Research on UAV Swarm Threats and Counter-UAV Swarm Technologies

[Abstract] UAV swarm technology is a form of distributed unmanned aerial vehicle application. By imitating the collective behavior of bees, it enables UAVs to work collaboratively. Unlike traditional single UAVs, swarm UAVs can achieve information exchange and task coordination among multiple drones, offering higher flexibility and efficiency. However, during its rapid development, it also faces numerous security threats. In-depth research on counter-UAV swarm technologies is necessary to ensure public safety.

1 Research Background and Significance

In recent years, with the rapid development of micro-electromechanical systems (MEMS), wireless communication, and artificial intelligence (AI) technologies, UAV swarm technology has gradually matured. Through distributed collaborative control, it enables the autonomous networking, information sharing, and task cooperation of multiple UAVs, finding wide applications in areas such as military reconnaissance, material delivery, and disaster relief. Incidents involving UAV swarms disrupting airport operations and stealing sensitive information have occurred globally. Traditional single-point defense methods exhibit significant limitations when facing swarm attacks characterized by "large numbers, high speed, and strong coordination." Notably, the militarization of UAV swarm technology has accelerated the evolution of modern warfare forms, and asymmetric warfare poses severe challenges to existing air defense systems. Therefore, focusing research on the threat characteristics of UAV swarms and developing targeted countermeasure technologies is essential for ensuring national security and social stability. It is also key to driving innovation in air defense technology systems and maintaining a balance in technological development.

2 UAV Swarm Threat Analysis

2.1 Suddenness and Stealthiness of Attack

Individual UAVs within a swarm are small in size with a small radar cross-section (RCS). They can fly at low or ultra-low altitudes, using terrain for concealment while approaching targets. The RCS of some small quadcopters is only about 0.01 m^2. In low-altitude environments, traditional air defense radars struggle to detect them effectively. Swarms can approach targets simultaneously from multiple directions, making attack timing and direction difficult to predict. This presents significant difficulties for defenders in early warning and response, often resulting in surprise attacks.

2.2 Powerful Destructive Capability

Although the payload of a single UAV is limited, UAV swarms leverage numerical superiority and coordinated attack capabilities to inflict massive damage on targets. They can carry explosives, incendiaries, or other offensive weapons to attack critical infrastructure such as power facilities, communication base stations, and transportation hubs. Against power facilities, UAV swarms can carry small bombs to precisely attack key equipment like transformers and circuit breakers in substations, causing widespread blackouts and severely disrupting normal societal operations. UAV

swarms can also attack military facilities, damaging command and control systems and weaponry, thereby weakening military operational capabilities.

2.3 Information Jamming and Theft

UAV swarms possess potent information warfare capabilities. They can jam electronic equipment like communications and radar in target areas using high-power jamming signals, rendering them inoperable. Electronic jamming equipment carried by UAV swarms can disrupt airport communication and navigation systems, hindering flight operations. Furthermore, equipped with various sensors like cameras and signal receivers, UAV swarms can conduct information gathering and theft in target areas. In the military domain, they can collect intelligence on enemy troop deployments and weapon systems, providing support for subsequent attacks. In the civilian domain, they can steal commercial secrets and personal privacy information, causing serious information security problems.

2.4 Difficulty in Defense and Tracking

Due to the large number of UAVs in a swarm and their high degree of coordination, traditional defense methods find it difficult to intercept them effectively. Air defense missile systems face problems such as high cost, slow reaction time, and limited interception capacity when confronting large-scale swarm attacks. The cost of a single air defense missile can be as high as hundreds of thousands of US dollars, while an individual UAV in a swarm might cost only a few hundred dollars. The economic disparity in using high-cost missiles against low-cost swarms is immense. After being attacked, UAV swarms can quickly adjust their formation and flight strategy to continue their mission, making it hard for defenders to track and sustain effective strikes. In simulated large-scale swarm attack scenarios, traditional air defense systems exhibit low interception success rates, while UAV swarms can adapt flexibly and persistently attack the target.

3 Research on Counter-UAV Swarm Technologies

3.1 Detection Technologies

3.1.1 Radar Detection Technology

Radar is a traditional target detection method. In the counter-UAV swarm domain, Multiple-Input Multiple-Output (MIMO) radar enhances the detection capability for low-altitude, slow-moving, small targets by transmitting multiple mutually orthogonal signals. A certain model of MIMO radar can detect small UAVs at ranges of several kilometers, effectively identifying low-altitude flying UAV swarms. Synthetic Aperture Radar (SAR) can image and track UAV swarms by monitoring their flight trajectories, providing accurate target information for subsequent defense decisions. However, radar detection is susceptible to interference in complex electromagnetic environments, leading to

reduced accuracy. Further optimization of anti-jamming algorithms and signal processing techniques is needed.

3.1.2 Optoelectronic Detection Technology

Optoelectronic detection technology includes infrared (IR) and visible light detection. IR detectors identify targets by detecting the infrared radiation signatures of heat-emitting components like UAV engines and motors. For low-altitude flying UAV swarms, IR detection offers high sensitivity, capable of identifying UAV IR signatures against complex backgrounds. Visible light detection uses high-definition cameras for real-time monitoring of target areas, employing image recognition algorithms to identify UAV shapes. Combined with AI, image recognition algorithms can quickly and accurately identify different types of UAVs and track their flight paths [4]. However, the effectiveness of optoelectronic detection diminishes significantly in adverse weather conditions like fog and rain, necessitating the development of adaptive image enhancement and target recognition technologies.

3.1.3 Acoustic Detection Technology

UAVs generate specific frequency noises during flight. Acoustic detection technology uses microphone arrays to collect these noise signals and employs signal processing algorithms to estimate the UAVs' position, speed, and number. Acoustic detection is effective for low-altitude, low-speed flying UAVs, particularly suitable for complex terrain areas like urban environments. A certain acoustic detection system can detect and locate UAV swarms within a radius of several hundred meters and distinguish between noise signatures of different UAV types. However, environmental noise interference is the main challenge for acoustic detection, requiring further improvements in noise filtering and feature extraction technologies to enhance accuracy.

3.2 Jamming Technologies

3.2.1 Radio Frequency (RF) Jamming Technology

RF jamming disrupts UAVs' communication links and navigation systems by transmitting specific frequency RF signals, causing them to lose control. Common RF jamming devices include directional jammers and vehicle-mounted jamming systems. Directional jammers can precisely jam single or a few UAVs at effective ranges of up to several hundred meters. Vehicle-mounted systems have higher power and coverage, capable of large-area jamming against UAV swarms within a certain region [5]. A vehicle-mounted RF jamming system can disrupt UAV GPS signals and data links within several kilometers, preventing them from receiving or sending commands, thus causing loss of control. However, with the development of UAV anti-jamming technologies, RF jamming requires

continuous optimization of jamming frequency strategies and power allocation schemes to improve effectiveness.

3.2.2 Laser Jamming Technology

Laser jamming technology uses high-energy laser beams to irradiate UAV optical sensors, such as cameras and photoelectric detectors, blinding or damaging them, thereby affecting the UAV's flight and mission execution capabilities. Laser jamming offers advantages like high precision, fast response, and long range. It also avoids electromagnetic pollution to the surrounding environment, making it suitable for areas with high electromagnetic compatibility requirements. However, laser jamming is significantly affected by weather; in adverse conditions like sandstorms and heavy rain, laser energy attenuates severely. Adaptive laser emission and tracking technologies need development to overcome these issues.

3.2.3 GPS Jamming Technology

GPS jamming technology transmits high-power jamming signals at the same frequency as GPS satellite signals, creating a strong electromagnetic interference field in space. When a UAV's GPS receiver picks up this interference signal, whose strength far exceeds normal GPS signals, the receiver struggles to extract accurate positioning information. This causes the UAV to obtain erroneous position, velocity, and time data, ultimately leading to disorientation. Based on application scenarios and functional requirements, GPS jamming devices are mainly categorized as handheld or fixed. Handheld GPS jammers are compact and portable; their power is relatively low but sufficient for effective jamming of UAVs within close range (typically hundreds of meters). They are suitable for security personnel dealing with illegal UAV intrusions at small event sites or localized areas. Fixed GPS jamming systems are powerful and can be deployed around critical facilities like airports, military bases, and key government departments. Through reasonable antenna placement and power adjustment, they can establish stable, large-area jamming protection zones within a radius of several kilometers, safeguarding critical facilities from potential UAV swarm information theft or attack threats.

3.3 Interception Technologies

3.3.1 Net Capture Technology

Net capture technology uses launching devices to fire specially designed capture nets into the air to ensnare UAVs. The nets are typically made of high-strength, lightweight materials, capable of capturing the UAV without damaging it. This technology is suitable for intercepting low-altitude and slow-moving UAVs. Net capture effectively avoids secondary damage to surrounding facilities and is a relatively safe interception method. However, its effective range is limited, and it is less effective

against high-speed or high-altitude UAVs, requiring combination with other interception technologies.

3.3.2 Counter-UAV Drone Technology

Counter-UAV drone technology uses specially designed interceptor drones to confront incoming UAV swarms. Counter-UAV drones can carry various weapons such as stun guns, capture nets, and jamming equipment. Coordinated with command and control systems, these drones can quickly identify and track target UAVs, selecting appropriate interception methods based on the situation. Upon detecting a target UAV, a counter-UAV drone can first emit jamming signals to disable it, then approach and use a stun gun to disable it for recovery. This method offers high flexibility and autonomy, effectively countering UAV swarm attacks in complex battlefield environments. However, counter-UAV drones themselves face the risk of attack, requiring enhanced self-protection and anti-jamming capabilities to ensure cooperative operational stability.

3.3.3 Anti-Aircraft Artillery and Missile Interception Technology

For large-scale, high-intensity UAV swarm attacks, anti-aircraft artillery (AAA) and missile interception technologies remain crucial. AAA features high rate of fire and dense firepower, enabling large-area engagement of low-altitude flying swarms. Modern AAA systems are equipped with advanced fire control radars and automatic loading mechanisms, capable of firing large volumes of shells in a short time to effectively intercept incoming swarms. Missile interception is suitable for striking long-range, high-speed UAVs, offering high precision and long range. However, due to high costs, missile interception is typically a last-resort defense measure for protecting critical strategic targets. In practical applications, deployment strategies for AAA and missiles need rational optimization, combined with other counter-UAV technologies, to enhance overall defense effectiveness.

3.4 Swarm Control Counter-Technologies

3.4.1 Swarm Jamming Technology

Targeting the collaborative control characteristics of UAV swarms, swarm jamming technology is developed to disrupt them. By analyzing the swarm's communication protocols and cooperative control algorithms, specific jamming signals are transmitted to disrupt their communication links and coordination mechanisms, causing the swarm to descend into chaos and fail to execute tasks normally. In practice, researchers can simulate UAV swarm communication signals and transmit matching jamming signals to disrupt their formation flying and eliminate their coordinated combat capability. However, as UAV swarm communication protocols become increasingly encrypted and

improved, swarm jamming technology needs to continuously track these changes and update jamming algorithms and signal patterns.

3.4.2 Deception Jamming Technology

Deception jamming technology misleads the flight direction and behavior of UAV swarms by transmitting false control commands or navigation signals. For example, it can send false target location information to cause the swarm to deviate from its intended attack direction, or send false return-to-home commands to make the swarm return to an incorrect location. Implementing deception jamming requires a deep understanding of the swarm's control algorithms and communication protocols, presenting high technical difficulty. However, once successfully executed, it can cause significant disruption. In practical applications, it requires combining real-time monitoring and data analysis to accurately grasp the swarm's state and timely adjust deception signals to increase the success rate.

3.4.3 Intelligent Countermeasure Technology

Utilizing AI technology to develop intelligent counter-UAV swarm systems. Such systems can monitor the behavioral characteristics of UAV swarms in real-time, predict their intentions using machine learning algorithms, and automatically generate corresponding countermeasure strategies. When the system detects an attack intent from a swarm, it can automatically deploy countermeasure resources and select the optimal jamming or interception method. Intelligent countermeasure technology offers high autonomy and adaptability, enabling rapid and effective responses to UAV swarm threats in complex and dynamic battlefield environments. However, training intelligent countermeasure systems requires vast amounts of sample data and powerful computing resources. They also face risks of algorithm compromise and adversarial attacks, necessitating continuous enhancement of algorithm security and robustness.

4 Conclusion

As an emerging technological force, UAV swarms bring innovative applications while posing severe challenges to social safety and military defense. Their characteristics – sudden attacks, powerful destructive capability, information jamming and theft abilities, and difficulty in defense and tracking – place immense pressure on traditional security measures. Therefore, active development and innovation in counter-UAV swarm technologies are essential to effectively address the threats posed by UAV swarms. In the future, with continuous technological advancement, both UAV swarm technology and counter-UAV swarm technology will continue to evolve. Sustained research and application of related technologies are crucial to safeguard public safety, national security, and maintain social stability and development.