Human Factors in Robots, Drones and Unmanned Systems, Vol. 179, 2025, 23–31
https://doi.org/10.54941/ahfe1006371

Blocking System for Autonomous Flight Drones

Ryushun Oka, Tahara Jumpei, Koshijima Ichiro, and Kenji Watanabe

Nagoya Institute of Technology, Gokiso-cho, Showa-Ku, Nagoya, Aichi, 466–8555 Japan

ABSTRACT

In recent years, the misuse of drones has emerged as a serious threat, particularly in scenarios involving criminal or terrorist activities. Drones typically rely on GNSS (Global Navigation Satellite Systems) and radio control signals for autonomous navigation, making them susceptible to interference-based countermeasures. While conventional solutions such as drone guns can neutralize individual threats by emitting high-power jamming signals, they are limited in scalability, precision, and the ability to manage swarm attacks. Moreover, indiscriminate jamming may inadvertently disrupt legitimate drones operating in the same airspace. Overcoming these challenges, the authors propose an active defense system that uses multiple directional antennas to generate focused, low-power interference zones. The system supports adaptive control over the jamming area and incorporates deception strategies, such as intentionally leaving navigable "gaps" to mislead unauthorized drones into controlled interception zones. A human-in-the-loop framework further enhances operational flexibility by allowing real-time decision-making. At the same time, a Local Positioning System (LPS) safeguards the operation of authorized drones even within jammed environments.

Keywords: Human factors in robots, Drones, Unmanned systems

INTRODUCTION

Drones are utilized in various industries due to their high versatility. On the other hand, there are growing concerns about their illicit use or so-called drone threats. Because of their versatility, drones can be exploited for terrorist attacks. For instance, one can imagine the damage that would result if a bomb or other hazardous material were attached to a drone, flown over Tokyo's Shinjuku district, and dropped there. Additionally, a camera-equipped reconnaissance drone could steal information from critical infrastructure operators. Consequently, law enforcement agencies worldwide are now employing various devices to counter the threats posed by drones.

EXISTING COUNTERMEASURES

To protect against drone threats, we must be able to detect them. There are many methods of drone detection, primarily using visible light or infrared, sound, or radio waves. However, each of these methods has its limitations.

Detection using visible or infrared light relies on visual observation or camera systems, making it greatly affected by obstructions and weather conditions, and there is also a limited range in which drones can be detected. Similarly, sound-based detection is limited by the properties of sound waves, which restrict the distance over which it can be effective (Abro et al., 2022) (Khan et al., 2022).

Radio wave-based detection employs radar systems, of which there are two types. The first type detects drones by transmitting radio waves and receiving the waves reflected from the drone. The second type detects drones by receiving the radio waves that control them. Both of these methods also have limitations in their detection range. For instance, if a drone is stealth-equipped or is an autonomous type that does not emit any radio waves at all, it may go undetected. Failing to detect such drones can gravely impact our ability to respond to these threats (Robin Radar Systems, 2022).

PROBLEM

In summary of the previous chapter, two major countermeasures against drone threats have been implemented in the real world. However, both methods assume that the drone has already been detected.

1. Physically Capturing Drones with Nets

To physically capture a drone using a net, one must prepare the net in advance, which can be time-consuming to deploy (Yu et al., 2022).

2. Using a Jamming Gun

Much like operating a conventional firearm, a jamming gun can quickly emit jamming signals at the target drone. However, because it provides only a one-to-one countermeasure, it cannot address threats posed by swarms of drones. Furthermore, if the jamming signals need to be emitted for an extended period, there is a high risk of interfering with other systems (Jensen, 2024).

Related Research

Research on GNSS jamming and spoofing has been conducted to disrupt drone flights through jamming. GNSS jamming can almost block location information in most drones, effectively turning off their "return-to-home" function. Meanwhile, GNSS spoofing has been reported to force a drone to land by guiding it into a designated "No-Fly Zone (NFZ)" (Zidane et al., 2024).

However, it has also been suggested that jamming may interfere with legitimate communications, potentially affecting a wide area (Gummadi et al., 2007). Furthermore, from a fuzzing perspective, it has been pointed out that research focusing on GNSS-based drone security has not progressed significantly, which remains an issue (Malviya et al., 2025). Hence, there is still room for further investigation into the emission of jamming signals targeting GNSS.

Proposed Method

In this study, we propose disrupting the flight of unauthorized drones by emitting radio waves that interfere with the reception of their GNSS and control signals. We employ multiple array antennas to transmit directional jamming signals to achieve disruption. Each jamming signal is weak, posing no impact on electronic devices used in public areas. However, by directing multiple jamming signals to a specific area and aligning their phases, it is possible to intensify the interference within that particular region to a level that disrupts the drone's regular operation (Jiang et al., 2023). By scanning this targeted interference area at high speed, we can create an interference plane, and by further moving that plane vertically, we can generate a three-dimensional interference region.

Simulation and Validation

In the previous chapter, we proposed a method to concentrate directional jamming waves (jamming signals) emitted from multiple array antennas onto a specific area and align their phases, thereby raising the interference level only within that target area to disrupt the regular operation of drones. To evaluate whether this is feasible, we conducted simulations.

In real urban environments, antenna installation heights are expected to vary due to differences in building elevations and terrain. The proposed system is designed such that each antenna is independently steered and beamformed. Even when antennas are positioned at different heights, phase adjustment maximizes the interference intensity at the target point. Furthermore, by integrating terrain data and building height information from a three-dimensional (3D) map, it is possible to implement an algorithm that dynamically recalculates the optimal interference location in real-time, enabling the system to adapt flexibly to complex and variable topographies.

The proposed system has a clear trade-off between the number of antennas, transmission power, and coverage area. Expanding the coverage area requires increasing the transmission power or deploying additional antennas. However, excessive power output may lead to unintended interference in non-targeted regions; therefore, increasing the number of antennas is generally preferred to achieve wider coverage while minimizing collateral effects.

This system utilizes beamforming technology to focus radio waves from multiple antennas onto a specific area. Adjusting the phase and amplitude of each antenna's signal allows interference to be concentrated within the desired region while minimizing its impact outside the target zone.

Since implementing this system necessitates deploying multiple high-gain directional antennas, the balance between cost and feasibility must be considered. At this stage, leveraging existing infrastructure—such as public facilities and communication towers—is a viable strategy for reducing initial installation costs.

As illustrated in Figure 1, five transmission points (Tx1 through Tx5) emit signals (continuous waves at 1575.420 MHz, corresponding to GPS L1) from three buildings toward a single point. Each antenna is assumed to maintain an ideal directional pattern in this simulation.

Building: (X : Y : Z = 100 m : 100 m : 200 m)
Antenna:
Directional Antenna (Height: 180 m)
Beamwidth (E-plane half-power and H-plane half-power): 5°
Maximum Antenna Gain: 31.628dBi
Receiver:
Isotropic (Height: 180 m)

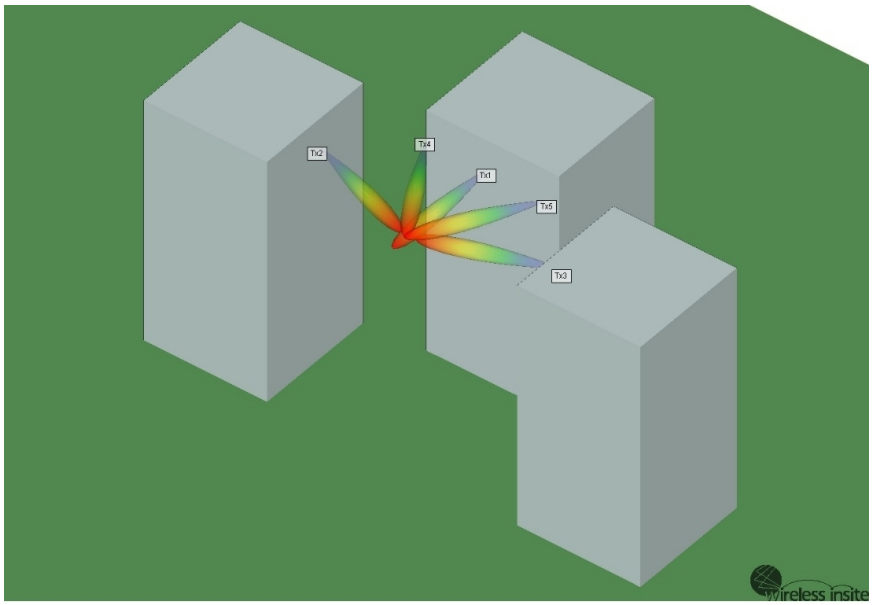

Figure 1: Antenna placement.

Simulation Results and Evaluation

Figure 2 shows the simulation results when radio waves are transmitted from each transmission point at the power levels indicated below (Isotropic). In each simulation, the received power at isotropic receivers placed at 0.5 m intervals is visualized as a heatmap.

Figure 2 shows that the radio waves emitted from each transmission point intersect at a single location, increasing the power level at that intersection. Because the power level at this intersection exceeds the threshold required for jamming, it is possible to perform jamming only at that specific point. Assuming that GNSS interference becomes effective at around −170 dBm/Hz, any point on the heatmap displaying a value (color) above the brown range indicates successful jamming.

Figure 3 shows a simulation (visualized as a heatmap) where the number of transmission points has been reduced from five to three yet still exceeds the necessary power threshold to achieve jamming levels similar to those in Figure 2. The power levels transmitted from each point under these conditions are as follows.

Tx1:-132dBm/Tx2:-133dBm/Tx3:-133dBm/Tx4:-132dBm/Tx5:-132dBm

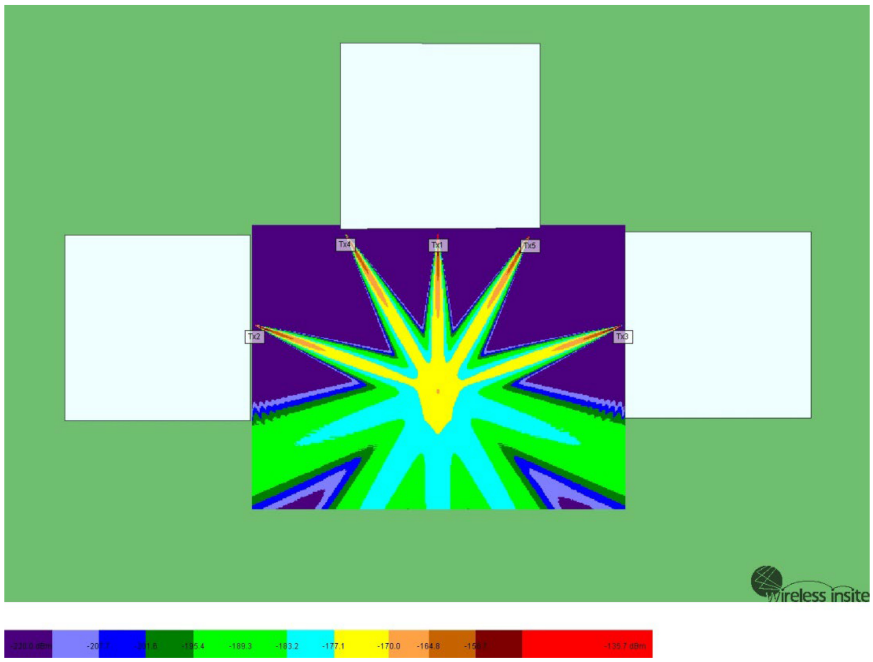

Figure 2: Total power (Tx:5Ver).

Tx1:-129dBm/Tx2:-131dBm/Tx3:-131dBm

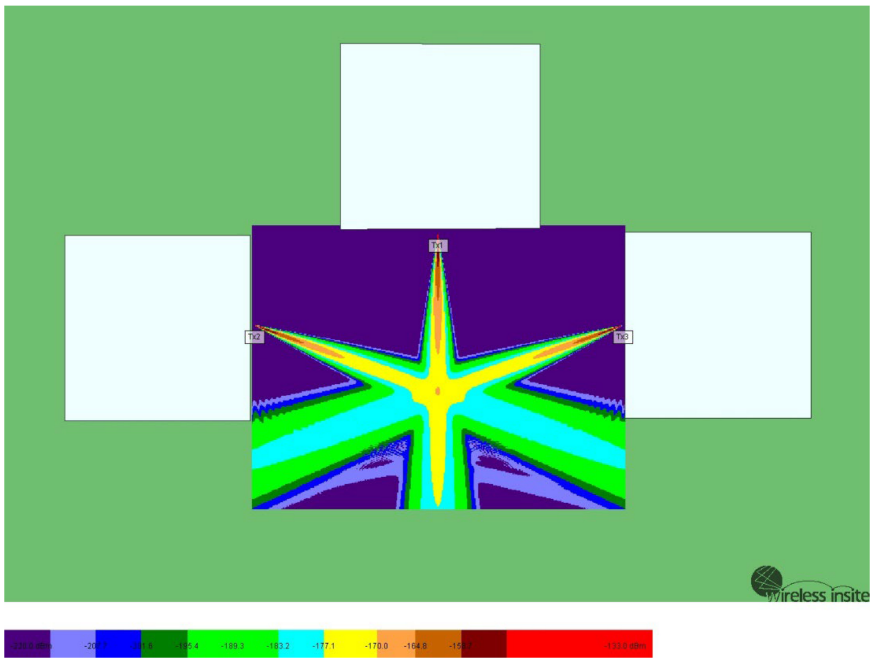

Figure 3: Total power (Tx:3Ver).

Because the power radiated from each transmission point has increased, each transmitter's effective jamming range has been significantly extended.

Figure 4 shows the case with five transmission points, as in Figure 2. The target point is scanned by controlling the antenna directivity so that the emitted signals exceed the power threshold necessary for jamming. Thus, it is possible to scan the jamming point by adjusting the antenna directivity.

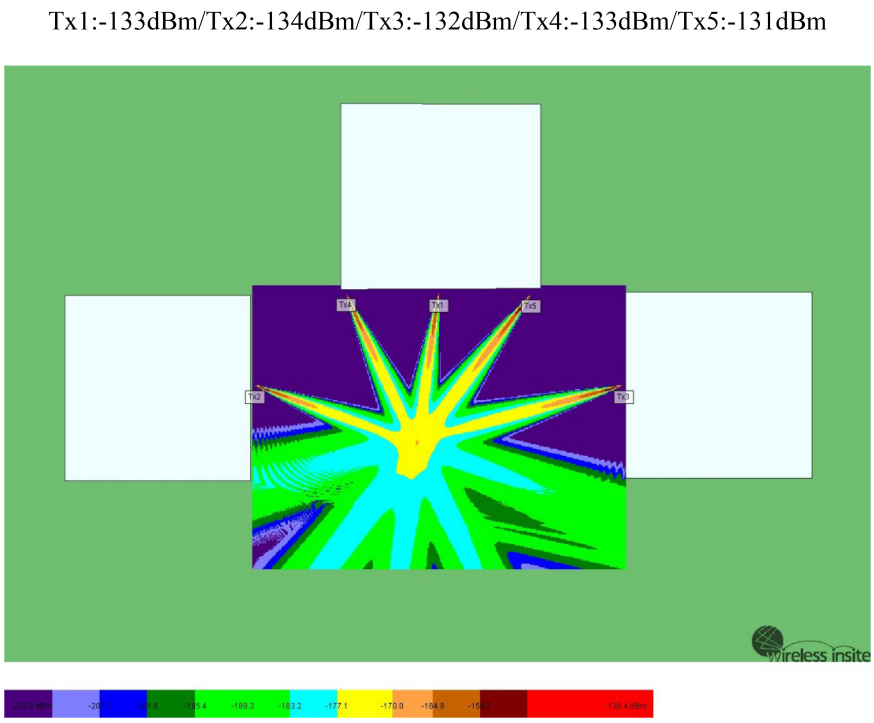

Figure 4: Total power (Tx:5 move Ver).

The Human-in-the-Loop Approach

The jamming-based drone countermeasure proposed in this study is a powerful technique capable of uniformly disrupting unauthorized drones across a wide area by emitting focused radio frequency interference. However, its high effectiveness introduces the potential risk of indiscriminately affecting unauthorized and authorized drones. In real-world environments, legitimate drones routinely operate in shared airspace, including those used for public services, logistics, and infrastructure inspections. Disrupting such drones, even unintentionally, can lead to significant social, operational, and legal consequences. To address this challenge, we integrate a human-in-the-loop framework that enables human operators to control and make real-time decisions. Rather than relying solely on static or automated jamming patterns, operators can dynamically adjust interference zones, implement strategic gaps, and respond to evolving threats based on situational awareness. This human-technology interaction enhances system safety and

adaptability and supports the implementation of deception-based tactics, as discussed in the following section.

Assumption of the attacker's perspective

Conventional drone countermeasures have traditionally been developed from the perspective of system operators, focusing primarily on defensive technical measures. However, from a human factors perspective, it is equally important to consider malicious actors' behavioral patterns and decision-making processes, namely unauthorized drone operators, and how they might attempt to evade or exploit the system.

The proposed system incorporates the philosophy of active defense, whereby it not only disrupts unauthorized drones through broad-area jamming but also strategically manipulates the attacker's behavior. Figure 5 illustrates a uniformly jammed area, within which a deliberate "gap" or "safe corridor" is intentionally left open. This gap is designed to appear as a weakness or blind spot in the system to entice the attacker.

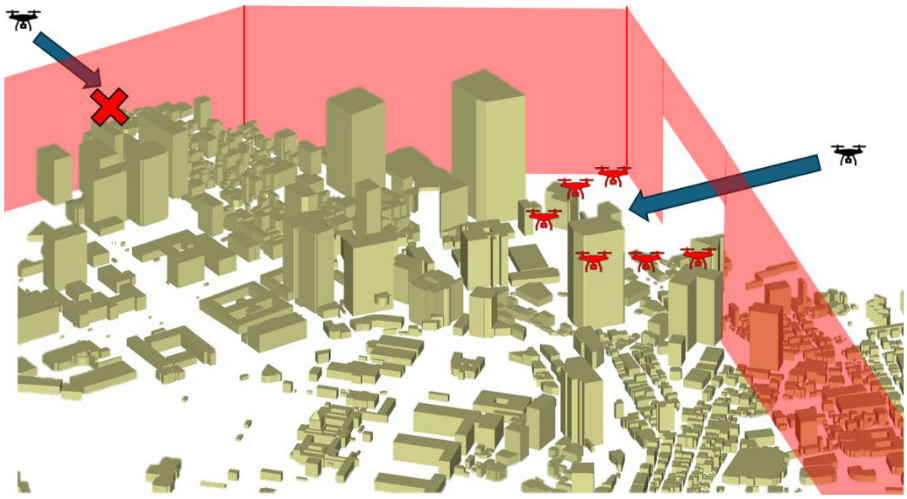

Figure 5: Defense and deception points of the proposed system (Black drone: Malicious UAV, red drone: Defensive UAV).

Due to the highly constrained operational space imposed by jamming, the attacker is psychologically guided toward this gap, believing it to be a safe path through the interference zone. Once the hostile drone enters the gap, it can be neutralized through a secondary defense mechanism, such as interception by a counter-drone or physical disablement using dedicated response units.

This approach limits the range of available attack vectors and gives the defender strategic control over the engagement by shaping the attacker's perception and choices. By integrating this tactic with a human-in-the-loop framework, system operators can dynamically adjust jamming parameters, activate or deactivate gaps in real-time, and respond adaptively to changing threats.

From a human factors standpoint, this strategy leverages both the system's technological capability and adversaries' psychological tendencies, enabling a more comprehensive and sustainable model of drone defense. *It should be noted that any physical countermeasures must comply with applicable legal and ethical guidelines.

Role of the Operator

The operation of conventional jamming systems requires monitoring and real-time decisions. The final judgment of "friend or foe" is typically entrusted to human situational awareness and decision-making abilities.

However, modern drone technologies are advancing rapidly, often surpassing human judgment capabilities, and hesitation in decision-making can hinder the timely deployment of jamming.

Remedies for Drones Other Than Unauthorized Ones

This method affects all drones passing through the target area, which may interfere with authorized drones. We propose introducing a local positioning system (LPS) that combines multiple positioning technologies to address this issue. For example, the transmitter (Tx) that emits the jamming signal can also be equipped with an LPS signal transmitter, allowing drones to calculate their position based on these signals.

With this approach, drones operating in jamming environments can still obtain their location data and safely continue flying. Furthermore, using pre-shared keys for encryption and authentication prevents unauthorized drones from calculating their location or impersonating authorized drones.

This approach also eliminates the need for the system operator to make direct jamming decisions, allowing for uniform interference against all non-authorized drones.

Detection and Provision of Drone Position Information

While the system's primary function is to emit radio signals toward drones, it can also receive reflected waves from flying objects and determine their positions. As a result, system operators can manage drones based on precise three-dimensional positional data that is independent of GNSS.

CONCLUSION

This study proposed a novel countermeasure method to prevent unauthorized drone flights by jamming GNSS signals and controlling radio waves. Conventional drone countermeasures, such as drone guns and physical capture methods, have issues, including one-to-one engagement constraints, time-consuming preparation, and the potential to interfere with surrounding electronic devices. By leveraging directional jamming technology using multiple array antennas, our approach focuses radio waves only on specific areas, providing a more efficient drone countermeasure.

Simulation results demonstrated that localized jamming is feasible by optimizing transmitter locations and that controlling the directivity enables

movement of the jamming area. This localized jamming makes it possible to deal with multiple drones while minimizing unnecessary radio interference.

However, this method may still affect legitimate drones, which remains challenging. To address this, we proposed using a local positioning system (LPS) so that authorized drones can continue to operate even in a jamming environment. We also examined combining encryption and authentication technologies to prevent spoofing by unauthorized drones.

Future tasks include conducting demonstration experiments in real-world environments and developing advanced techniques for controlling the jamming area. Additionally, jamming technology's legal and ethical implications must be carefully considered. The outcomes of this research contribute to advancing drone countermeasure technologies, and further studies toward refinement and practical implementation are warranted.

REFERENCES

Abro, G. E. M., Zulkifli, S. A. B. M., Masood, R. J., Asirvadam, V. S. and Laouiti, A. (2022) 'Comprehensive review of UAV detection, security, and communication advancements to prevent threats', *Drones*, 6(10), p. 284. Available at: https://doi.org/10.3390/drones6100284.

Gummadi, R., Wetherall, D., Greenstein, B. and Seshan, S. (2007) 'Understanding and mitigating the impact of RF interference on 802.11 networks', Computer Communication Review (CCR), 37, pp. 385–396. Available at: https://doi.org/10.1145/1282427.1282424.

Jensen, J. (2024) 'Drone jammers: An inside look at counter UAS technology for drone pilots', *UAV Coach*, 25 July. Available at: https://uavcoach.com/drone-jammer/.

Jiang, Y., Zhou, L., Tang, Y., Tu, Y., Liu, C. and Shi, Q. (2023) 'A collaborative jamming algorithm based on multi-UAV scheduling', *Proceedings of the 2023 IEEE 23rd International Conference on Communication Technology (ICCT)*, pp. 372–377. Available at: https://doi.org/10.1109/ICCT59356.2023.10419673.

Malviya, V. K., Minn, W., Shar, L. K. and Jiang, L. (2025) 'Fuzzing drones for anomaly detection: A systematic literature review', Computers & Security, 148, p. 104157. Available at: https://doi.org/10.1016/j.cose.2024.104157.

Khan, M. A., Menouar, H., Khalid, O. M. and Abu-Dayya, A. (2022) 'Unauthorized drone detection: Experiments and prototypes', *arXiv*. Available at: https://arxiv.org/abs/2212.01436.

Robin Radar Systems (2022) 'The pros and cons of radio frequency analysers in drone detection'. Available at: https://www.robinradar.com/blog/radio-frequency-analysers-drone-detection.

Yu, D., Judasz, A., Zheng, M. and Botta, E. (2022) 'Design and testing of a net-launch device for drone capture', *AIAA SCITECH 2022 Forum*. Available at: https://doi.org/10.2514/6.2022-0273.

Zidane, Y., Silva, J. S. and Tavares, G. (2024) 'Jamming and spoofing techniques for drone neutralization: An experimental study', Drones, 8(12), p. 743. Available at: https://doi.org/10.3390/drones8120743.