SATIG: AI-Enhanced Threat Detection in Drone

Yamini G[1], Suhani Sharma[2], Sushmitha K[3], Umme Asma[4], Zainab Tabha[5]

[1]Yamini G , Computer Science & Engineering, Dayananda Sagar Academy of Technology & Management
[2]Suhani Sharma , Computer Science & Engineering, Dayananda Sagar Academy of Technology & Management
[3]Sushmitha K , Computer Science & Engineering, Dayananda Sagar Academy of Technology & Management
[4]Umme Asma , Computer Science & Engineering, Dayananda Sagar Academy of Technology & Management
[5]Zainab Tabha , Computer Science & Engineering, Dayananda Sagar Academy of Technology & Management

---***---

Abstract - The SATIG (Self-Adaptive Threat Intelligence Grid) project addresses the growing concern of drone-based threats in military and defense operations. With the increasing use of autonomous drones, there is a rising risk of cyberattacks, spoofing, jamming, and coordinated intrusions that current security systems struggle to manage. The system combines computer vision, anomaly detection, and threat grading. SATIG aims to improve response speed, reduce false positives, and enhance adaptability to unknown threats. The project demonstrates how AI and cooperative decision-making can offer a scalable and intelligent approach to modern drone security.

Key Words: Drone security, real-time detection, multi-agent systems, reinforcement learning, anomaly detection, SATIG.

1.INTRODUCTION

Modern aerial defense systems are increasingly dependent on drones for surveillance, reconnaissance, and mission-critical operations. However, with the growing use of autonomous drones comes a rising threat from cyberattacks, GPS spoofing, and coordinated intrusions. These threats can compromise data integrity, mission success, and overall airspace security.

Our project, SATIG (Self-Adaptive Threat Intelligence Grid), proposes an AI-powered, real-time threat detection and response framework designed specifically for defense drones. By integrating machine learning algorithms, multi-agent reinforcement learning (MARL), and decentralized intelligence sharing, SATIG aims to create a dynamic, self-adaptive drone security system that can detect anomalies, evaluate risks, and autonomously respond to evolving threats.

Existing counter-drone systems often fall short in dealing with these advanced and evolving threats. Most conventional systems are reactive, based on predefined rules or static signatures, and require centralized infrastructure. As a result, they struggle to adapt to new types of attacks or operate effectively in dynamic, high-risk zones where decisions need to be made in real time. To address these challenges, we propose SATIG (Self-Adaptive Threat Intelligence Grid)—an intelligent, AI-driven security framework designed specifically for military drone defense.

SATIG is designed to not only detect known threats but also to adapt continuously by learning from new attack patterns and sharing intelligence across nodes in real time. This makes it a robust and scalable solution for defending military drones and sensitive aerial zones in modern threat landscapes.

2. BODY OF PAPER

- **Purpose:**
  To develop a scalable, intelligent, and real-time drone threat detection and response system capable of protecting military UAVs from both cyber and physical attacks. SATIG aims to enhance national defence operations by enabling autonomous threat classification, adaptive learning, and collaborative countermeasures among drone defence units.
- **Scope:**
  The SATIG framework is designed for deployment in military environments where drones are used for surveillance, mission planning, and reconnaissance. It focuses on detecting unauthorized drones, cyber intrusions, signal spoofing, and other anomalies using a combination of visual data and network signals. The system integrates AI models, real-time analytics, and cooperative decision-making to ensure secure and continuous drone operation.
- **Problem_Statement:**
  Modern military drones are increasingly exposed to complex and evolving threats, including cyberattack, unauthorized drone intrusions. There is a critical need for a self-adaptive, intelligent security framework capable of detecting, classifying, and responding to threats autonomously and cooperatively.
- **Existing_Systems:**
  Current anti-drone solutions are typically centralized, rule-based, and unable to respond to unknown or evolving threats. They depend on predefined parameters and do not support real-time learning or collaboration between defense units. These systems are often inadequate for high-stakes environments such as military zones, where threats can change rapidly, and delayed responses can lead to mission failure or data breaches.
- **Proposed_System:**
  SATIG introduces an AI-driven, decentralized threat intelligence grid that leverages sensor data (e.g., GPS, RF, video) and machine learning models to detect and classify drone-based threats. It uses CNNs, autoencoders, and LSTM networks for anomaly detection.

3. LITERATURE SURVEY

The rise of military drones has brought significant advancements in surveillance and defense, but it has also opened the door to increasingly complex cybersecurity threats. Researchers have explored various approaches to detect and mitigate these risks using AI and machine learning technologies.

Several studies have utilized deep learning for visual identification of unauthorized drones. For instance, convolutional neural networks (CNNs) have shown promise in recognizing drone types and detecting anomalies in video feeds. However, these systems often struggle to adapt dynamically to new or unseen threats without retraining.

Other research efforts have focused on analyzing drone flight data to spot unusual behavior patterns. Techniques such as Isolation Forest and One-Class Support Vector Machines have been effective for identifying outliers in telemetry, but their dependence on fixed thresholds limits their ability to keep up with evolving attack methods.

Sequential models like LSTM networks have also been applied to predict abnormal flight trajectories, offering improved detection of subtle, time-based threats. Despite this, deploying these models in real-time scenarios remains challenging due to their computational demands.

On the response side, reinforcement learning has been explored to automate countermeasures, such as jamming or evasive actions. Yet, many of these systems operate in isolation, lacking coordination among multiple defense agents, which is critical for handling sophisticated multi-drone attacks.

Recent advancements highlight the importance of decentralized threat sharing to build a collective defense. Protocols like MQTT enable communication between units, enhancing situational awareness. Nevertheless, integrating such decentralized communication with adaptive AI threat evaluation and coordinated multi-agent response is still an emerging area.

The SATIG framework aims to address these gaps by combining real-time adaptive learning, multi-modal data fusion, and multi-agent reinforcement learning to create a proactive and scalable drone security system capable of evolving alongside emerging threats.

4. SYSTEM ANALYSIS

System_Analysis:
SATIG is designed to counter modern threats targeting military UAVs through real-time perception, decision-making, and collaborative defense. The system uses multi-modal sensors (visual, RF, GPS, LIDAR) to collect data and detect anomalies. These are evaluated using AI models to predict intent and classify threats, followed by autonomous response execution.

Functional Requirements:

- Detection of unauthorized drone behavior based on pattern anomalies.
- Risk scoring and threat classification using AI.
- Autonomous execution of appropriate response (log, alert, block).

Non-Functional Requirements:

- High availability and real-time processing capabilities.
- Low-latency communication for distributed drones.
- Robust security protocols for data integrity and communication.

5. SYSTEM DESIGN

System Design - The SATIG employs a layered approach:

A. Perception layer : Collects data from onboard sensors: GPS, RF scanners, video cameras, and LIDAR.

B. Comprehension Layer : Fuses sensor inputs to build situational context (speed, trajectory, proximity, zone violations).

C. Projection Layer : Predicts future behavior using LSTM and CNN models to assess intent.

D. Threat Grading Module : Assigns a risk score based on:

- Distance from sensitive assets
- Drone trajectory and speed
- Payload estimates
- Historical behavior patterns

E. Response Engine-Decides among:

- No action (safe)
- Log and monitor (suspicious)
- Active countermeasure (danger)
- Executes response such as alerting, jamming signals, or evasive path changes.

Architecture:
Sensor data is collected continuously during drone operation. Data is processed using pre-trained AI models for anomaly detection and classification. Results are shared with nearby drones using the decentralized grid. Collaborative action is taken (e.g., evasive maneuvers, alert to command center, signal jamming) based on consensus.

6. CONCLUSIONS

SATIG presents a pioneering framework for intelligent drone security in defense applications. By merging multi-modal data, machine learning, and decentralized coordination, SATIG offers a fast, scalable, and adaptive solution for detecting and countering rogue drones. The integration of threat grading and real-time collaborative action enables proactive responses even in complex scenarios. Future improvements may include drone swarm coordination and integration with satellite-based threat systems.

ACKNOWLEDGEMENT

We express our gratitude to our institution, Dayananda Sagar Academy of Technology and Management, and the support of our professors, especially Prof. Yamini G, for their guidance throughout the project.

REFERENCES

1. K. Hartmann and C. Steup, “The Vulnerability of UAVs to Cyber Attacks—An Approach to the Risk Assessment,” 2013 5th International Conference on Cyber Conflict (CYCON), IEEE, pp. 1-23, 2013.

2. R. K. Mohanta, R. S. Yadav, and S. K. Sahu, “Drone Based Smart Surveillance System Using Cloud Computing,” Procedia Computer Science, vol. 132, pp. 1053–1063, 2018.

3. F. Xia, W. Wang, and Y. Yang, “Big Data Analytics and Intelligent Cloud-Based Systems in UAV Networks,” IEEE Network, vol. 33, no. 1, pp. 54–61, 2019.

4. P. W. Hall and A. G. Barto, “Reinforcement Learning: An Introduction,” MIT Press, 2nd Edition, 2018.

5. M. Gharibi, R. Boutaba, and S. L. Waslander, “Internet of Drones,” IEEE Access, vol. 4, pp. 1148–1162, 2016.

6. S. Suresh, A. S. Pande, and A. Kumar, “Drone Intrusion Detection using Deep Neural Networks,” 2020 IEEE International Conference on Artificial Intelligence and Computer Engineering (ICAICE), pp. 509–513.

7. Y. Li, T. Zhang, and Y. Wang, “Anomaly Detection of UAV Flight Behavior Using LSTM Networks,” Sensors, vol. 20, no. 14, 2020.

8. R. K. Kodali, S. Sahu, and A. Mahalakshmi, “MQTT based Secure Communication for IoT Applications,” 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI), IEEE.

9. H. Chae, D. Kim, H. Park, and J. Kim, “Dronet: Efficient Convolutional Neural Network Detector for Real-Time UAV Applications,” IEEE Transactions on Industrial Informatics, vol. 16, no. 1, pp. 472–479, Jan. 2020.

10. A. Ferrag, L. Maglaras, A. Derhab, and H. Janicke, “Security for UAV Networks: A Survey,” IEEE Communications Surveys & Tutorials, vol. 22, no. 2, pp. 1193–1223, 2020.