied to identify specific violations, such as:
Persons: Students loitering in hallways during class hours.
Cars: Vehicles parked in unauthorized areas (e.g., grounds or near classrooms).
Time and location data (if available) are logged for each detected violation.
Capture Evidence
For each detected violation, the system captures a snapshot of the relevant frame.
The snapshot includes annotated bounding boxes and labels for clarity.
Generate and Send Alerts
The system prepares an alert message containing:
A description of the violation.
The captured snapshot as evidence.
Additional details such as time and approximate location.
The alert is sent to a designated Telegram account using the Telegram Bot API.
Notification to Authorities
Authorized personnel receive the alert in real-time on their mobile devices through the Telegram app.
The alert enables them to take immediate action, such as addressing the violators or notifying security teams.
Continuous Monitoring
The drone continues to stream video, and the system processes it in a loop, ensuring real-time surveillance and violation detection.
.The proposed system of this project is shown in Fig 1.

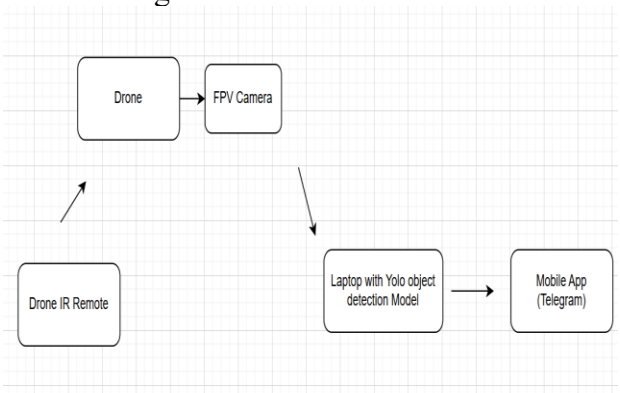

Fig 1 Block Diagram

5. WORKING FLOW STEPS

Drone Video Capture:
The FPV drone captures live video using an onboard camera.
The video feed is transmitted to a laptop via a wireless FPV system or Wi-Fi module.
Video Processing on Laptop:

The YOLO algorithm processes the video feed in real-time to detect persons and cars.
Bounding boxes are drawn around detected objects, and their positions are tracked.
Violation Detection:
Logic is implemented to identify violations, such as individuals in hallways during class hours or cars parked in unauthorized areas.
Alert System:
When a violation is detected, the system captures an image of the scene.
The image and details of the violation (e.g., time, location) are sent to a designated Telegram account.
Authority Notification:
Authorized personnel receive alerts on their mobile devices via the Telegram bot, enabling quick action.

6. CONCLUSION

The system successfully detects persons and vehicles in real-time using the YOLO algorithm, with high accuracy and minimal latency. Violations are flagged, and alerts with snapshots are sent to the Telegram account of authorized personnel within seconds, enabling prompt corrective actions. This FPV drone-based monitoring system offers an efficient and automated solution for campus surveillance. The integration of deep learning with real-time video streaming ensures accurate detection and fast response to unauthorized activities. Future improvements could include enhanced violation detection logic, integration with campus maps for precise location tagging, and deployment at multiple sites for broader coverage.

REFERENCES

[1] G. Ding, Q.Wu, L. Zhang, Y. Lin, T. A. Tsiftsis, and Y.-D. Yao. An Amateur Drone Surveillance System Based on Cognitive Internet of Things, IEEE Communications Magazine, Volume (56), Issue (1), Jan. 2018.

[2] T. Lagkas, V. Argyriou, S. Bibi and P. Sarigiannidis. UAV IoT Framework Views and Challenges: Towards Protecting Drones as Things', Sensors, 2018, 18,4015.

[3] Shruthi , Soudha N, Khalid Akram, Mustafa Basthikodi, Ahmed Rimaz Faizabadi. IoT based automation using Drones for Agriculture, 2019 JETIR May 2019, Volume 6, Issue 5.

[4] A.K. Saha , J. Saha , R. Ray , S.Sircar , S. Dutta , S. P. Chattopadhyay , H. N. Saha. IOT-Based Drone for Improvement of Crop Quality in Agricultural Field, 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC). Las Vegas.

[5] Motlagh, N.H.; Bagaa, M.; Taleb, T. UAV-based IoT platform: A crowd surveillance use case.IEEE Commun. Mag. 2017, 55, 128–134.

[6] Kersnovski, T.; Gonzalez, F.; Morton, K. A UAV system for autonomous target detection and gas sensing. In Proceedings of the Aerospace Conference, Big Sky, MT, USA, 4–11 March 2017; pp. 1–12.

[7] Kumbhar, A.; Guvenc, I.; Singh, S.; Tuncer, A. Exploiting LTE-Advanced HetNets and FeICIC for UAV-assisted public safety communications. IEEE Access 2018, 6, 783–796.

[8] Dr.M.V. Sruthi "A NOVEL OPTIMIZATION TECHNIQUE TO LINEAR DISCRIMINANT REGRESSION FOR FACE RECOGNTION"

[9] Merwaday, A.; Guvenc, I. UAV assisted heterogeneous networks for public safety communications. In Proceedings of the Wireless Communications and Networking Conference Workshops (WCNCW), New Orleans, LA, USA, 9–12 March 2015; pp. 329–334