Journal of Electronic Research and Application, 2025, Volume 9, Issue 5
http://ojs.bbwpublisher.com/index.php/JERA
ISSN Online: 2208-3510
ISSN Print: 2208-3502

Research on Anti-UAV Technology in Urban Environments

Lei Wang*, Haotian Chen, Tao Xi, Lei Xia

Armed Police Non-Commissioned Officer School, Hangzhou 311400, China

Corresponding author: Lei Wang, 1434551457@qq.com

Abstract: With the rapid development of drone technology, drones are increasingly used in urban environments, but they also bring many security risks, such as illegal reconnaissance, smuggling, and terrorist attacks. Therefore, it is of great significance to study the anti-UAV technology in the urban environment. This paper analyzes the advantages and disadvantages of existing technologies and their applicability in the urban environment from the aspects of UAV detection, identification, and countermeasures, and discusses the future development trend of anti-UAV technology, aiming to provide a reference for urban safety protection.

Keywords: Urban environment; Anti-UAV technology; Detection; Identification; Countermeasure

Online publication: October 21, 2025

1. Introduction

Unmanned aerial vehicle (UAV) is widely used in aerial photography, logistics, agriculture, emergency rescue, and other fields due to its flexible and efficient characteristics. However, when drones operate in urban environments, they may be used for illegal activities, such as sensitive area detection, contraband smuggling, and even terrorist attacks. Such “black flight” acts pose multiple threats to public safety. In recent years, there have been many cases around the world: at Gatwick Airport in the UK in 2018, large delays in flights due to drone incursions directly caused economic losses of up to 15 million pounds [1]; two years later, Los Angeles International Airport in the United States encountered similar interference incidents many times [2]. These events not only exposed the weak links of the low-altitude supervision system in the urban environment but also highlighted the necessity and urgency of developing and applying anti-UAV technology in the urban environment.

The complexity of the urban environment has brought many challenges to anti-UAV technology. First of all, there are a large number of tall buildings and infrastructure in the urban environment. These obstacles will block or reflect the detection signal, resulting in reduced detection accuracy. Secondly, various electromagnetic signals in the urban environment overlap with each other, and the communication and navigation signals of the UAV are

susceptible to interference. Finally, the city is densely populated, and anti-drone measures need to avoid harm to innocent people and infrastructure. Therefore, it is of great significance to study anti-UAV technology suitable for the urban environment to ensure urban public safety. Aiming at the security threats caused by illegal activities of UAVs in the urban environment, this paper systematically analyzes the current situation and challenges of detection, identification, and countermeasures technology, and looks forward to the future development direction of intelligence and multi-technology integration, so as to provide a reference for urban low-altitude security protection.

2. Threats and challenges of drones in urban environments

2.1. Threat of drones

With the popularization of drone technology, drones play a key role in urban governance, but their small size and strong mobility have spawned multiple security threats.

The UAV has the characteristics of miniaturization, which can easily penetrate dense buildings and then carry out an illegal investigation. For example, continuous monitoring of confidential areas of enterprises, or sneaking photos of residents' privacy from high altitude. In 2019, there were many incidents of drone peeping in Seoul, the Republic of Korea, which exposed obvious loopholes in low-altitude supervision at that time.

The modified drones can carry explosives or dangerous chemicals to carry out precise strikes. The typical case is the attack on the Saudi Aramco oil facility, which directly led to the fluctuation of the global energy supply chain and derived new terrorist threats, such as poisoning and spreading biological agents.

In addition, the disorderly flight of drones may also invade civil aviation routes, and there is a risk of collision with large aircraft. Globally, similar incidents occur from time to time. Although no major accidents have been caused, such incidents have posed a systematic pressure on civil aviation safety.

These three types of risks are intertwined, which not only involve the infringement of individual rights and interests but also relate to the safety of key facilities and even threaten the order of urban air traffic management.

2.2. Special challenges of urban environments

Anti-UAV technology in urban environments faces multiple technical challenges. Firstly, the complex electromagnetic environment of the city brings significant interference. The dense radio signals in the city can easily inundate the GPS navigation signals of the UAV, resulting in a decrease in positioning accuracy. At the same time, the electromagnetic noise will also interfere with the signal reception of the detection equipment, reducing the recognition efficiency of radar waves and optical sensors. Secondly, high-density buildings will form a natural barrier, and reinforced concrete structures will have effects such as reflection, absorption, and occlusion of radar waves. Low-altitude drones can use building gaps to avoid detection, and optical sensors have visual blind spots and cannot capture targets on the back of buildings. Finally, in densely populated areas, the risk of countermeasures will be aggravated. Although traditional hard-killing methods can destroy drones, the spread of energy may cause harm to the surrounding population and infrastructure, which requires countermeasures to seek a balance between efficiency and safety. These three challenges are superimposed on each other, which not only tests the anti-interference ability of the detection system, but also puts forward higher requirements for the accuracy of the countermeasures.

3. Anti-UAV technology in urban environments

3.1. Detection technology

In the anti-UAV system, detection technology is the core foundation of building a low-altitude defense system, and its performance directly determines the early warning and accurate identification ability of illegal UAVs. The following is a detailed analysis of the principles, advantages, and limitations of mainstream detection technologies.

Radar detection can obtain the position and velocity information of a UAV by transmitting electromagnetic waves and receiving reflected signals to achieve target detection. Phased array radar (AESA) and multiple-input multiple-output radar (MIMO) technologies developed in recent years have significantly improved anti-UAV capabilities. Phased array radar has the characteristics of fast beam scanning and strong anti-interference, which can effectively track small UAVs flying slowly at low altitude. The multi-input multi-output radar improves the detection accuracy and anti-clutter capability through multi-antenna cooperation. However, the urban environment has obvious limitations on radar performance, and the reflected clutter generated by ground buildings and vehicles can easily inundate the UAV signal, resulting in difficulty in target recognition. The radar cross-sectional area of a small UAV is small, the reflected signal is weak, and it is easy to be ignored. The high-rise occlusion will also greatly reduce the radar detection range and form a coverage blind area [3].

In optical and infrared detection, optical detection relies on visible light imaging equipment (such as cameras) to capture the visual characteristics of drones, and infrared detection uses thermal imaging technology to identify thermal signals generated by drone engines or motors. The combination of the two can improve the all-weather detection ability. Among them, the infrared has more prominent advantages at night or in low-light conditions, and can effectively locate the hidden UAV. However, optical detection is greatly affected by the weather, and rainy days or strong light interference will reduce the recognition rate; The infrared detection distance is short and vulnerable to environmental temperature interference (such as high temperature ground may mask the thermal signal of the UAV). In addition, optical and infrared devices are large in size and high in deployment cost, making it difficult to achieve wide-area coverage in dense urban areas [4].

Radio frequency analysis can identify the brand, model, and even serial number of a UAV by intercepting the communication signals (such as remote-control instructions and image transmission data) between the UAV and control terminal. It belongs to passive detection technology and avoids active emission signals interfering with the urban electromagnetic environment. The technology can also analyze the flight direction and distance of the UAV through signal strength and frequency changes. However, the limitations of RF analysis are prominent, and it is invalid for UAVs using autonomous flight mode or a pre-programmed path. With the upgrading of UAV encryption technology, the difficulty of cracking communication protocols continues to increase, which limits the accuracy of target recognition [5].

Acoustic detection is based on the unique voiceprint characteristics generated by the rotation of the UAV propeller. Passive detection is realized by comparing the pre-built voiceprint library. The equipment is small in size and low in cost, which is suitable for wide deployment in urban environments. However, urban noise (such as traffic, construction) will seriously interfere with the identification of acoustic signals, resulting in an increase in the rate of false positives; moreover, the effective distance of acoustic detection is short (usually only tens of meters), so it is difficult to form an effective early warning for medium and long-distance UAV, and it is more used as an auxiliary detection method [6].

3.2. Recognition technology

The recognition technology based on machine learning realizes recognition by constructing a classification model and automatically extracting the feature patterns of UAV images, sounds, or radio frequency signals. Deep learning algorithms (such as convolutional neural network, CNN) can efficiently process image data and quickly distinguish multi-model targets by learning hierarchical features of UAV appearance (such as propeller structure and fuselage contour). Recurrent neural network (RNN) is more suitable for analyzing the temporal characteristics of sound or signal and identifying the type of communication protocol. Its advantage is that it has strong adaptability, can adapt to new UAVs through continuous learning, and can still maintain a high recognition rate in complex urban backgrounds. However, the limitations are obvious. The performance of the model depends on large-scale and diversified training data, while the types of drones and flight scenarios in urban environments are complex, and the cost of data collection is high. Real-time performance is difficult to meet the demand, and high-end CNN model inference takes up to hundreds of milliseconds, which may lead to target escape due to delay. In addition, the model is vulnerable to adversarial sample attacks (such as specific textures or interference signals), and there is a risk of misjudgment [7,8].

Multi-sensor fusion integrates multi-modal data such as radar, optics, infrared, and acoustics, and constructs a redundant sensing network to improve recognition reliability. Radar provides all-weather position and velocity information, but it is susceptible to ground clutter interference. Optical sensors obtain high-definition images during the day, but are limited by weather and light; infrared thermal imaging penetrates darkness at night, but the detection distance is limited. Acoustic detection is low-cost and passive, but it is vulnerable to urban noise pollution. Through data-level, feature-level, or decision-level fusion algorithms (such as Kalman filter, D-S evidence theory), the advantages of each sensor (such as radar positioning + optical confirmation model + infrared verification thermal signal) can be integrated to reduce the false alarm rate. Its advantage is to break through the bottleneck of single sensor performance and adapt to complex urban environments. However, the limitations are significant, and the system complexity and cost are high. It is necessary to deploy a variety of heterogeneous sensors and build a high-speed fusion platform. It is difficult to synchronize multi-source data, and the difference in sampling rate and resolution of different sensors may lead to fusion error. In addition, the fusion algorithm needs to balance real-time and accuracy. The high complexity model may lose its practical value due to the calculation delay, and the simplified algorithm may reduce the recognition accuracy [9,10].

3.3. Countermeasure technology

The interference and blocking class of anti-drone technology mainly realizes countermeasures through signal interference, and the core includes two means of communication and navigation interference and satellite decoy. Communication and navigation jamming blocks the UAV's GPS navigation signal or manipulation link by transmitting directional RF signals, forcing it to go out of control, but there are two major problems: one is that the jamming may affect the city's legitimate communication equipment, such as affecting other users' GPS navigation; the other is that the technical effect is limited as the UAV's anti-jamming ability improves [11]. Satellite deception, on the other hand, induces UAVs to misjudge their position to land or return by injecting false positioning signals, the advantage of which lies in non-destructive countermeasures, but the limitations are more prominent: firstly, false signals will cascade to affect all the GPS equipment in the defense zone, interfering with the normal operation of the city; and secondly, the implementation of the technique requires precise control of the signal injection, making it more difficult to operate [12].

The control hijacking category of technology seizes control by cracking drone communication protocols, with the core advantage of non-destructive takeover of flight. Its principle relies on software-defined radio and AI algorithms, such as the Pulsar system of the US company Anduril, which can dynamically adapt to new protocols and realize efficient hijacking. However, the development of the technology faces two bottlenecks, one is that modern drones generally use encryption algorithms such as AES and RSA, and the difficulty of protocol cracking continues to increase; the second is that in-depth research on drone communication protocols is required, the technical threshold is high, and the cracking strategy needs to be continuously updated to cope with protocol upgrades. Although AI technology can partially alleviate the pressure of protocol adaptation, encryption upgrade, and protocol diversity still restrict the popularization of the technology [13]. Control hijacking techniques are more suitable for dealing with a single or a small number of UAVs, and their efficiency may decrease in swarm attack scenarios, and they need to be used in conjunction with other techniques.

Physical destruction technology realizes countermeasures by directly destroying the structure of UAVs, mainly including high-energy lasers, high-power microwaves, and particle beam weapons. High-energy lasers burn key components through thermal effects, with fast response and anti-electromagnetic interference advantages, suitable for urban environments, but the laser beam may cause fires in surrounding buildings or burns to personnel, with a high risk of collateral damage [14]. High-power microwaves paralyze UAVs by interfering with electronic systems, with a wide range of effects, suitable for dealing with UAV swarms, but may affect the normal operation of urban electronic equipment, and the equipment is large in size and low in deployment flexibility [15]. Particle beam weapons destroy targets with particle beams close to the speed of light, with extremely high energy density and penetration, but with high technological complexity and high cost, they are difficult to apply to urban scenarios on a large scale [16]. The physical destruction class of technology has a direct countermeasure effect, but security, cost, and deployment limitations in urban environments are the main obstacles to its popularization.

4. Future development trend

4.1. Intelligentization and automation

Future anti-drone systems will be more intelligent and automated. Through artificial intelligence and machine learning technologies, the system can automatically identify the type of threat of drones and select the most appropriate countermeasures. Deep learning-based intrusion detection systems (IDS) can monitor the abnormal behavior of drones in real time, automatically determine whether they are threatening, and select the appropriate countermeasures based on the type of threat. Such systems also have self-learning and optimization capabilities, dynamically adjusting the detection and recognition algorithms by continuously analyzing historical and real-time data, thus improving accuracy and reliability [12].

4.2. Multi-technology integration

It is difficult for a single anti-drone technology to meet the demands of complex urban environments. The future development trend is to integrate multiple technologies, such as the combination of radar and optical sensors, and the synergy of jamming and physical destruction technologies. A multi-technology fused anti-UAV system can enhance the overall effectiveness by complementing each other's strengths [17]. Specifically, the radar provides the position and speed information of the UAV, the optical sensor supplements the appearance characteristic data, the jamming technology forces the UAV to enter the uncontrolled state, and the physical destruction technology

implements the final blow to the uncontrolled target, forming a full-process coverage of "detection-recognition-countermeasures."

4.3. Miniaturization and portability

To meet the needs of diverse scenarios in urban environments, anti-UAS will evolve towards miniaturization and portability. Miniaturized counter-unmanned aircraft systems can increase system flexibility and deployability by reducing the size and weight of equipment. For example, compact radar and optical sensors can be easily mounted on rooftops or walls of urban buildings; portable jamming and destruction equipment is easy to carry to designated areas [18]. In addition, the system's high-energy-density battery and lightweight design extend the endurance of the system, which, combined with an easy-to-use operator interface and automated controls, reduces the requirement for operator expertise and further enhances its utility.

4.4. Legal and ethical considerations

As anti-drone technology develops, the associated legal and ethical issues are becoming more prominent. Thermal imaging tracking may involve public privacy invasion, while electromagnetic suppression jamming carries the risk of affecting legitimate communications. Therefore, there is a need to fully consider legal and ethical constraints along with technological development. For example, it is necessary to formulate norms for the use of anti-drone technology, clarifying under what circumstances anti-drone technology can be used and what principles need to be followed in its use; and to formulate ethical guidelines for anti-drone technology, making it clear that the use of anti-drone technology must not infringe on public privacy and must not cause interference with lawful communications, and so on. In addition, there is a need to strengthen the regulatory and review system, to regulate the process of technology development, production, and application through an approval system, and to set up a special review mechanism to assess the legality, ethicality, and safety of the technology, so as to ensure that the development of the technology is harmonized with social norms.

5. Conclusion

Anti-drone technology in urban environments is an important means to ensure urban public safety. This paper analyzes the existing technology in detail from three aspects: detection, recognition, and countermeasure, and discusses the future development trend. Although the current technology has achieved certain results, there are still many challenges, such as the problem of detection accuracy under the complex electromagnetic environment, the real-time problem of high-precision recognition technology, and the collateral damage problem of physical destruction means. In the future, with the development of intelligence, multi-technology integration, miniaturization, and other trends, anti-drone technology will play a greater role in urban security protection. In addition, the development of the technology needs to be combined with legal and ethical constraints to ensure its rational and legal application. Research on anti-drone technology in urban environments still needs to be deepened to cope with the increasingly complex drone threats and to safeguard the security and stability of cities.

Disclosure statement

The authors declare no conflict of interest.

References

[1] Xu R, Luo F, 2019, Evolutionary Game Research of Supervision on Unmanned Aerial Vehicle Interference. China Safety Science Journal, 29(05): 25–30.

[2] Lv S, Zhang X, Yin W, 2020, Literature Review of Police UAV Research. Journal of Hunan Police Academy, 32(06): 105–111.

[3] Li D, Gong J, Yan J, et al., 2024, Counter-Drone Radar Based on Radar Automatic Target Recognition Technology. Radio Engineering, 54(04): 765–779.

[4] Xia W, Yang X, Xi J, et al., 2024, Structure Characteristics Sensing Method of Unmanned Aerial Vehicle Group Based on Infrared Detection. Infrared and Laser Engineering, 53(01): 257–268.

[5] Xue C, 2024, Radio Frequency Identification for UAVs Under Different Scale Features of Signals, Master's thesis, Xidian University.

[6] Jin D, Wang X, 2025, Overview of Anti-UAV Acoustic Detection System. Electronic Technology, 54(04): 340–341.

[7] Nader A, Abdulrahman A, Turki A, et al., 2024, Deep Learning for Unmanned Aerial Vehicles Detection: A Review. Computer Science Review, 51100614.

[8] Jia J, Chen Z, Guo W, et al., 2025, Research on Image Recognition Technology for Unmanned Aerial Vehicle Inspection Based on Deep Learning. Computer Application Abstracts, 41(7): 121–123.

[9] Montanez JO, Suarez JM, Fernandez AE, 2023, Application of Data Sensor Fusion Using Extended Kalman Filter Algorithm for Identification and Tracking of Moving Targets from LiDAR–Radar Data. Remote Sensing, 15(13).

[10] Li G, Liu Y, Zheng Q, et al., 2025, Review on Multi-Sensor Data Fusion Research for Unmanned Aerial Vehicles. Journal of Software, 36(04): 1881–1905.

[11] Xiao Q, 2022, Research on Key Technology of Civilian Counter UAV Electromagnetic Interference, Master's thesis, Fujian University of Technology.

[12] Xue M, Zhou X, Kong W, 2021, Research Status and Key Technology Analysis of Anti-UAV System. Aerospace Technology, (05): 52–56 + 60.

[13] Qiu B, 2024, Overview of Anti-Drone Technology: Integration of Communication Technology and Artificial Intelligence. ZTE Technology Journal, 30(02): 89–99.

[14] Guo S, Ci M, Liu K, et al., 2024, Ability of High-Energy Laser in Combating Typical Air Targets. Laser & Optoelectronics Progress, 61(15): 1–7.

[15] Wu L, Ren Y, 2024, Research Status and Development Trend of High Power Microwave Weapons Counterattack Unmanned Aerial Vehicle. Movable Power Station & Vehicle, 55(01): 60–66.

[16] Ling L, Wang L, Pi M, et al., 2023, High-Power Microwave Technology Countering UAVs in the United States: Research Status and Implications. National Defense Technology, 44(03): 74–80.

[17] Ya Z, Zhang J, Lan S, et al., 2025, Analysis of Multi-Modal Armored Anti-Drone Sensing Model Based on BEV Technology, Chinese Institute of Command and Control, Proceedings of the 13th China Command and Control Conference (Volume I), 170–175.

[18] Zheng D, 2023, Spain's Indra Defense Company Launches 'Crow' Anti-UAV System. Small Arms, (01): 65.