Anti-Drone Systems Design: Safeguarding Airspace through Real-Time Trustworthy AI Paradigm

Simeon Okechukwu Ajakwe, Rubina Akter, Da Hye Kim, Golam Mohatsin, Dong Seong Kim, Jae Min Lee
Department of IT Convergence Engineering, Networked System Laboratory
Kumoh National Institute of Technology, Gumi, South Korea
(simeon.ajakwe, dahem91,golam248, dskim, ljmpaul)@kumoh.ac.kr, rubinaakter2836@gmail.com

Abstract

This paper provides a noble direction for guaranteeing safety of airspace for the use of drones in various transportation and logistics services in a smart city. Yolov5 deep learning model was used for visual drone detection and payload identification. The model showed 99.9% drone detection accuracy in less time but misidentified some of the attached objects due to its concealment. For robust discerning and countering of drones' usage for illegal, devious, and deadly purposes, the model's improvement is necessary to maintain sanity in airspace through responsible AI products for next-generation scenarios.

Ⅰ. Introduction

The polarization and proliferation of use of drones and its' derivatives for transportation and logistics without adequate check of legitimacy and privacy protection has sparked global concerns as it portends great security risk [1]. The drones' inexpensiveness, ease of operation, and dynamic evolution of its underlying technologies has created a gruesome challenge for developing an encompassing system for countering usage of drones for illegal and obnoxious purposes.

Though, Drone Transportation System (DTS) guarantees speedy service delivery, the influx of drones into the airspace is creating social panic as incidences of drone accidents, drone hijacking, terrorist attacks, privacy invasion, across border smuggling, etc., are on the increase [2]. These concerns question the verity of Artificial Intelligence (AI) responsiveness in maintaining technological friendly environment in its quest to mimic humans.

Anti-drone systems help to defend against drone accidents, and counter terrorist and illegal airspace activities perpetrated using unmanned aerial vehicles (UAV) [3]. However, the narrow mindedness of existing anti-drone systems in terms of militarization, lack of adaptive and simultaneous multi-drone detection, identification, interception, and neutralization method, poor response procedures, absence of drone flight regulation, amongst others, demands an environmentally friendly, robust, reliable, and ethical based approach to keep sanity in the airspace and restore societal confidence in AI technologies and its products.

This paper provides a conceptual framework on trustworthy anti-drone system design for maintaining sanity in the airspace. It explores and emphasizes the need for convergence technologies in the design of responsible AI products.

Ⅱ. Main subject

An Anti-drone system is an event-triggered critical-mission based hard real-time system deployed to detect a drone's location, determine its legality/illegality, harmfulness or otherwise, and decide the best method of neutralizing its' operation. These multi-dimensional task cuts across the convergence of computer vision, cognitive reasoning, wireless sensor, network, edge computing, blockchain, etc. [4]. The design of this event-triggered critical-mission real time system must therefore incorporate demanding response time, predictable peak load performance, environmentally friendly pace control and autonomous safety measure features as seen in figure1.

AI especially Deep Convolutional Neural Network (DCNN) coupled with detection techniques (visual, acoustic, radio frequency, thermal, and radar) has proven a veritable tool for solving complex dynamic event-driven problems as drone detection and identification [5]. DCNN Object detection models such as Faster RCNN, Yolo, SSD, MobileNet, etc. provides accurate and timely drone detection. Yolov5 model is used in this paper for object detection and identification respectively.

Besides identifying drone's source and its intended action in real-time, accurate and quick identification and interception of the payload (explosives, gun, recording device, etc.) attached to a drone is of utmost critical importance as the drone is just a vehicle conveying the object.

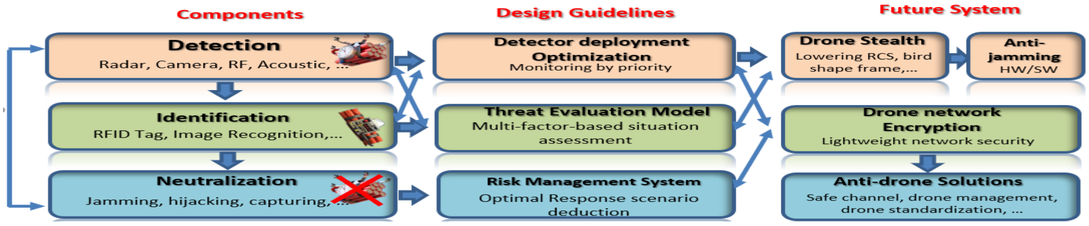
Components
Design Guidelines
Future System
Detection
Radar, Camera, RF, Acoustic, ...
Identification
RFID Tag, Image Recognition,...
Neutralization
Jamming, hijacking, capturing,...
Detector deployment Optimization
Monitoring by priority
Threat Evaluation Model
Multi-factor-based situation assessment
Risk Management System
Optimal Response scenario deduction
Drone Stealth
Lowering RCS, bird shape frame,...
Anti-jamming
HW/SW
Drone network Encryption
Lightweight network security
Anti-drone Solutions
Safe channel, drone management, drone standardization, ...

Fig1: Components and Design factors of Anti-drone system

To achieve this, a super-positioning strategy is formulated with features of drone model, characteristics and sensitivity of deployment area, and assessing potential threat level (high/low).

The perceived damage likely to occur *R* is a function of the payload attached, flight path and response time expressed as:

$$R= (R_{object} + R_{path})^{Rtime}, \quad \cdots \; (1)$$

where R_{object} is physical threat level, R_{path} is flight path and R^{time} is response time with maximum value set at, β, and 1 respectively. Physical threat level (R_{object}) is a function of the drone's weight/mass and speed derived from its kinetic energy given as:

$$K= \tfrac{1}{2}mv^2, \quad \cdots \; (2)$$

where **m** and **v** are drone's mass and speed respectively. A variation from the default drone weight is a signal that a potential payload is attached. Timely visual identification of the attached object is of vital importance in deciding the neutralization strategy to adopt. Hence, the overall damage of a drone in airspace is a function the drone size, noise, payload, and scanability as shown in equation 3.

$$R_{total} = \max\,[\alpha\,(R_{object,\,kinetic} + R_{object,noise} + R_{object,\,payload} + R_{object,\,scannable}) \text{ x } N_{drone}], \quad \cdots \; (3)$$

with N_{drone} being the number of swarming drones.

To achieve this requires transiting from weak AI (Artificial Narrow Intelligence) to General AI-based Anti-drone system which must have specialized environment-sensitive multi-drone detection capability, intuitive payload identification ability, adaptive and situation-based defensibility, co-operative interconnectivity and security alertness, scalability, and above all, efficient non-militarized neutralization strategy in handling envisaged UAVs.

Experimental simulation was carried out using 2000 datasets generated through testbed setup for drone detection and payload identification. Table 1 shows the dataset description and result of drone detection signifying high accuracy within minimal time.

Table1: Dataset Description and Detection Result

Type of drone	No. of items	Data Split (%)	Precision	Detection Time
Anafi-Ext	500	Training, Test, Valid (70, 20,10)	99.9%	0.022s
DJIFPV	500		100%	0.022s
Other drones	1000		99.9%	0.021s

For payload object identification, seven objects; bomb, guns, missile, etc. were attached to several drones and positioned at different distances as shown in the results in figure 2 and figure 3 respectively.

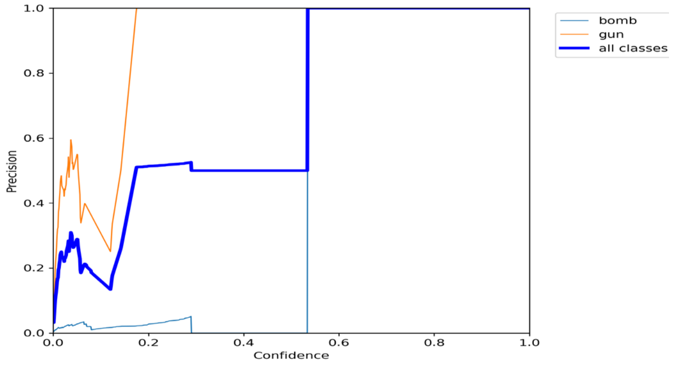

Figure 2: Model Precision of Payload

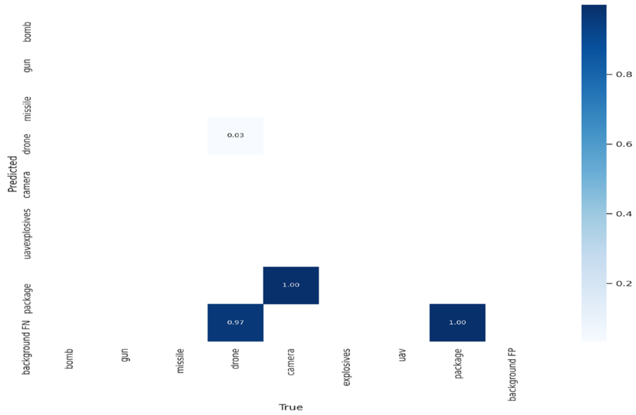

Figure 3: Confusion Matrix of Payload

The results in figure 2 shows that with Yolov5 model, payload attached to drones at various distances can be visually identified which determines the anti-drone's adaptive response strategy. However, as seen in figure 3, there are still misidentification of payloads due to object concealment which could result in wrong response. Hence, model improvement is necessary.

Ⅲ. Conclusion

Maintaining sanity and security in airspace because of drone usage influx remains a daunting challenge. This paper emphasized the need for responsive AI-driven real-time identification and interception of illegal drones to guarantee environmental safety. Unravelling payload content is crucial for accurate visual payload identification. More research efforts should be made in this direction.

ACKNOWLEDGMENT

This research work was supported by Priority Research Centers Program through NRF funded by MEST (2018R1A6A1A03024003) and the Grand Information Technology Research Center support program (IITP-2021-2020-0-01612) supervised by the IITP by MSIT, Korea.

References

[1] Chen H., Wang Z., and ZhangL," Collaborative Spectrum Sensing for Illegal Drone detection: A Deep-Learning-Based Image classification Perspective," China Communications 17(2), (2020) 81-92

[2] Haviv E. Elbit, "Drone Threat and CUAS Technology: WhitePaper, Elbit Systems 1 (01), 2019, 1-19

[3] Seongjoon P, Hyeong T.K, Sangmin L. Hyeontae Joo, and Hwangnam K, "Survey on Anti-Drone Systems: Components, designs, and Challenges", IEEE Access 9(2021), 42635-42659

[4] Seung-Hwan Kim, Jae-Woo Kim, Dong-Seong Kim, "Energy Consumption Analysis of Beamforming and Cooperative Schemes for Aircraft Wireless Sensor Networks" Applied Sciences, vol.10, no.12, pp.4374-4391, June 2020

[5] R. Akter, V. -S. Doan, G. B. Tunze, J. -M. Lee and D. -S. Kim, "RF-Based UAV Surveillance System: A Sequential Convolution Neural Networks Approach," 2020 International Conference on Information and Communication Technology Convergence (ICTC), 2020, pp. 555-558