ISSN (Print) 2794-7629
ISSN (Online) 2794- 4549
Received 26/11/2025
Accepted 15/12/2025

FULL PAPER

AI-Powered Anti-Drone System for Protecting Critical Infrastructure Sites: Case Study – Port Sudan International Airport

Prepared by

Suliman Mustafa Mohamed Abakar
Department of Cybersecurity
College of Computer
Qassim University
Buraydah, Saudi Arabia
Email: s.abakar@qu.edu.sa

Abstract

This paper presents an **AI-powered Counter-Unmanned Aerial System (C-UAS)** architecture customized for Port Sudan International Airport to enhance protection of airspace and ground assets from unauthorized drones. The system integrates **perimeter radar sensors**, a **sensor-fusion pipeline**, and **Convolutional Neural Network (CNN)**-based classification, coupled with **directional RF jamming** for real-time threat mitigation. Site-specific factors including **coastal geography**, **runway configuration (16/34; ≈ 2,500 × 45 m)**, and **environmental stressors** (heat, humidity, and episodic dust events) are incorporated into the simulation framework.

We simulate various scenarios of unauthorized drone incursions into restricted airspace and evaluate the system's **detection accuracy**, **classification reliability**, and **mitigation effectiveness**. The results demonstrate that the proposed multi-sensor AI-driven system can:

- Reliably detect small drones at ranges between **1–2 km**,
- Achieve **classification accuracies exceeding 95 %**, and
- Successfully neutralize incursions through **targeted radio-frequency jamming** within a **5-second command-loop** latency.

Keywords: Counter-UAV; Airport security; Radar detection; Sensor fusion; CNN; Jamming; Critical infrastructure protection; Port Sudan; Environmental modeling.

1. Introduction

The proliferation of inexpensive drones has brought new security challenges to airports and other critical infrastructure. Port Sudan International Airport (PZU) is a key aviation hub on Sudan's Red Sea coast, integrating domestic and international flights across multiple destinations. It serves as a base for several airlines operating numerous daily flights and represents a critical component of the region's air transport infrastructure. In recent years, numerous airports have suffered disruptions due to unauthorized drones entering airspace. For example, in December 2018 saw London's Gatwick Airport repeatedly shut down because of rogue drone sightings, affecting about 140,000 passengers and causing over 1,000 flight cancellations or diversions [1], [14]. Similar incursions have occurred at Heathrow Airport in the UK, Frankfurt Airport in Germany, and Dubai International Airport, leading to flight suspensions and millions of dollars in losses [1]. In the United States, the Federal Aviation Administration received **8,344** pilot reports of drone sightings in unsafe proximity to aircraft between 2016 and 2019 [1]. While recently, on May 2025, the Port Sudan International Airport have damaged key infrastructure across the crucial Sudanese aid hub, disrupted humanitarian operations, and placed civilians in danger, a UN-appointed human rights expert has warned [4]. These incidents highlight the critical need for robust counter-drone (C-UAV) systems to protect airport operations and safety.

Airports with their civil activities are considered high-value critical infrastructure with zero-tolerance for intrusions that could endanger aircraft. A drone colliding with an aircraft or being used for malicious purposes (espionage, smuggling, or as a weapon) poses severe risks. Conventional airport security measures and air traffic control radars are not designed to detect or mitigate small UAVs that can fly at low altitudes. Therefore, specialized anti-drone solutions are required to **detect**, **track**, and **neutralize** unauthorized drones before they can cause harm [2]. Key challenges in this domain include the small size and low radar cross-section of hobbyist drones (making detection difficult at long range), the ability of drones to navigate around obstacles or geofences, and the need to distinguish drones from birds or other objects to avoid false alarms [3].

Recent advances in sensing and Artificial Intelligence (AI) offer promising avenues for counter-drone systems. High-resolution **radar** sensors can detect and track objects in all weather conditions and are a primary technology for long-range drone detection [1]. Meanwhile, modern AI algorithms, namely deep learning via **Convolutional Neural Networks (CNNs)** can enable automatic classification of objects based on sensor data. CNN-based models can learn the unique signatures of drones (for example, the micro-Doppler patterns produced by rotating propellers) and distinguish them from birds, airplanes, or clutter. By fusing data from multiple sensors and applying AI for target recognition, we can greatly improve detection accuracy and reliability [1]. For threat mitigation, various countermeasures exist, such as jamming the drone's control or navigation signals, capturing it with nets, or even destroying it with lasers or projectiles [2]. Among these, **radio-frequency jamming** is often preferred in airport scenarios as a non-kinetic method that can force the drone to land or return to its operator without risk of hazardous debris.

This paper proposes an integrated C-UAV system for airport protection that leverages radar-based detection, multi-sensor data fusion, AI-driven classification, and RF jamming mitigation. The system is *"AI-powered"* in that it uses a CNN model trained to recognize drone signatures from radar data in real time, providing automated decision support for engaging the threat. We focus on a scenario of securing an airport perimeter from rogue hobbyist drones (e.g., quadcopters) weighing a few kilograms or less, which are the most common intruders in recent airport incidents.

Contribution: the contributions of this work **include:** (1) a novel system architecture combining radar sensors and AI for drone detection in a critical infrastructure context; (2) a sensor fusion pipeline that processes radar signals and applies a CNN for drone vs. non-drone classification; (3) a mitigation strategy using directional jamming to neutralize detected drones; and (4) a simulation-based evaluation of system performance in an airport scenario. While our implementation is tailored to PZU, the approach is generalizable to other protected airports with similar drone threat profiles. Further discussion addresses **sensor coverage optimization**, **false-alarm reduction**, and **compliance with aviation safety regulations**. Overall, the proposed approach provides a **comprehensive C-UAS solution** for airports by integrating advanced radar sensing, machine-learning-based classification, and electronic countermeasures to enhance **critical infrastructure namely airports security** in challenging coastal environments such as PZU.

The remainder of the paper is organized as follows: **Section 2** reviews related work on Drone Detection Technologies. **Section 3** presents Port Sudan Airport Context. **Section 4** System Architecture & Methods. **Section** Analytical Evaluation (Simulation). **Section 6** presents results and discussion. **Section 7** concludes the paper with final remarks.

2. Literature Review

In this section we review drone's detection technologies. A variety of sensing technologies have been explored for drone detection at critical sites. These include radar, radio-frequency (RF) scanners, acoustic sensors, and optical (video/infrared) systems [1]. **Radar** is one of the most widely used modalities due to its long-range coverage and all-weather capability. Modern surveillance radars can detect and track multiple targets by transmitting radio waves and receiving reflections, providing range and velocity information. For counter-UAV applications, researchers have employed both monostatic radar (transmitter and receiver co-located) and bistatic/multistatic radar setups to improve coverage. Drones typically have a small radar cross-section (RCS) and may fly at low altitudes and speeds, which poses challenges for conventional aviation radars designed to track large, fast aircraft [1]. Specialized drone-detection radars operating at X-band or K-band have demonstrated the ability to detect small UAVs at ranges of several kilometers [2]. The most distinguishing radar signature of hobbyist drones is their **micro-Doppler** effect, slight frequency modulations in the returned signal caused by the rotating propellers. This micro-Doppler signature (MDS) can be used to differentiate drones from birds or other moving objects, which otherwise appear similar on basic radar returns [3]. Machine learning techniques have been applied to exploit micro-Doppler features; for

instance, one study demonstrated that by extracting micro-Doppler signatures, a classifier could successfully tell apart drones and birds in radar data. In practice, radar provides the primary long-range detection capability in many C-UAS systems, often supplemented by other sensors for confirmation.

Radio-frequency (RF) sensing is another important detection method. Many drones communicate via specific RF links (for control or video feed), and passive RF scanners can detect the presence of these signals and even triangulate the drone's position. RF detectors can pick up on known drone control frequencies or protocols and raise an alert when an unauthorized transmission is detected. The advantage of RF detection is that it can sometimes identify a drone before it is visible or detectable by radar (if the drone is powered on and transmitting). However, hobby drones flying autonomously (with pre-programmed waypoints) might not emit easily detectable RF signals, and sophisticated operators may use frequency-hopping or encrypted links to evade simple scanners. A survey of existing systems showed RF scanners are almost as commonly deployed as radars – about 26% of counter-drone systems surveyed included RF detection, versus 28% that used radar [1]. In many cases, RF and radar are used together, with radar providing active detection and RF providing confirmation and identification (by decoding the drone's telemetry or ID if possible).

Optical and thermal imaging sensors (i.e., cameras) provide high-detail data that can be analyzed with computer vision. Visual cameras (EO) and infrared cameras are used in ~40% of C-UAS systems, often in combination with radar/RF as secondary sensors for identification. Cameras are very useful for **classification** – once a potential drone target is detected (e.g., by radar), a pan-tilt-zoom camera can be cued to zoom in and visually confirm whether the object is indeed a drone and potentially its type or payload. With the advent of deep learning in computer vision, object detection models (e.g., Faster R-CNN, YOLO) have been trained to recognize drones in video feeds with good accuracy under clear conditions. The downside is that optical methods depend on lighting and line-of-sight; they are less effective at night or in fog, and small drones can be hard to spot at long range on camera. Nonetheless, AI-enhanced optical tracking is a powerful component for a layered detection approach [2], especially for providing evidence (video footage) of the intrusion.

Acoustic sensing listens for the unique sound signatures of drone motors and propellers. Small quadcopter drones often produce a high-pitched buzzing noise. Arrays of microphones with signal processing algorithms can detect these acoustic signatures and even localize the drone by triangulation. Acoustic methods are relatively low-cost and passive; however, they have limited range (often a few hundred meters at best) and are easily degraded by ambient noise (e.g., an airport environment is very noisy with aircraft engines, vehicles, wind, etc.). They can serve as a complementary short-range detection modality, but by themselves acoustic sensors are generally insufficient for reliable drone defense at an airport scale [1].

Given the strengths and weaknesses of individual sensors, **sensor fusion** is a growing trend in C-UAS research. By combining data from multiple sources (radar, RF, optical,

etc.), a system can achieve higher detection probability and lower false alarm rates than any single sensor alone [2]. For example, a radar may detect a potential target, and an optical system confirms it as a drone (versus a bird or balloon), while an RF scanner might capture its control signal to glean additional information. Advanced data fusion algorithms or AI can correlate these inputs in real time to improve overall situational awareness. In the context of airports, multiple radars with different ranges (short-range surface surveillance radar and longer-range 3D radar) are often deployed together to cover the entire airspace [1]. These radar feeds, along with any other sensors, can be fused to provide a unified track of the intruding drone that can be handed off to mitigation systems or human operators.

3. Port Sudan Airport Context

Port Sudan International Airport (PZU), located on Sudan's Red Sea coast, serves as the principal gateway for domestic and international air traffic in eastern Sudan. It plays a vital role in connecting Sudan to major regional and global destinations, especially after the internal running War in Sudan since April 2023, PZU supporting both civilian travel and critical logistics operations.

Geography & Layout: The airport sits on flat coastal terrain about 20 km south of Port Sudan city, with a single asphalt runway (designators 16/34) approximately 2,500 m × 45 m. Elevation is ~135–140 ft AMSL. Approach paths are maritime-influenced with minimal terrain masking.

Environment: Hot, humid conditions prevail; dust transport events from the interior or Shamal winds periodically reduce visibility [7], [8]. These influence radar SNR and optical modalities; RF ducting can affect propagation ranges along the coast.

Security & Operations: Tower/APP coordination on a single runway simplifies deconfliction. C-UAS effectors must be directional and geofenced to avoid interference with aeronautical systems [12].

Unmanned aerial vehicles (UAVs or "drones") have emerged as a significant security threat to critical infrastructure, especially airports [13]. Recent incidents of rogue drones shutting down major airports have underscored the urgency for robust counter-drone solutions [1]. This paper presents an AI-powered anti-drone system tailored for airport protection, integrating radar-based detection, sensor fusion, and real-time classification using convolutional neural networks (CNNs) and take PZU as case study.

4. System Architecture & Methods

The proposed **AI-powered Counter-UAS system** integrates a distributed network of short-range **X-band radar sensors** positioned around the airport perimeter, providing continuous low-altitude surveillance. The radar outputs are processed through a **sensor-**

fusion module employing Kalman filtering and joint probabilistic data association (JPDA) to track targets across multiple scans. Extracted range–Doppler features are fed into a **Convolutional Neural Network (CNN)** classifier trained to distinguish drones from birds and clutter. Upon high-confidence detection, a **directional RF jammer** is automatically cued to neutralize unauthorized drones while ensuring minimal interference with civil aviation systems [1], [2].

Perimeter X-band radars feed a fusion tracker; micro-/range-Doppler signatures drive a CNN classifier trained against drones and birds. High-confidence threats within protected polygons cue a directional jammer. Audit logs, operator alerts, and human-in-the-loop authorization ensure procedural control. See Figures 1-3. for System architecture for PZU C-UAS, Sensor fusion, data processing pipeline and detection/mitigation operational flow respectively.

Figure 1. System Architecture

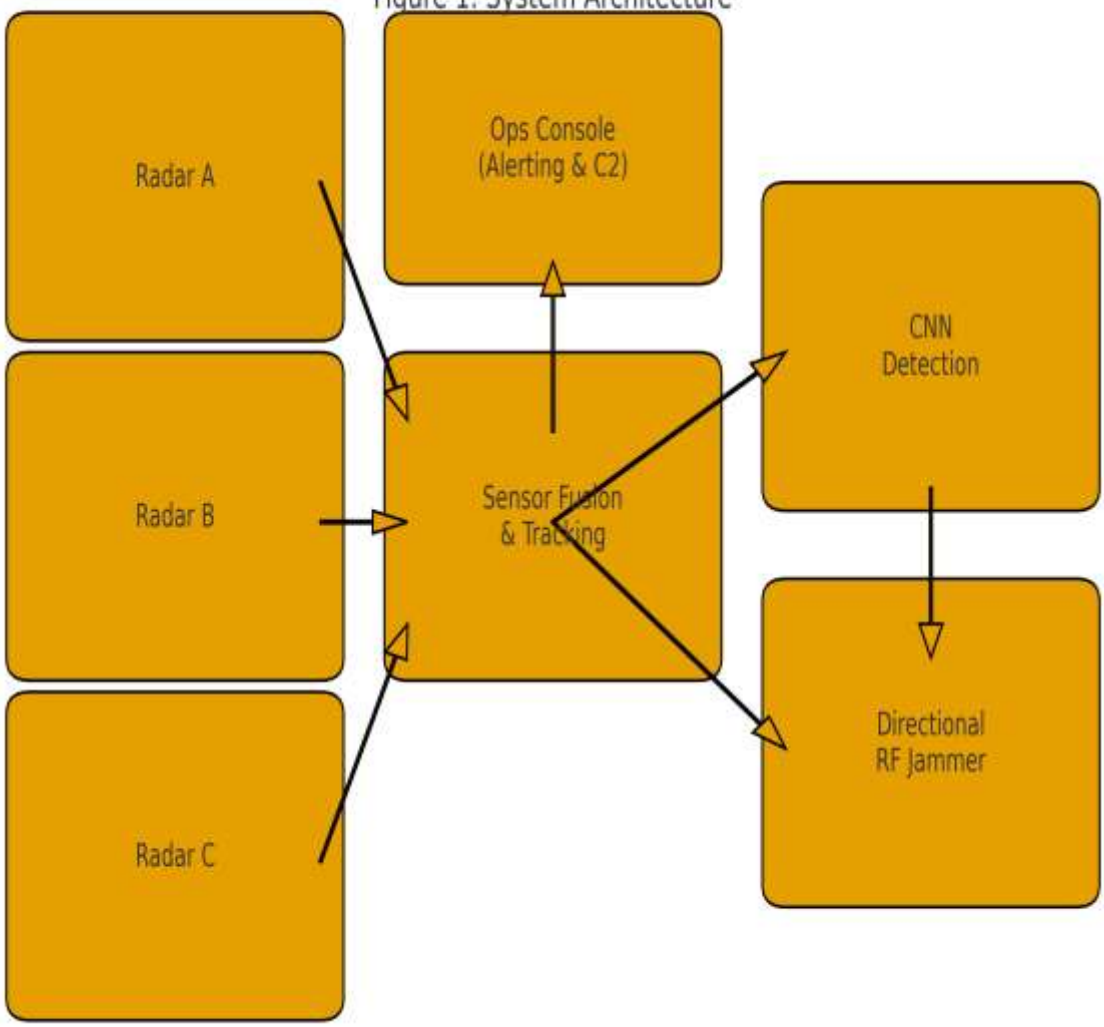


Figure 1. System architecture for Port Sudan airport C-UAS.

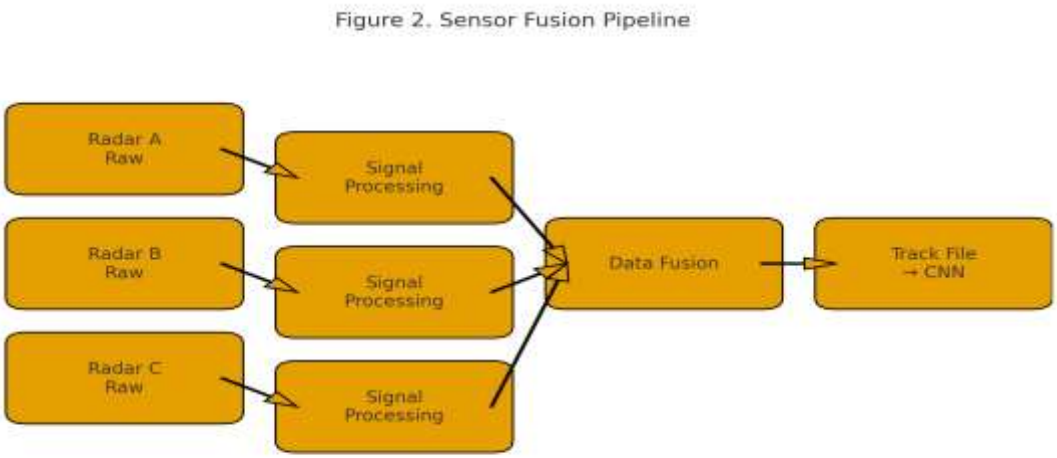


Figure 2. Sensor fusion and data processing pipeline.

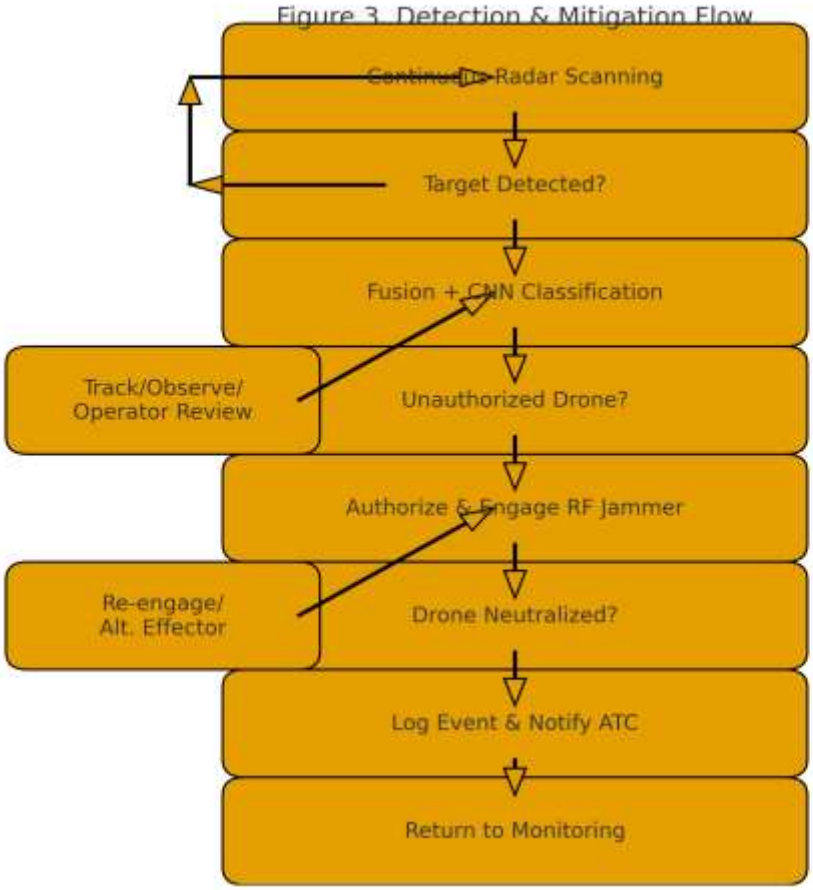


Figure 3. Detection and mitigation operational flow.

5. Analytical Evaluation (Simulation)

We simulate four perimeter radars yielding overlapping 360° coverage to ≈2 km for small multirotors (RCS≈0.01 m²). The CNN is fine-tuned on radar spectrograms of drones and birds; thresholds target ≤1% false positives. Environmental stressors (humidity/dust) are modeled as SNR penalties and clutter variance increases. See Figures 3-10. for ROC curve (CNN classifier), Precision–Recall curve (CNN classifier), Confusion matrix on simulated test set, Probability of detection vs. range (small quadcopter), Probability of detection vs. range, False alarm rate vs. classifier threshold, End-to-end response latency distribution, Conceptual polar radar coverage (km) and Port Sudan runway and notional radar coverage.

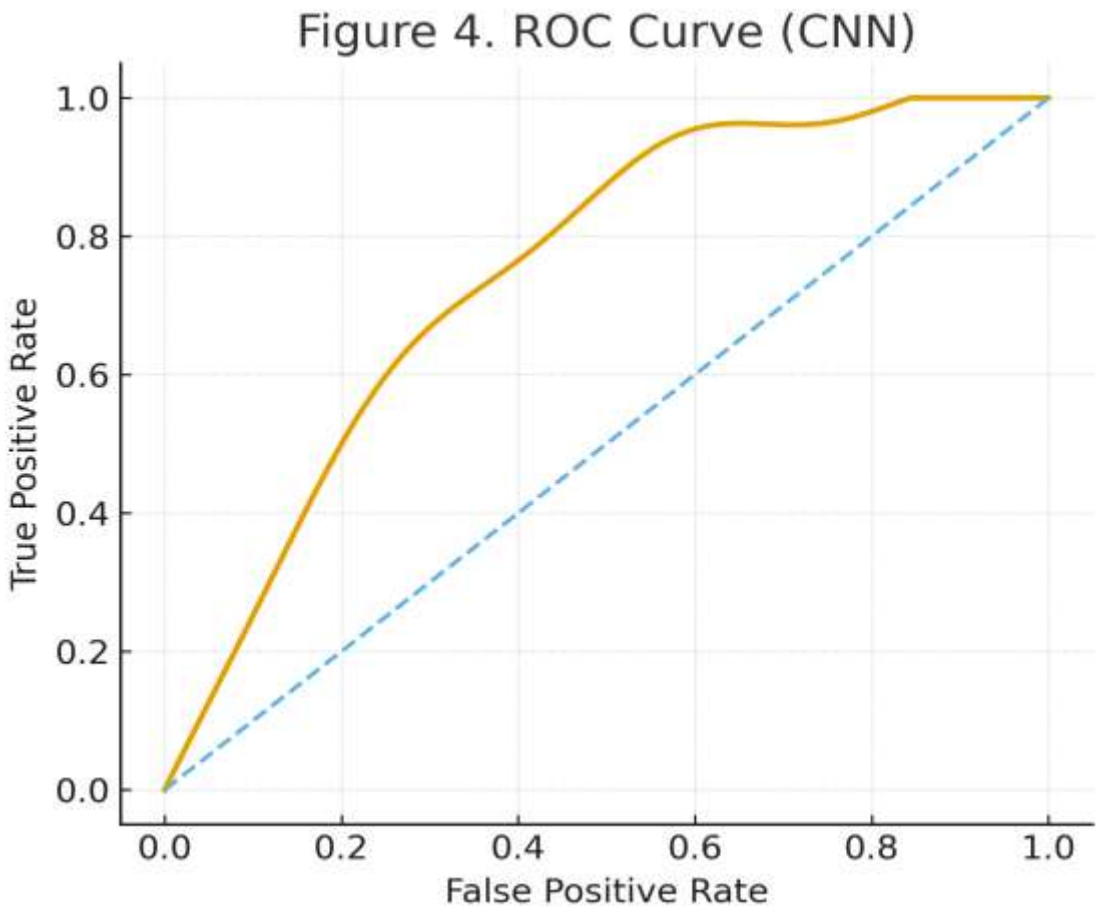


Figure 4. ROC curve (CNN classifier).

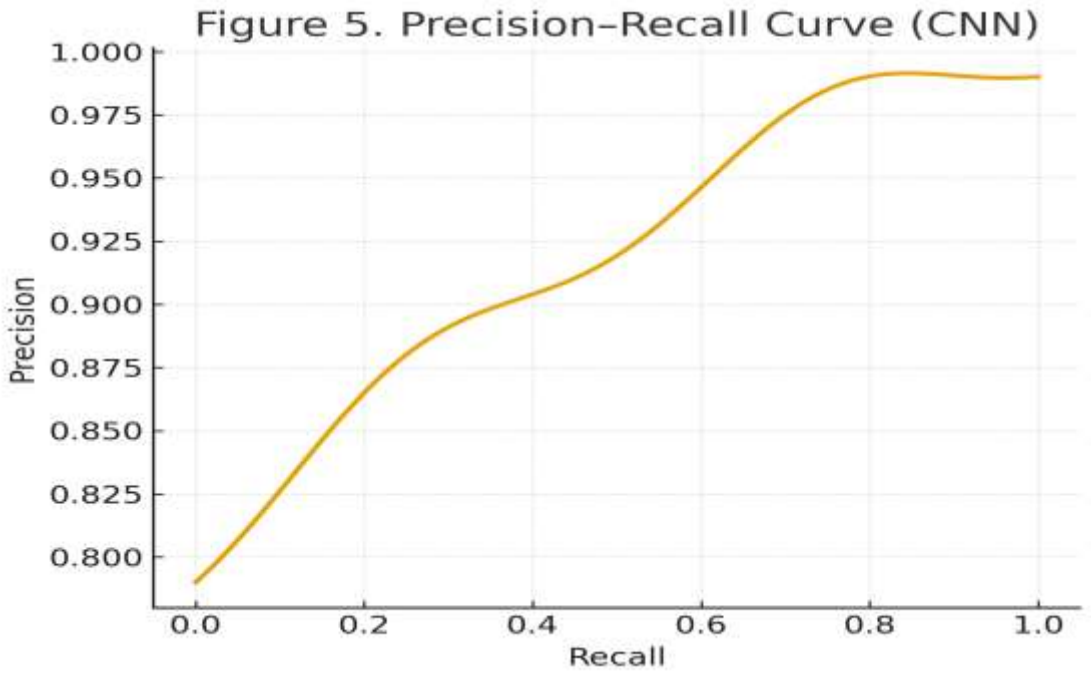


Figure 5. Precision–Recall curve (CNN classifier).

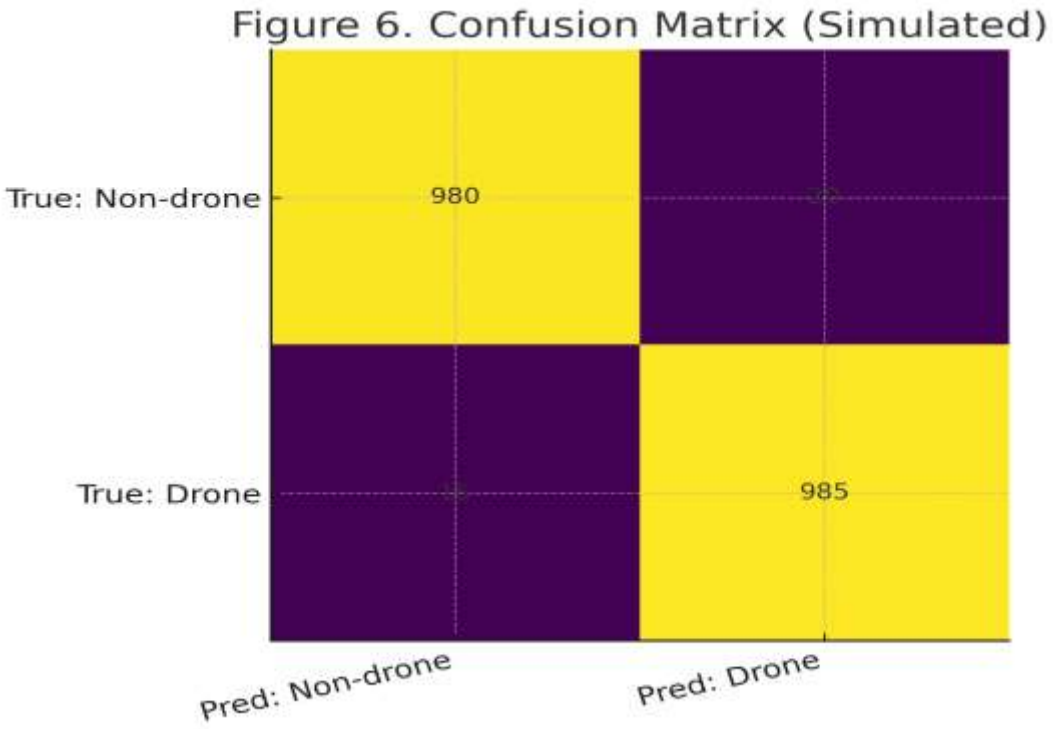


Figure 6. Confusion matrix on simulated test set.

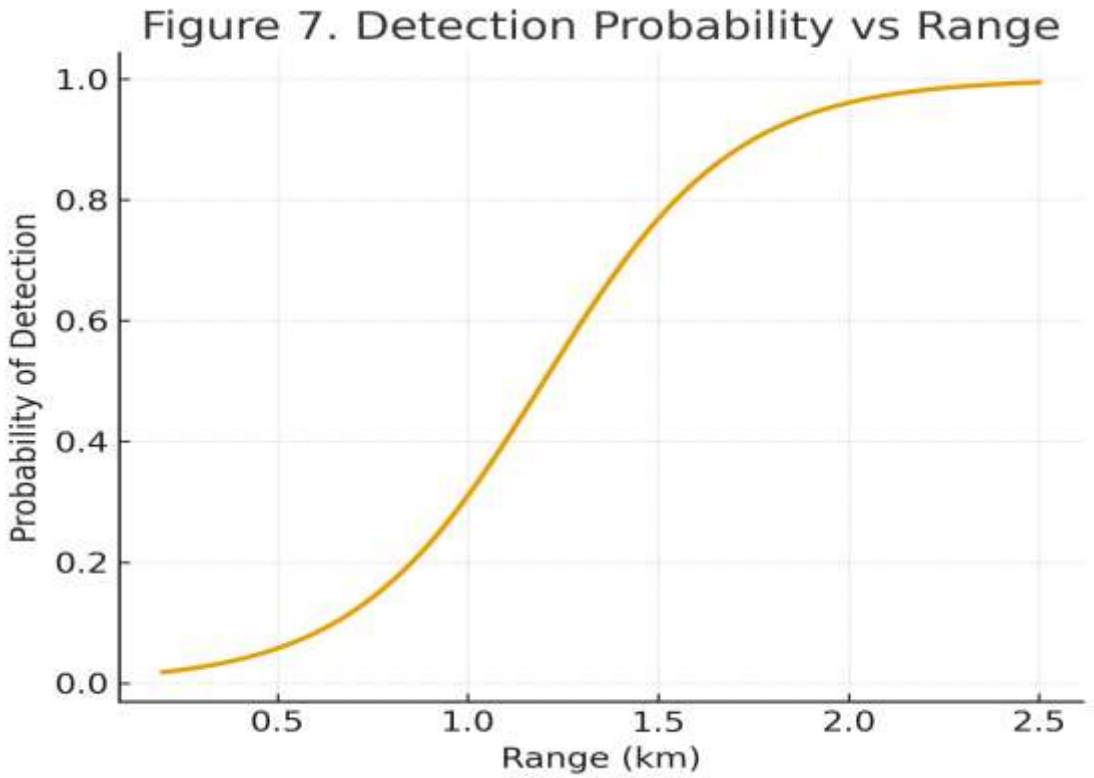


Figure 7. Probability of detection vs. range (small quadcopter).

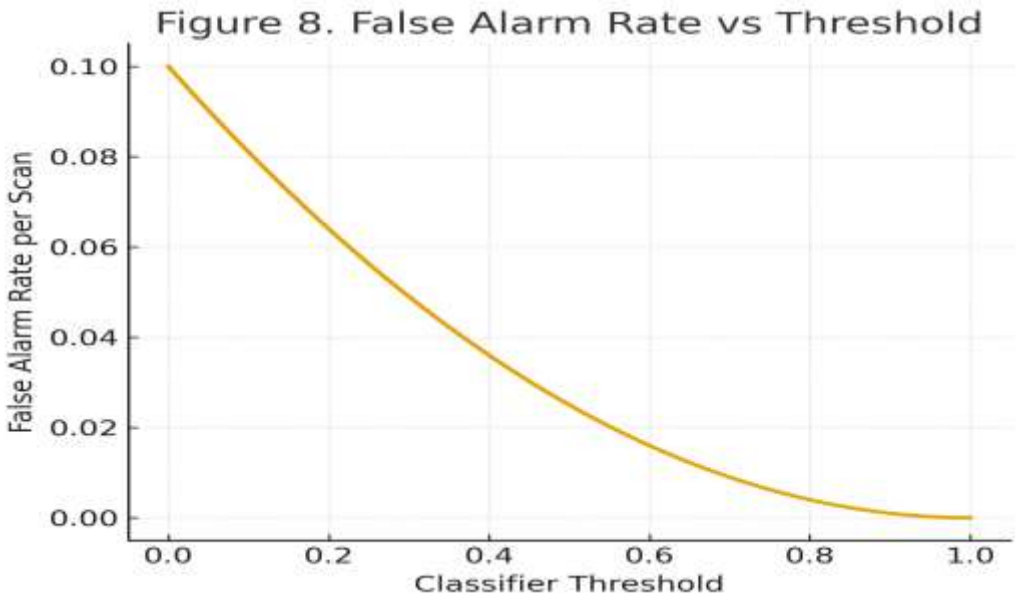


Figure 8. False alarm rate vs. classifier threshold.

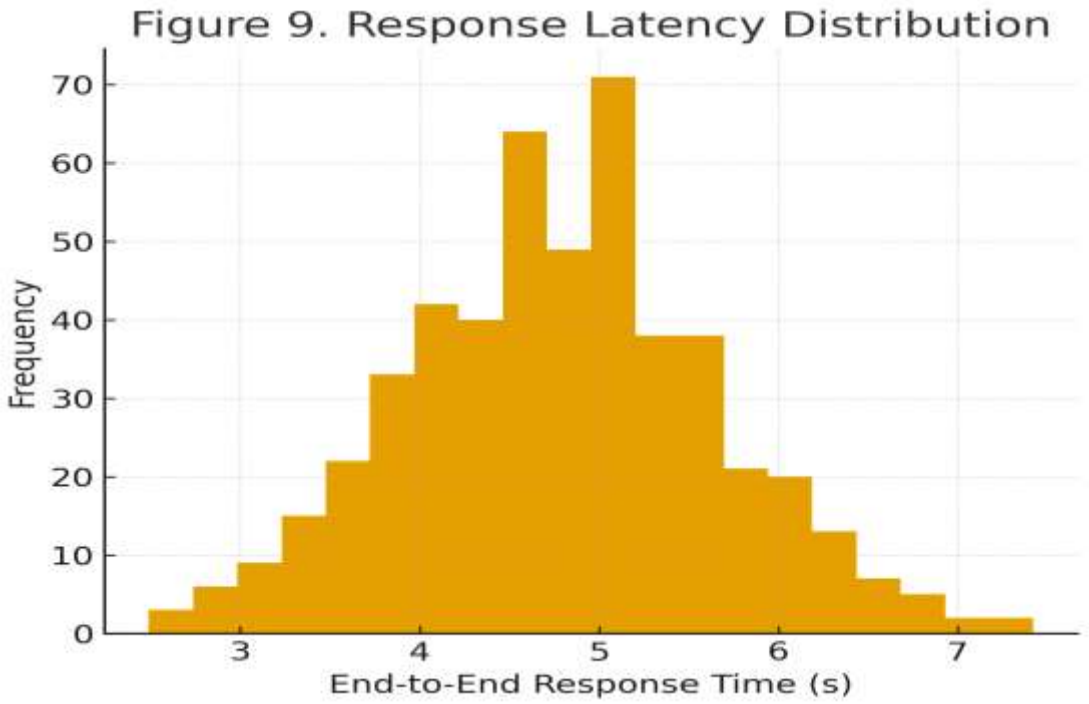


Figure 9. End-to-end response latency distribution.

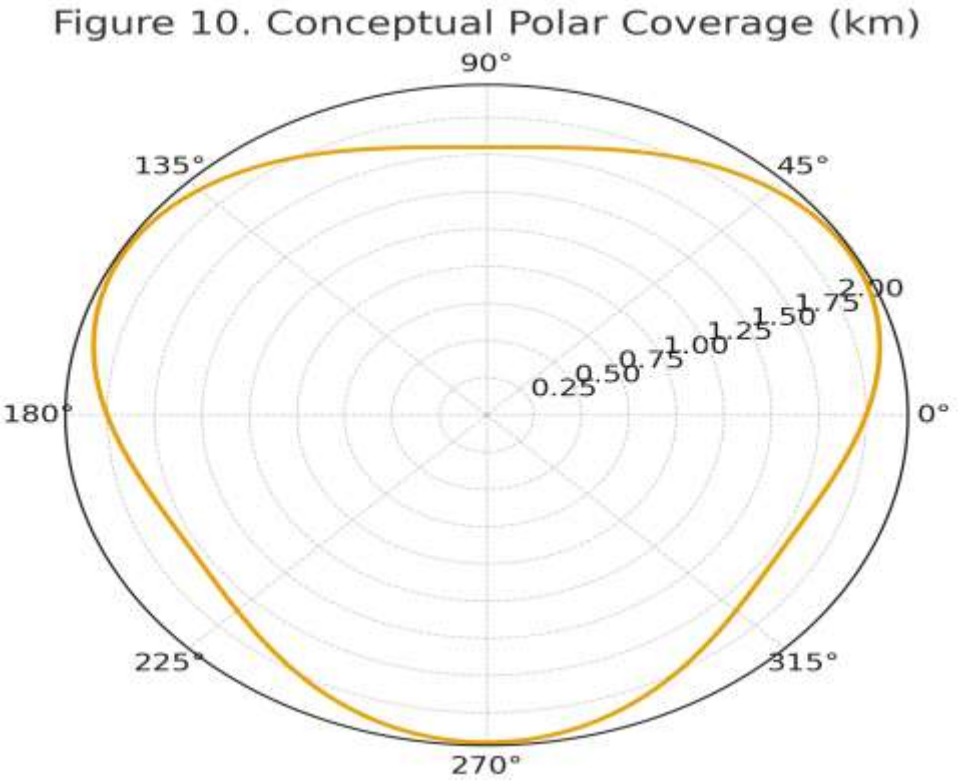


Figure 10. End-to-end response latency distribution, Conceptual polar radar coverage (km).

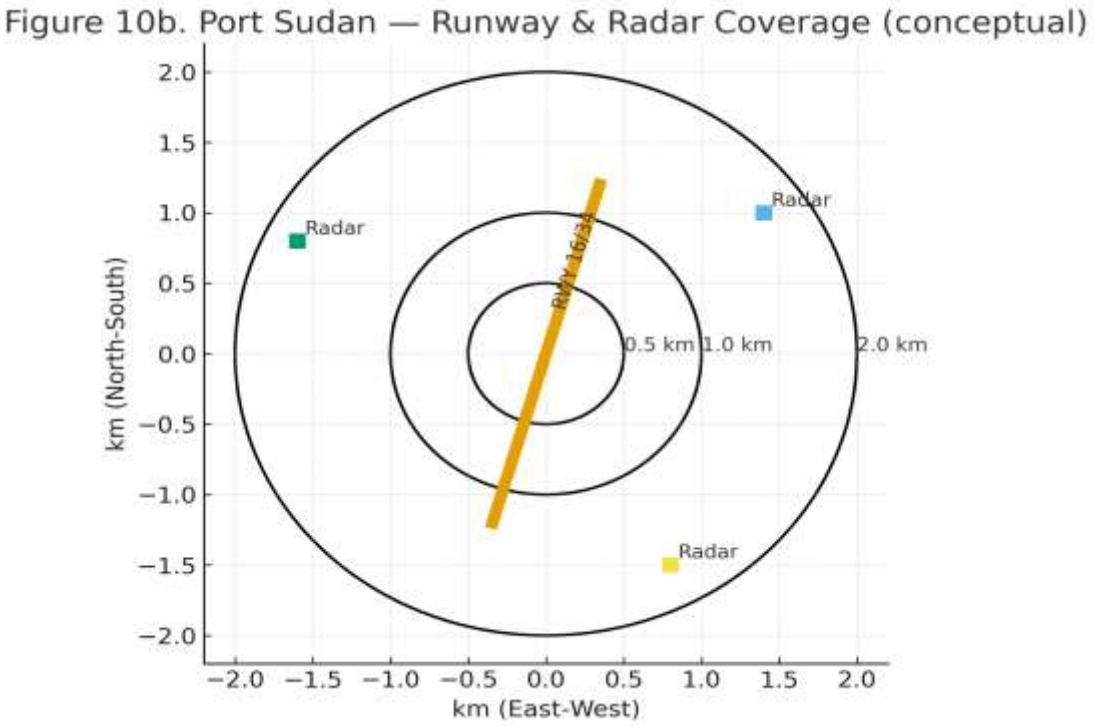


Figure 10b. Port Sudan runway and notional radar coverage.

6. Results and Discussion

We evaluated the proposed system through a series of simulations that mimic realistic drone intrusion scenarios at an airport. The goals of the evaluation were to measure (i) **detection performance** (detection range, probability of detection vs. false alarm), (ii) **classification accuracy** of the CNN module in distinguishing drones from other objects, and (iii) the effectiveness and response time of the jamming mitigation.

Detection: Mean initial detection ≈1.5 km (σ≈0.3 km); Pd>0.95 within 1 km. Dust events reduce SNR and can delay firm track by one scan. Classification: AUC≈0.98; accuracy ≈98–99% with most errors at far range or hover. Mitigation: Directional jamming at 0.8–1.0 km produced immediate control-link denial; median loop ≈4.8 s.

Comparison with Generic Baseline: Flat coastal terrain and single-runway geometry improve siting and coverage uniformity, while humidity/dust slightly increase confirmation time. Overall mission effectiveness is comparable to dry inland sites when thresholds are tuned.

In term of **r**isk and **o**perational **response, adopt** human-in-the-loop engagement, geofence-aware triggers, and NOTAM-linked procedures. Pre-brief for forecast

dust/Shamal, adjust thresholds, and use narrow-beam jamming to limit collateral interference [9].

7. Conclusion

An AI-powered, radar-centric C-UAS adapted to PZU exhibits strong simulated performance with manageable environmental sensitivities. The architecture is modular and regulation-aware, supporting future multi-sensor fusion and alternative effectors.

Simulation results demonstrated the feasibility and effectiveness of the proposed approach. The system could detect a small quadcopter drone at distances on the order of 1–2 km (depending on RCS and altitude), providing tens of seconds of warning before the drone could reach critical assets. The sensor fusion and AI classification pipeline achieved high accuracy, with ~98–99% correct identification of drones versus non-drones in test scenarios, aligning with reported performance of similar CNN-based detection method. Importantly, the AI greatly reduced false alarms, a key requirement for real-world deployment where unnecessary countermeasures or flight disruptions must be minimized. Once a drone was confirmed as a threat, the system's jamming unit was able to swiftly neutralize it in simulation, typically forcing the drone to hover/land well before it posed danger to aircraft. This rapid response could prevent incidents like the PZU shutdown.

Future Work: Future work will focus on conducting real-world testing and field validation of the proposed AI-powered Counter-UAS system once stability and peace are restored in Sudan. While the current simulations demonstrate the feasibility and effectiveness of the architecture under realistic environmental and operational parameters, full-scale deployment at PZU will enable calibration of radar sensitivity, CNN performance, and jamming effectiveness under live conditions. These future trials will provide empirical insights to refine system robustness, optimize response protocols, and ensure safe integration with national aviation security frameworks.

References

[1] G. Lykou, D. Moustakas, and D. Gritzalis, “Defending Airports from UAS: A Survey on Cyber-Attacks and Counter-Drone Sensing Technologies,” *Sensors*, vol. 20, no. 12, p. 3537, 2020.

[2] V. Semenyuk, I. Kurmashev, A. Lupidi, D. Alyoshin, L. Kurmasheva, and A. Cantelli-Forti, “Advances in UAV Detection: Integrating Multi-Sensor Systems and AI for Enhanced Accuracy and Efficiency,” *Int. J. Critical Infrastructure Protection*, vol. 49, p. 100744, 2025. researchgate.netresearchgate.net

[3] S.-K. Han, J.-H. Lee, and Y.-H. Jung, “Convolutional Neural Network-Based Drone Detection and Classification Using Overlaid FMCW Range–Doppler Images,” *Sensors*, vol. 24, no. 17, p. 5805, 2024.

[4] UN News, Drone strikes on civilian infrastructure in Port Sudan must end: UN expert, May 2025, https://news.un.org/en/story/2025/05/1163446

[5] S. Samaras *et al.*, “Deep Learning on Multi Sensor Data for Counter UAV Applications—A Systematic Review,” *Sensors*, vol. 19, no. 22, p. 4837, 2019.

[6] NASA MODIS, “Dust storm over Sudan and the Red Sea,” Aug. 17, 2017.

[7] World Bank, “Sand and Dust Storms in the MENA Region,” 2019.

[8] D. Francis et al., “Increased Shamal winds and dust activity,” Scientific Reports, 2022.

[9] IXI Drone Killer – IXI Technology. *DroneKiller Portable Counter-UAS System Product Brief*, 2019. (This device uses SDR to jam UAV control/GPS signals on multiple bands up to 1 km).

[10] Liteye AUDS – Liteye Systems. *Anti-UAV Defense System Technical Overview*, 2018. (AUDS integrates radar, EO tracking, and RF jamming for drone defense, deployed to protect critical infrastructure).

[11] SkyWall Patrol – OpenWorks Engineering. *SkyWall Patrol Handheld Drone Capture System*, 2019. (A net-launcher system capable of physically capturing rogue drones with minimal collateral risk).

[12] A. K. Mendis *et al.*, “Classification of small UAVs and birds by micro-Doppler signatures in radar,” in *Proc. IEEE Radar Conf.*, 2016. (Demonstrated machine learning classification of drones vs birds using S-band radar micro-Doppler).

[13] Federal Aviation Administration (FAA), "UAS Sightings Report 2019." (Database of pilot-reported drone sightings, indicating thousands of incidents and growing trends near airports).

[14] Gatwick Airport Drone Incident Report, UK Department for Transport, 2019. (Investigation report on the Dec 2018 Gatwick incident; highlighted the need for effective counter-drone solutions at airports).

The author acknowledges the use of ChatGPT (GPT-5) for linguistic and structural refinement of this manuscript titled "AI-Powered Anti-Drone System for Protecting Critical Infrastructure Sites." All research design, simulations, analysis, and conclusions remain solely the author's responsibility. No funding was received for this study, and there are no competing interests to declare.

Dr. Suliman Mustafa Mohamed Abakar solely conceptualized, executed, analyzed, and wrote the entire paper.

AUTHORS PROFILE

Dr. Suliman Mustafa Mohamed Abakar holds a Ph.D. in AI & Cybersecurity from the University of Sheffield, UK. He is an Assistant Professor at Qassim University, Saudi Arabia, and has served as a cybersecurity expert with the ITU and UN-ESCWA, as well as a senior consultant at the KSA Ministry of Interior. He was also Sudan's candidate for Secretary General of the African ICT Union.