JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

UNMANNED GROUND INTRUSION DETECTOR

AKASH A S[1], AVINAV PRASAD[2], BHARATH KUMAR K[3] , CHIRANTH C[4] ,

SUMA SANTOSH[5]

Student, Department of Electronics and Communication Engineering, KSIT, Banglore, India[1-4]

Guide, Assistant Professor, Department of Electronics and Communication Engineering, KSIT, Bangalore, India[5]

ABSTRACT

Real-time monitoring for unauthorized physical intrusion is a critical security challenge, particularly in restricted or remote areas where conventional systems can be complex and costly. This paper presents the design and implementation of a low-cost, real-time ground intrusion detection system. The primary objective is to develop a prototype capable of sensing ground vibrations and instantly notifying a user both locally and remotely. The system architecture is centered on an Arduino UNO microcontroller, utilizing an SW-420 vibration sensor for disturbance input, a passive buzzer for the local audible alert, an HC-05 Bluetooth module for remote wireless notification to a paired mobile device and an ESP32 cam for live monitoring. The software employs edge-detection logic to process the sensor's digital output, ensuring that a single, precise alert is generated per intrusion event rather than continuous, redundant triggers. The resulting prototype successfully identifies vibration events that exceed a user-calibrated sensitivity threshold, concurrently sounding the alarm and transmitting an alert string to a smartphone. This work demonstrates a viable and highly accessible solution for small-scale security, providing an effective, dual-alert mechanism suitable for asset protection or temporary perimeter monitoring.

keywords : Arduino uno, Intrusion detection, Vibration sensor, Sw-420, Real Time Monitoring, Wireless Alert, Security system, Microcontroller

I. INTRODUCTION

The Unmanned Ground Intrusion Detector is a smart security system designed to detect unauthorized individuals in restricted or high-security areas without the need for constant human supervision. It uses multiple sensors such as infrared, ultrasonic, and vibration sensors to accurately sense movement or disturbances in the surrounding area. These sensors send signals to the Arduino Uno microcontroller, which processes the data and triggers appropriate actions when an intrusion is detected. A camera module is integrated into the system to capture real-time visuals of the detected area, allowing for visual confirmation of any suspicious activity. To enhance communication, a Bluetooth module is included to send instant alert messages directly to the user's mobile phone whenever an intrusion occurs. This ensures that the user can respond immediately, even from a remote location. Additionally, a buzzer is connected to the system to produce an audible alarm whenever motion or vibration is detected, thereby providing immediate local warning. The combination of these components makes the system effective in low-light, remote, and high-risk environments, offering continuous and reliable security coverage. This project provides an efficient, cost-effective, and automated solution for modern security needs. It is particularly suitable for borders, military bases, industrial zones, and critical infrastructures, where 24/7 human monitoring is difficult. In conclusion, the Unmanned Ground Intrusion Detector enhances security by combining advanced sensors, automation, wireless communication, and real-time alerts in one integrated system. An Unmanned Ground Intrusion Detector is a security system designed to detect foreign individuals in restricted areas. Eliminates the need for human supervision by using automated detection methods. Integrates sensors, for accurate real-time monitoring. Effective in low-light, 2 remote, and high-risk areas. Enhances security for borders, military bases, industrial zones, and critical infrastructure.

II. LITERATURE REVIEW

[1] The presents a method for detecting and tracking moving objects using thermal infrared video sequences. The proposed system is designed to work efficiently under low-light and night conditions where normal cameras fail. It uses advanced image processing and motion tracking algorithms to identify and follow targets in real time. The study emphasizes the importance of thermal imaging for continuous surveillance in dark or obscured environments. The method achieves high detection accuracy and stable tracking even with background noise. This approach is highly useful for border security and night surveillance systems. Conclusion: Thermal imaging combined with tracking algorithms improves detection performance in dark environments.

[2] This paper provides a detailed survey of multi-sensor fusion techniques used for perimeter intrusion detection in railway security systems. It discusses how combining sensors like infrared, vibration, radar, and sound improves the accuracy and reliability of detection. The authors analyze various fusion algorithms that integrate data from multiple sources to reduce false alarms. The study highlights the challenges in outdoor and high-speed environments and how sensor fusion helps overcome them. It also explores applications in smart surveillance systems and critical infrastructure protection. Conclusion: Combining different sensors offers robust detection and higher reliability for outdoor environments.

[3] This paper reviews recent developments in crowd density estimation and people-counting systems using image processing and deep learning methods. It explains how convolutional neural networks (CNNs) and other AI models are applied to detect, track, and count people in complex environments. The study compares different datasets, algorithms, and performance metrics for crowd monitoring. It highlights the use of deep learning to enhance accuracy, reduce errors, and adapt to varying crowd sizes and lighting conditions. The paper also discusses the potential applications in public safety and event management. Conclusion: Deep learning significantly improves the accuracy and reliability of crowd detection and density analysis.

[4] This paper reviews the latest research and advancements in multi-camera, multi-object tracking systems used for surveillance and security applications. It highlights how multiple cameras can be networked to monitor wide areas and track several moving targets 4 simultaneously. The study discusses the algorithms used for object association, motion prediction, and identity management across different camera views. It emphasizes the challenges of occlusion, lighting variations, and synchronization between cameras. The paper concludes that multi-camera systems provide more reliable and scalable security coverage than single-camera setups. Conclusion: Multi-camera tracking is essential for large-scale perimeter and public security applications.

[5] This paper presents an extensive survey of deep learning approaches for crowd counting and analysis. It reviews convolutional neural networks (CNNs) and other AI models that estimate crowd density and detect group movement patterns in complex environments. The study compares different architectures, training datasets, and evaluation metrics used in recent research. It shows that AI-based models can handle varying crowd densities, occlusions, and lighting conditions more effectively than traditional techniques. The paper also discusses real world applications in surveillance, event management, and public safety. Conclusion: Neural networks outperform traditional methods in detecting and analyzing group intrusions and crowd behavior.

[6] This paper introduces a method for detecting humans using aerial thermal imaging combined with fully convolutional neural networks (FCNs). The system is designed to identify human targets even in low-visibility or nighttime conditions. It processes thermal images captured from drones or aerial platforms to detect heat signatures with high precision. The authors demonstrate how CNNs enhance accuracy, reduce false detections, and perform effectively in harsh or cluttered environments. The research shows strong potential for search and rescue, defense, and surveillance applications. Conclusion: Thermal imaging integrated with CNNs provides highly accurate human detection under dark and extreme conditions.

[7] This paper proposes an automated system for detecting and tracking multiple humans in continuous image sequences. It uses vision-based algorithms and motion detection techniques to identify and follow targets in real time. The approach minimizes human supervision and improves the efficiency of surveillance operations. The authors discuss methods to handle occlusions, background noise, and varying lighting conditions effectively. The system achieves high accuracy in detecting multiple moving objects simultaneously. Such automation is vital for large-scale or remote security monitoring. Conclusion: Automated vision-based systems significantly enhance the efficiency and accuracy of human detection in security applications.

[8] This review paper focuses on multi-target tracking systems that use networks of cameras to monitor large and complex areas. It summarizes various algorithms for object identification, matching, and re-identification across multiple camera views. The study highlights the benefits of combining artificial intelligence with multi-camera systems to reduce blind spots and improve coverage. It also discusses synchronization and data fusion challenges in large-scale surveillance systems. The review concludes that integrating AI with camera networks provides more reliable and scalable intrusion detection. Conclusion: Multi-camera systems integrated with AI offer high efficiency and robustness for perimeter and area intrusion detection.

[9] This paper introduces a wireless sensor network-based “virtual fence” for detecting unauthorized entries along large boundaries or perimeters. The system uses distributed sensor nodes to monitor vibration, motion, or temperature changes in the environment. It provides a low-cost and energy-efficient alternative to traditional wired surveillance systems. The proposed design can operate in remote or harsh conditions where manual monitoring is difficult. The authors demonstrate that the network can accurately detect intrusions and send alerts in real time. Conclusion: Wireless sensor networks are an effective and energy-efficient solution for unmanned ground intrusion detection over large areas.

[10] This paper presents a comprehensive survey of intrusion detection systems (IDS) designed for networked unmanned aerial vehicles (UAVs). It classifies different IDS models based on architecture, detection techniques, and communication frameworks. The author discusses major challenges in UAV security, including limited computational power, data transmission security, and mobility constraints. The paper evaluates both signature-based and anomaly based approaches for UAV intrusion detection. It also explores various network topologies and their impact on detection performance. Conclusion: Developing efficient UAV-IDS systems requires balancing security performance with minimal computational and energy resources.

[11] This paper, "Intrusion Detection Systems for Networked Unmanned Aerial Vehicles: A Survey," presents an overview of existing Intrusion Detection Systems (IDS) designed for UAV networks. It explains how UAVs, though valuable in civilian and military uses, are highly vulnerable to cyber attacks due to their wireless and distributed nature. The authors classify UAV-IDS mechanisms based on components such as data sources, deployment strategies, detection methods, and intrusion types. Various IDS models—signature-based, anomaly based, specification-based, and hybrid—are reviewed with examples from prior research. The 6 paper identifies key challenges like detection latency, computational overhead, and effective threat modeling. Finally, it outlines future research directions focused on developing lightweight, efficient, and resilient UAV-IDS frameworks capable of maintaining high detection accuracy under constrained conditions.

[12] This paper presents a systematic literature review of intrusion detection systems (IDS) designed for Unmanned Aerial Vehicles (UAVs) using machine learning (ML) and deep learning (DL) techniques. It explores the main threats and vulnerabilities affecting UAV networks and evaluates the effectiveness of ML and DL algorithms in identifying such intrusions. The study categorizes existing research by algorithm type, dataset, and detection performance. It highlights that deep learning approaches often outperform traditional machine learning models in terms of accuracy and adaptability. However, challenges like limited UAV resources, data scarcity, and model interpretability remain. The paper concludes by suggesting hybrid and lightweight IDS frameworks for better real-time UAV protection.

[13] This paper introduces a deep learning-based intrusion detection system (IDS) designed to protect ROS 2-powered Unmanned Ground Vehicles (UGVs) from Denial-of-Service (DoS) attacks. Using a Large Language Model (LLM) to simulate adversarial DoS scenarios, the authors generate realistic attack data for model training. The framework applies rigorous data cleaning and feature engineering, emphasizing metrics such as burstiness and topic entropy to capture abnormal network behaviors. Four deep learning models—MLP, LSTM, CNN, and VAE—are evaluated, with the MLP achieving 97% accuracy and an AUC of 0.998. The paper highlights how interpretability tools like Integrated Gradients enhance understanding of model decisions.

[14] This paper provides an extensive survey of Intrusion Detection Systems (IDS) tailored for Unmanned Aerial Vehicles (UAVs). It examines the unique security vulnerabilities in UAV networks and classifies existing IDS approaches based on architecture, detection techniques, and deployment strategies. The authors review methods such as signature-based, anomaly based, and specification-based systems used to detect attacks. The study also analyzes current datasets, performance metrics, and real-world implementations of UAV-IDS. Key research challenges like resource constraints, detection latency, and scalability are highlighted.

[15] This paper proposes an AI-enabled Intrusion Detection System (IDS) framework to enhance the security of Unmanned Aerial Vehicle (UAV) networks. It leverages machine 7 learning and deep learning techniques to detect and mitigate various cyber threats targeting UAV communication links and control systems. The authors emphasize the integration of block chain technology to ensure data integrity and trust among UAV nodes. Extensive experiments demonstrate improved detection accuracy, reduced false alarms, and enhanced resilience against sophisticated attacks.

[16] This paper presents a hybrid intrusion detection system (IDS) combining deep learning and federated learning to enhance the cyber security of Unmanned Aerial Vehicles (UAVs). The proposed framework allows UAVs to collaboratively detect cyber attacks without sharing raw data, ensuring privacy preservation. It uses Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) models to identify both known and unknown intrusions with high accuracy. Experimental results show that the hybrid model achieves superior detection performance while minimizing communication overhead and latency.

[17] This paper presents an intrusion detection method for UAV airborne networks using an Improved Stratified Sampling and Ensemble Learning (ISSEL) approach. The model clusters normal data with KMeans++ and performs distance-based sampling to balance datasets without losing global features. It integrates five tree-based classifiers—Decision Tree, Extra Trees, Random Forest, GBDT, and XGBoost—combined through an adaptive F1-based weighting strategy. The ISSEL method achieved 99.42% accuracy and significantly improved detection of minority-class attacks.

[18] This paper introduces FIDSUS, a federated intrusion detection system (IDS) designed to enhance the security of UAV swarm networks in dynamic and resource-constrained environments. It tackles challenges of data privacy, communication instability, and client heterogeneity through federated learning (FL) with an affinity matrix that measures client similarity. FIDSUS enables collaborative learning among UAVs without sharing raw data, ensuring privacy and robustness. It integrates historical and current feature representations to mitigate model forgetting and improve adaptability.

[19] This paper conducts a systematic literature review (SLR) on machine learning-based intrusion detection systems (IDS) designed for the Internet of Drones (IOD). It analyzes 62 peer-reviewed studies published between 2014 and 2024, covering IDS types, algorithms, datasets, attack classifications, and software environments. The review identifies a significant rise in research activity since 2019, highlighting the growing importance of drone cyber 8 security. It classifies IDS models into traditional, hybrid, and deep learning-based approaches, emphasizing the shift toward adaptive and intelligent solutions.

[20] This paper presents a quantitative simulation framework to analyze the detection and mitigation of rogue UAV intrusions in 5G networks using Low Earth Orbit (LEO) satellite backhaul. It models hybrid terrestrial–non-terrestrial systems to evaluate latency, reliability, and the impact of satellite outages on border security operations. The study introduces a local fallback mechanism to reduce mitigation delays during backhaul outages. Results from Monte Carlo simulations show that fallback limits delays to 2 seconds, ensuring timely UAV lockdown

III. PROBLEM IDENTIFICATION

1. Heavy reliance on manual monitoring: Traditional security systems depend on human guards and operators, leading to human error, fatigue, and limited coverage for large perimeters.

2. Limited detection capability: Many current systems are optimized for individual intruders, not for detecting groups of people moving together, which is a common scenario in border security or large restricted zones.

3. Poor performance in challenging environments: Standard camera systems struggle in fog, or adverse weather conditions, making them unreliable for 24/7 monitoring. \

IV. OBJECTIVES

1. Detect and view intruders : Develop a system capable of viewing the person entering a restricted area simultaneously, which is essential for border security and sensitive zones.

2. Unmanned and automated operation : Design an autonomous system that minimizes human intervention by using and sensors for real-time decision-making.

3. 24/7 monitoring capability : Ensure continuous operation with wireless data transmission for remote areas.

V. METHODOLOGY

1. The methodology for the ground intrusion detector project involves a systematic integration of hardware and software.

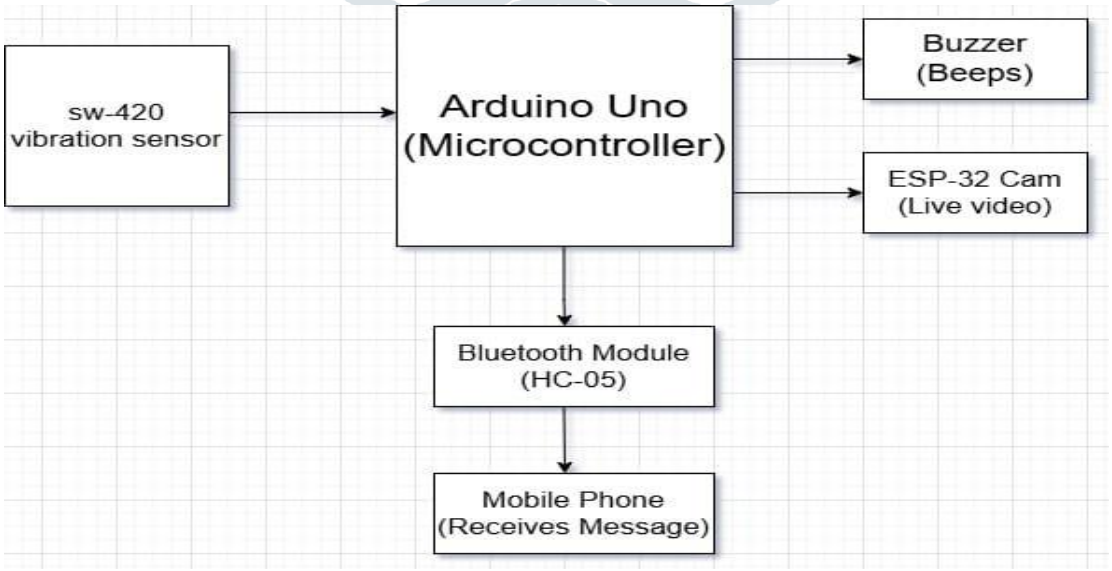
2. First, the hardware is assembled by connecting the SW-420 vibration sensor's digital output to an Arduino UNO input pin (Pin 7) and a passive buzzer to pin (Pin 9).

3. The next step is wiring the HC-05 Bluetooth module, which requires a 1kΩ voltage divider on its RX pin to safely step down the Arduino's 5V signal. Next, the software is developed in the Arduino IDE ensures the system triggers only on the initial change in the sensor's state (from HIGH to LOW), preventing redundant alerts.

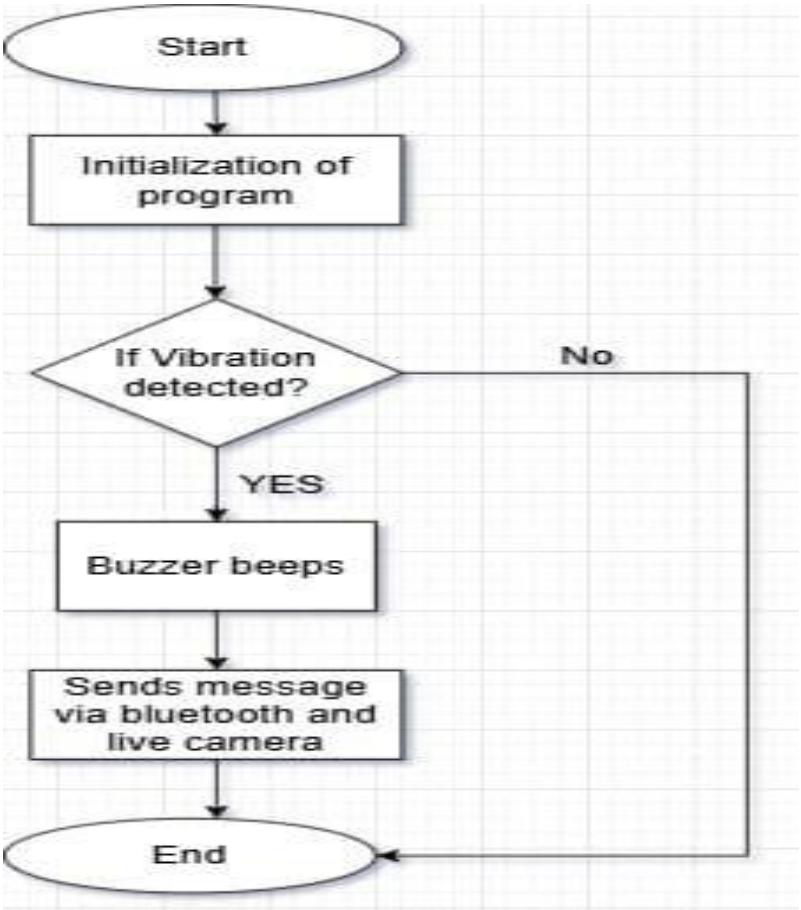
4. Upon this trigger, the code simultaneously sends an alert string (e.g., "ALERT!") via a Software Serial port to the Bluetooth module and calls a function to beep the buzzer. For implementation, the Bluetooth module's 5V pin must be disconnected during the code upload process to avoid serial port conflicts.

5. Finally, the system is calibrated and tested by pairing the HC-05 with a smartphone, running a serial terminal app, and physically adjusting the sensor's onboard potentiometer to achieve the desired sensitivity for detecting intrusions and implemented ESP32 cam for live monitoring

VI. BLOCK DIAGRAM



VII. FLOWCHART



VIII. COMPONENTS USED

Component	Specification	Quantity	Purpose
Arduino Uno	ATmega328P, 16MHz, 2KB RAM, 10-bit ADC	1	Main microcontroller
SW-420 Sensor	Comparator:LM393,operating voltage:3.3v-5v	1	Vibration sensor
ESP-32 cam	dual-core ESP32-S microcontroller, an integrated OV2640 camera (2MP), and Wi-Fi/Bluetooth connectivity	1	Live monitoring
Bluetooth module(HC-05)	V2.0+EDR 3.3v	2	Wireless data transfer
Passive buzzer	Custom 3-5v	1	Virtual ground creation
1kΩ and 2kΩ	Tolerance:5%	1	Voltage divider
Breadboard	830-pin solderless	1	Prototyping assembly
Connecting Wires	22AWG breadboard jumpers	20	Circuit interconnection

IX. WORKING

1.Armed and Ready (Idle State):

When the Arduino is powered on, it immediately runs the setup() code. This "arms" the system by sending a "System is ON" message to your phone's Bluetooth terminal app.

The Arduino then enters its main loop(), where it will spend all its time.

In this idle state, the SW-420 sensor is quiet. Because it's an "active-low" sensor, its Digital Out (DO) pin sends a constant HIGH (5V) signal to the Arduino's Pin 7.

The Arduino reads this HIGH signal, compares it to the previous state (which was also HIGH), and sees no change. As a result, it does nothing and simply loops again. This check happens thousands of times per second.

2. Intrusion Detected (The Trigger)

An intruder stomps or creates a strong vibration near the sensor.

This physical shock is strong enough to cross the sensitivity threshold you set with the blue potentiometer.

The sensor's internal circuit instantly triggers, and its DO pin flips from HIGH to LOW (0V).

3. The Alert (The Response)

The Arduino, on its very next loop, reads Pin 7 and sees the new LOW signal.

The code now checks its logic: if (current Sensor State == LOW && las tSensor State == HIGH).

This condition is TRUE! The system has detected a change from quiet to active. The Arduino now executes the two commands inside the if block:

Wireless Alert: It immediately sends the text "ALERT: Ground Intrusion Detected!" to the Bluetooth module. The HC-05 transmits this message over the air to your paired phone, and it appears in your serial terminal app.

Local Alarm: It calls the trigger Alarm() function. This function takes control for a moment and sends a series of high-frequency pulses to the passive buzzer on Pin 9, causing it to beep three times.

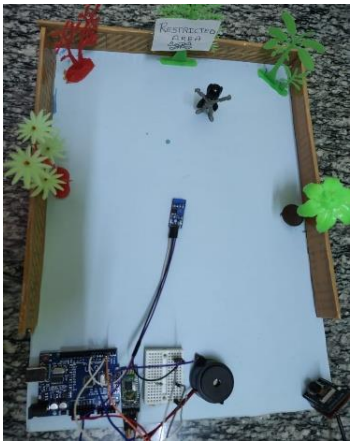
4. Reset and Re-Arm (The "Edge Detection")

At the end of the loop, the code sets lastSensorState = currentSensorState. So, lastSensorState is now also LOW.

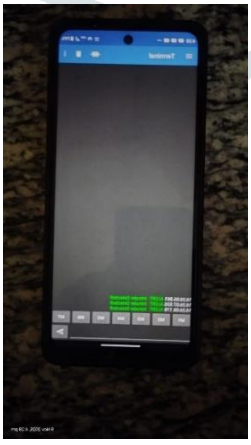
If the vibration continues (e.g., the intruder is still walking), on the next loop the code will check again. currentState is LOW and lastSensorState is also LOW. The if condition is FALSE.

This prevents the system from sending thousands of alerts and beeping continuously. It will only trigger the alarm one time for the start of the vibration.

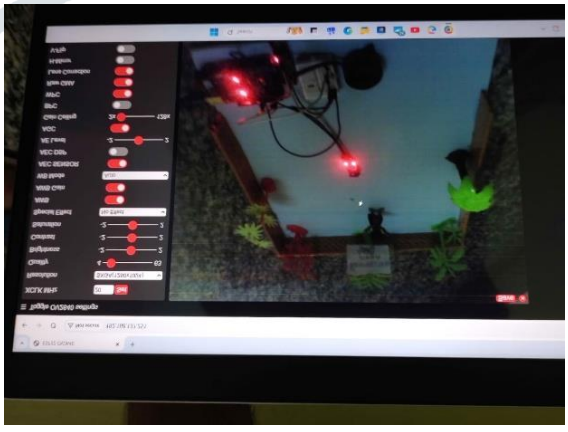
The system will only be able to trigger again after the vibration stops (sensor goes back to HIGH) and a new vibration begins (sensor goes back to low



Ground Intruder detector



Message to mobile



camera view

X. RESULTS

The ground intrusion detector system was successfully assembled and tested. Upon powering the system, the HC-05 Bluetooth module successfully paired with an Android smartphone, and the Bluetooth serial terminal application received the "System is ON" initialization message, confirming a stable communication link. The SW-420 sensor's sensitivity was calibrated using its onboard potentiometer to effectively filter out ambient noise while remaining responsive to distinct ground shocks.

During testing, simulated intrusion events (e.g., sharp taps on the surface, stomping near the sensor) consistently produced the expected outcome. In every test case, the system's response was instantaneous:

The passive buzzer immediately triggered, emitting the programmed three-beep audible alarm.

Simultaneously, the "ALERT: Ground Intrusion Detected!" message was received in the smartphone's serial terminal with no discernible latency.

The system's edge-detection logic performed correctly, issuing only one alert per intrusion event and automatically re-arming when the vibration ceased. The system remained stable and responsive throughout repeated test cycles.

XI. CONCLUSION

This paper successfully demonstrates the design and implementation of a functional, low-cost, and effective ground intrusion detector with a dual-alert capability. The prototype proves the viability of integrating an SW-420 sensor with an Arduino UNO to provide both an immediate, localized audible warning via a buzzer and a remote notification to a user via a Bluetooth module. The system is responsive, reliable, and easily deployable.

The primary limitation of this prototype is its operational range, which is constrained by the Class 2 (approx. 10-15 meter) range of the HC-05 Bluetooth module. The system is therefore best suited for small-scale applications, such as securing a single room, personal property, or a campsite.

Future work could significantly enhance this project's capabilities. Replacing the HC-05 module with a Wi-Fi (e.g., ESP8266) or LoRa module would extend the notification range from meters to potentially kilometers, enabling true remote monitoring over the internet. Additionally, an accelerometer could replace the binary sensor to allow for more sophisticated data analysis, potentially using machine learning to differentiate between false positives (like a passing vehicle) and genuine intrusions (like footsteps).

REFERENCES

[1] J. Deng, “FIDSUS: Federated Intrusion Detection for Securing UAV Swarms in Smart Aerial Computing,” IEEE Internet of Things Journal, 2025.
[2] M. Ogab, “Machine Learning-Based Intrusion Detection Systems for the Internet of Drones: A Systematic Literature Review,” IEEE Access, 2025.
[3] R. Upadhyay, “Quantitative Analysis of UAV Intrusion Mitigation for Border Security in 5G with LEO Backhaul Impairments,” arXiv preprint, 2025.
[4] A. Sharma, “A Hybrid Intrusion Detection System for Unmanned Aerial Vehicles Using Deep Learning and Federated Learning Approaches,” IEEE Access, 2025.
[5] L. Lin, H. Ge, and H. Zhou, “UAV Airborne Network Intrusion Detection Method Based on Improved Stratified Sampling and Ensemble Learning,” Drones, 2025
[6] E. F. da Silva, “A Deep Learning-Based Intrusion Detection System for Safeguarding ROS 2-Powered Unmanned Ground Vehicles Against DoS Attacks,” IEEE Access, 2025
[7] T. Shi, P. Guo, and R. Wang, “A Survey on Multi-Sensor Fusion Perimeter Intrusion Detection in High-Speed Railways,” MDPI Sensors, vol. 24, no. 2, pp. 150–162, 2024.
[8] M. Wang and X. Yu, “A Comprehensive Survey of Crowd Density Estimation and Counting,” IET Image Processing, vol. 18, no. 5, pp. 451–470, 2024
[9] R. Gupta, “AI-Enabled Secure Intrusion Detection for UAV Networks,” Proceedings of the IEEE International Conference, 2023
[10] H. Hu and H. Fu, “Deep Learning in Crowd Counting: A Survey,” IET Journals, vol. 14, no. 7, pp. 901–915, 2023
[11] X. Zhang and J. Luo, “Multi-Camera Multi-Object Tracking: A Review of Current Trends and Applications,” Neural Computing and Applications, vol. 35, pp. 12589–12605, 2023.
[12] R. Patel and A. Sharma, “Human Detection in Aerial Thermal Imaging Using a Fully Convolutional Network,” Infrared Physics & Technology, 2022.
[13] S. Gupta and V. Kumar, “Automatic Multiple Moving Human Detection and Tracking in Image Sequences,” Expert Systems with Applications, 2021.
[14] R. P. Singh, “Systematic Literature Review for Detecting Intrusions in Unmanned Aerial Vehicles Using Machine and Deep Learning,” Sensors, 2021.
[15] S. N. Bairagi, “Intrusion Detection Systems for Unmanned Aerial Vehicles: A Survey,” Electronics (MDPI), vol. 10, no. 15, 2021.
[26] L. Chen and F. Wang, “Ground Surveillance Radar for Perimeter Security: A Comprehensive Review,” Journal of Radar Systems, 2020.
[17] Z. Liu and E. Ristani, “Multi-Target Tracking in Multi-Camera Networks: A Review,” Pattern Recognition, 2020.
[18] P. Kumar and S. Rao, “Virtual Fence for Intrusion Detection Using Wireless Sensor Networks,” IEEE Sensors Journal, 2020.
[19] J. Li and Y. Wang, “Detection and Tracking of Moving Targets for Thermal Infrared Video Sequences,” Sensors Journal, vol. 18, no. 6, pp. 1–12, 2018.
[20] G. Choudhary, “Intrusion Detection Systems for Networked Unmanned Aerial Vehicles: A Survey,” Aerospace, 2018.