TRANSNAV
http://www.transnav.eu
the International Journal on Marine Navigation and Safety of Sea Transportation
Volume 19
Number 3
September 2025
DOI: 10.12716/1001.19.03.27

Survey on Intentional Interference Techniques of GNSS Signals and Radio Links between Unmanned Aerial Vehicle and Ground Control Station

J. Dułowicz[1,2], P. Skokowski[2] & J.M. Kelner[2]
[1] *Cyber Defense Forces Component Command, Warsaw, Poland*
[2] *Military University of Technology, Warsaw, Poland*

ABSTRACT: With the rapid development of unmanned aerial vehicle (UAV) technology, UAVs are gaining increasing importance in civilian, industrial, and military applications. UAVs are used for environmental monitoring, medical deliveries, emergency response, and reconnaissance missions. However, their widespread use also introduces new security challenges, driving the advancement of counter-unmanned aerial systems (C-UASs). This paper provides a comprehensive review of intentional interference techniques targeting the radio links between UAVs and ground control stations, as well as global navigation satellite system (GNSS) signals, which are essential for autonomous and remote-controlled UAV one operations. The paper examines the radio frequency spectrum utilized by UAVs and characterizes their typical radio emissions. It presents a detailed classification of jamming methods, ranging from conventional noise jamming to advanced intelligent jamming and spoofing techniques. Furthermore, it explores a wide range of spoofing attacks against GNSS receivers, including replay attacks, signal forgery, estimation-based spoofing, and cooperative advanced methods. Each technique is analyzed in terms of implementation complexity and operational effectiveness. In addition, the paper highlights commercial C-UAS solutions, showcasing practical approaches to UAV mitigation through targeted signal disruption. This review offers an in-depth overview of current threats and defense technologies, serving as a foundation for future research on adaptive and selective UAV neutralization methods.

1 INTRODUCTION

The development of unmanned aerial vehicles (UAVs) is one of the most innovative and dynamic areas in the field of aviation advancement [1]. In recent years, there has been a significant increase in interest in this topic from private companies, the military, and governments around the world [2], [3]. This phenomenon is driven by the intended use of UAV systems in medical, transportation, and military applications. As UAV technology has evolved, so has the demand for counter-unmanned aerial systems (C-UASs), called also anti-drone systems [4]. Initially, UAV technology was used for recreational purposes, but over time, its range of functions has expanded to include the execution of a variety of tasks. Application areas for UAVs (calls also drones) include agriculture, environmental monitoring, public safety, combat operations, and the entertainment industry [5], [6]. In addition, recent years have seen a marked increase in interest in artificial intelligence (AI) techniques, enabling the implementation of autonomous systems in UAV applications [7]. Integrated AI systems allow for independent decision-making and adaptability to vicinity changes in the execution of UAV tasks [8].

The combination of sensor arrays, machine learning algorithms, and modern wireless communication systems enables task execution with minimal human involvement [9]. The advancement of UAV technologies increases their potential for use in national defense applications [10]. Most commonly, they are used in reconnaissance operations (such as border surveillance and intelligence gathering) as well as in military missions to minimize risk to personnel. As drones are increasingly used for various purposes, there is a growing need to develop effective C-UASs [4]. These systems employ a range of techniques for UAV detection and neutralization. These include radar-based systems (both passive and active), visual recognition techniques, acoustic detection methods (both passive and active), and radio signal recognition techniques [11]. In the context of national security, C-UASs may serve as a component of strategic military defense, as well as to reduce terrorist attacks or crimes committed using drones [12].

The rest of the paper is organized as follows. Section 2 presents analysis of the radio spectrum in terms of UAV navigation and communication systems. Review of radio emissions used in UAV communication links and GNSS signals is described in Section 3. Classifications of jamming methods targeting UAV radio links and GNSS receivers are shown in Sections 4 and 5, respectively. Section 6 describes sample of commercial hardware solutions of C-UAS. Finally, paper summary is contained in Section 7.

2 ANALYSIS OF RADIO SPECTRUM IN TERMS OF UAV SYSTEMS

In the operation of UAVs the primary control frequencies are typically defined within the 2.4 GHz and 5 GHz bands. Additionally, unlicensed bands, so-called industrial, scientific, medical (ISM) bands, ranging from 900 MHz to 1.3 GHz, are commonly utilized for drone communication in scientific, transportation, and emergency medical response applications [13]. Considering the capability of a jamming system to disrupt drones operating across various frequency bands, it is advisable to implement detection mechanisms not only for commercial bands (i.e., 2.4 and 5 GHz) and amateur bands (i.e., 433 MHz), but also for other ISM bands, in order to enhance the versatility of the jamming system.

The general range of commercial frequency usage should be assumed to span from 900 MHz to 5.8 GHz. However, unlicensed bands above 6 GHz (i.e., from 5.925 GHz to 7.125 GHz) [14], as well as the 433 MHz amateur band, should not be completely excluded. UAVs also utilize GNSS technologies to obtain positional information, support positional correction, and enable automated route-based flight. GNSSs commonly used include the United States Global Positioning System (GPS), China's BeiDou Navigation Satellite System (BDS), the European Union's Galileo, and Russia's GNSS (i.e., GLONASS) [15]. These GNSSs operate within the following frequency ranges [16]:

- GPS: L1 (1227.60 ± 10.23 MHz) and L2 (1575.42 ± 10.23 MHz);
- GALILEO: E1 (1227.60 ± 1.023 MHz) and E5b (1575.42 ± 1.023 MHz);
- BDS: B1 (1561.098 ± 2.046 MHz) and B2 (1207.14 ± 2.046 MHz);
- GLONASS: L1 (1602.5625 ± 4 MHz) and L2 (1246.4735 ± 4 MHz).

When designing and implementing a potential C-UAS, it is recommended to develop a jamming or spoofing solution that targets the most commonly used communication frequencies between an operator (i.e., ground station) and UAV, as well as the frequencies employed by GNSSs. A more comprehensive solution should also include other unlicensed and non-standard (e.g., governmental) frequency bands to ensure broader system effectiveness.

3 OVERVIEW OF RADIO EMISSIONS USED IN UAV COMMUNICATIONS AND GNSS SIGNALS

Currently, a significant number of UAVs operate on frequencies close to those used in the Wi-Fi standard [17]. This section presents aspects related to the detection of radio signals emitted by commercial drones. Radio emissions of an UAV typically consists of two main components, i.e., control and video transmission links. The first one is responsible for motor control and sensor data transmission, while the second link type is commonly referred to as first person view (FPV) from the UAV camera. By detecting a drone's signal, it is possible to determine the operating channel by converting the signal from the time domain into the frequency domain. This is most often accomplished using the fast Fourier transform (FFT) algorithm. Figure 1 illustrates a comparison between the remote-control, Wi-Fi channel, and FPV video signals in the frequency domain [17].

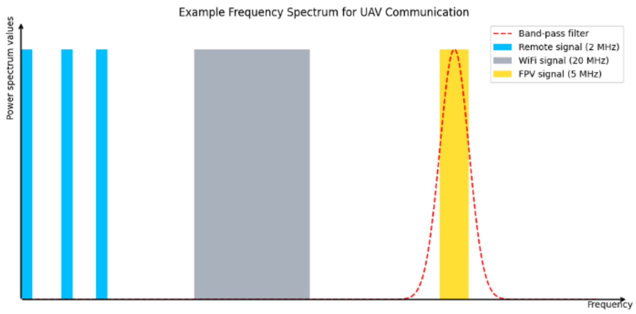
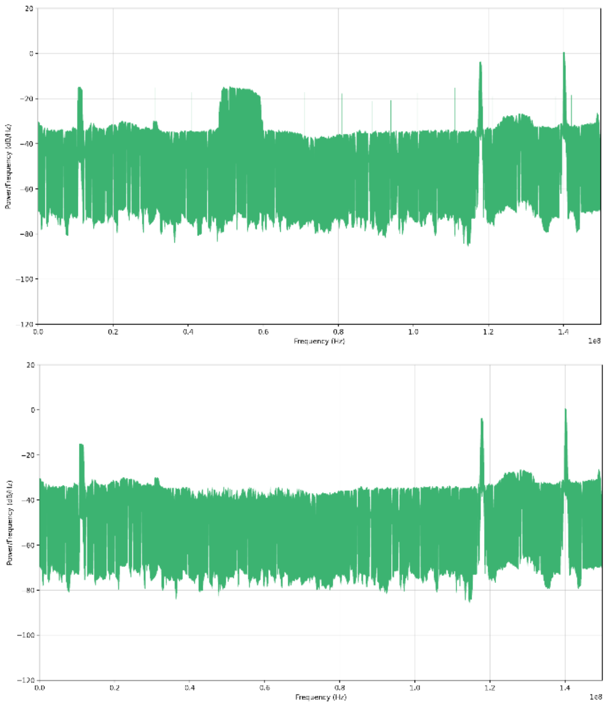


Figure 1. Comparison of remote-control, Wi-Fi channel, and FPV video signals.

The remote-control signal is represented by three narrow sub-bands, each with a bandwidth of up to 2 MHz. The FPV signal is shown as a continuous wideband signal with a bandwidth of approximately 9 MHz. Both the remote control and FPV signals fall within the standard 20 MHz Wi-Fi channel. Table 1 presents the frequency ranges for the FPV (map transmission signal), remote control, and Wi-Fi signals. Figure 2 depicts spectra of sample radio signals emitted by a UAV [17].

Table 1. Frequency ranges for the FPV signal, control signal, and Wi-Fi signal.

Signal type	Frequency band	Bandwidth
Map transmission (FPV) signal	2.404÷2.47 GHz 5.725÷5.775 GHz	9 MHz
Remote-control signal	2.404÷2.47 GHz	2 MHz
Wi-Fi signal	2.40÷2.483 GHz 5.15÷5.85 GHz	20 MHz



a)

b)

Figure 2. Sample spectra of radio signals emitted by UAV: (a) with and (b) without of FPV signal [17].

Figure 2 (a) shows that the spectrum of radio signals emitted by a UAV can be divided into several key segments. The initial segment constitutes the first part of the remote-control signal with a bandwidth of approximately 2 MHz. Next, there is an FPV sub-band with a bandwidth of about 9 MHz. The last two sub-bands correspond to the second and third parts of the remote control signal, each with a bandwidth of approximately 2 MHz. It should be noted that the remote-control signal is characterized by a higher power level and significantly narrower bandwidth compared to the FPV signal, which may be important when selectively jamming specific portions of the UAV radio transmission. In the case of jamming only the remote-control signal, it is possible to deceive the UAV operator by making the signal quality degradation appear unintentional. Figure 2 (b) presents the UAV emission excluding the FPV signal.

As we mentioned, each UAV additionally is supported by GNSS. Figure 3 draws exemplary spectra of different GNSS signals [18].

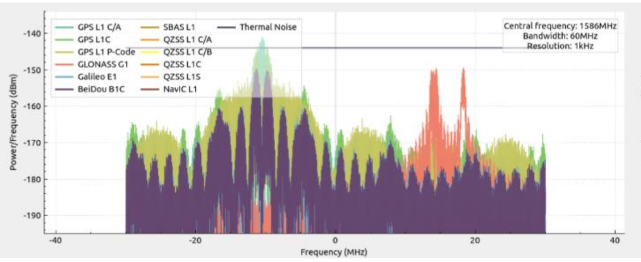


Figure 3. Sample spectra of GNSS signals [18].

When attempting for jamming the connection with a UAV or spoofing GNSS signals, it should be considered the operating frequency ranges of these systems, the power levels of the signals, as well as the their channel bandwidths.

4 CLASSIFICATION OF UAV RADIO LINK INTERFERENCE AND JAMMING METHODS

This section describes a classification of jamming methods targeting UAV radio links. Jamming is defined as intentional interference caused by the generation of radio signals with sufficient power to disrupt the operation of the targeted device. Often, when the useful signal reaches the receiver along with a jamming signal, it becomes impossible to extract meaningful information [19]. Jamming methods can be classified as follows [20]:

– narrowband noise jamming [21], [22], [23];
– wideband noise jamming ("brute-force") [21], [24], [25];
– ultra-wideband (UWB) noise jamming [15], [26];
– swept noise jamming [20], [27], [28];
– intelligent noise jamming [20] [24] [29];
– response jamming (spoofing) [30], [31].

4.1 *Narrowband Jamming*

Narrowband jamming can be classified as single-frequency jamming, pulsed jamming, or low-bandwidth signal jamming [22]. Unlike wideband jamming, narrowband jamming can achieve higher instantaneous power values, which also affects its effective range [21], [23].

4.2 *Wideband Noise Jamming*

Noise jamming is a method of interference using noise with specific characteristics, power level, and bandwidth, aimed at reducing the signal-to-noise ratio of the useful signal. This type of interference is widely used in communication channel disruption [21], [24]. In this type of jamming, studies have been conducted on the effectiveness of Gaussian noise and phase noise, tested through simulation methods [25].

4.3 *Ultra-Wideband Jamming*

UWB jamming uses a wideband noise signal that spans the entire frequency range of the targeted signal. As a result, this type of jamming can be used to disrupt a UAV control channel, video link, or the entire UAV communication link. However, its major drawback is the high-power requirement needed to ensure a sufficient noise-to-signal ratio to effectively jam the selected signal [15], [26]. Figure 4 presents a comparison of spectra of narrowband (a) and wideband (b) jamming signals.

4.4 *Sweep Noise Jamming*

Sweep noise jamming is a type of jamming that involves rapidly sweeping a relatively narrowband signal across the entire frequency range of the target signal [28]. The jamming signal may consist of noise or pulsed signals. At any given moment, only a specific frequency band is jammed, which may be insufficient for disrupting systems that use frequency-hopping spread spectrum (FHSS). Although the frequency range of the jamming signal overlaps with that of the target signal, there is no guarantee that the ranges will align at every moment during the jamming process. However, this form of jamming is effective against direct sequence spread spectrum (DSSS) signals with stationary spectra [20]. Figure 5 shows an example of fifth-generation (5G) channel jamming using the sweep noise jamming method, with a sweep rate of 10 hops per second [27].

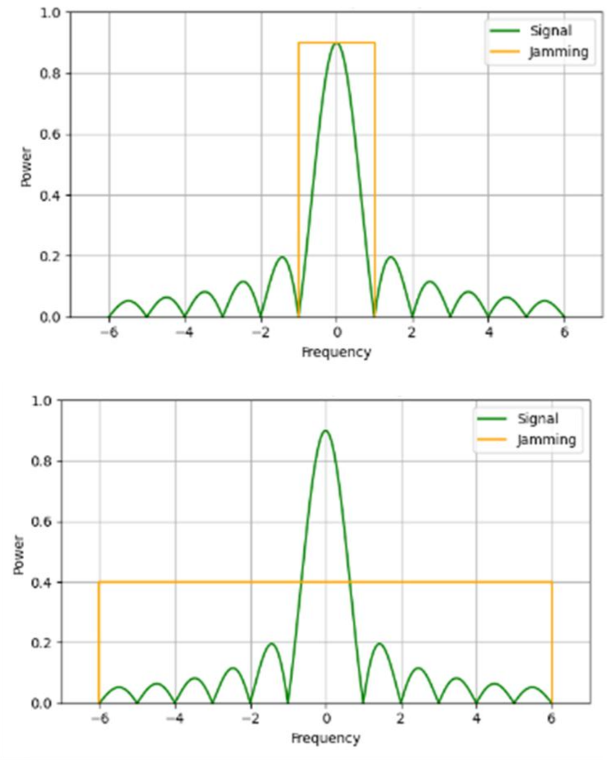


Figure 4. Comparison in frequency domain between (a) narrowband and (b) wideband jamming for example signal [20].

Figure 5. Example of 5G channel jamming using sweep noise technique with sweep rate of 10 changes per second [27].

4.5 *Intelligent Noise Jamming*

Intelligent noise jamming uses only those signals that are necessary to disrupt communication between the transmitter and the receiver of the desired signal. Prior knowledge of the type of signal being jammed is required in order to determine its structure in relation to relevant frequency sub-bands. Based on the analysis of selected UAV communication protocols and the received signal, it is possible to identify critical points where interference can disrupt the connectivity of the given system. This method allows for energy-efficient and less invasive generation of a jamming signal by reducing the bandwidth of the jamming spectrum. The method of generating such a signal is similar to response jamming or spoofing [20], [24], [29].

4.6 *Response Jamming (Spoofing)*

Response jamming, also known as spoofing, is a method of generating falsified signals based on the received signal. Unlike traditional jamming methods, this technique does not aim to interrupt communication between the transmitter and receiver but instead it generates an artificial signal intended to deceive the receiver (in this case, a UAV). This involves receiving the original signal, analysing and extracting the necessary data, modifying it, and then generating a fake signal in such a way that the receiver is unaware that it comes from an external source. The growing number of UAV manufacturers and communication protocols makes it difficult to develop a universal spoofing approach. However, some existing UAVs have been subjected to practical tests that determine their vulnerability to spoofing attacks [30], [31].

5 CLASSIFICATION OF GNSS JAMMING AND SPOOFING METHODS

For most GNSS receivers, the received satellite signal strength is very low, making it susceptible to interference. To minimize the impact of interference on GNSS reception, filtering systems are used to reduce noise in the receiver chain. However, when a jammer or spoofer is used, there is a high probability that the real GNSS signal will be filtered out and the receiver will instead accept the interference or the spoofed signal [32]. GNSS spoofing attacks can be classified as follows:

- Replay spoofing attack (RSA):
  - Direct replay type interference [33],
  - High power replay interference [34], [35],
  - Selective delay replay interference [36], [37], [38], [39],
  - Multi-antenna receiver replays interference [40];
- Forgery spoofing attack (FSA):
  - Direct-generation forgery [41],
  - Analysis-generation forgery [42], [43],
  - Denial environment forgery [44],
  - Full-channel forgery [45], [46];
- Estimation spoofing attack (ESA):
  - Security code estimation and replay [47],
  - Forward estimation attack [48];
- Advanced spoofing attack (ASA):
  - Nulling attack [40],
  - Cooperative interference attack [49].

5.1 *Replay Spoofing Attack*

Replay spoofing involves delaying the transmission of a GNSS signal received by the receiver using a spoofing system. These types of attacks are simple to implement and offer moderate effectiveness.

5.1.1 *Direct Replay Type Interference*

This type of interference involves recording and replaying a received GNSS signal. It is generally not used due to its low effectiveness compared to other methods [33].

5.1.2 *High Power Replay Interference*

This method uses a high-power spoofed signal to deceive the GNSS receiver. The receiver may interpret the spoofed signal as genuine, mistaking the real satellite signal for multipath interference, thereby accepting the fake signal [34], [35].

5.1.3 *Selective Delay Replay Interference*

This interference method aims to delay the satellite signal in such a way that it alters the phase of the spreading code reaching the GNSS receiver [36], [37], [38], [39].

5.1.4 *Multi-Antenna Receiver Replay Interference*

In this method, multiple jamming devices located at different positions are used, making it harder for a GNSS receiver with a multi-antenna system to detect the angle of arrival of the spoofed signal [40].

5.2 *Forgery Spoofing Attack*

Forgery spoofing adjusts the receiver's signal parameters and generates a fake GNSS signal that leads to erroneous position readings. This method is of moderate implementation complexity and moderately good effectiveness.

5.2.1 *Direct-Generation Forgery*

This spoofing technique uses an field-programmable gate array (FPGA), digital signal processor (DSP), or software-defined radio (SDR) to directly emulate GNSS signals based on preloaded parameters. A radio signal is generated that closely mimics a real satellite signal. Some GNSS receivers may reject the spoofed signal. This method requires only a transmitter (no receiver) [41].

5.2.2 *Analysis-Generation Forgery*

Similar to direct-generation forgery but includes a receiver and analytical modules. Based on the real GNSS signal, the system creates a spoofed signal with parameters similar to the actual ones at a given time and location [42], [43].

5.2.3 *Denial Environment Forgery*

An advanced form of spoofing that builds on analysis-generation forgery by first emitting strong interference to block satellite signals. After the disruption, a spoofed GNSS signal is generated and the interference is stopped, increasing the chance that the receiver will accept the fake signal as genuine [44].

5.2.4 *Full-Channel Forgery*

Full-channel forgery is an advanced spoofing technique that emulates fabricated GNSS signals across all satellite channels simultaneously [46]. This method is significantly more convincing than previous techniques and remains effective even when basic anti-spoofing measures are in place. As an additional classification, spoofing attacks can be divided into static and dynamic types [45]. In the case of the static attack, a spoofed GNSS signal is sent to the UAV that does not change over time. Despite the drone's actual physical movement, the GNSS system will indicate that the UAV is fixed. This type of attack may be useful for simulating system failures or feeding false status information to the UAV's control system (i.e., operator). Figure 6 illustrates an example of a drone being spoofed using a static attack.

Figure 6. Spoofing UAV position using static attack.

Figure 7. Spoofing UAV position using dynamic attack.

A dynamic spoofing attack involves delivering an emulated GNSS signal to the detected UAV, containing variable signals corresponding to different positions (a multi-point set of coordinates that change over time). In this case, the GNSS system will indicate that the UAV is moving along a predefined path, regardless of its actual position or whether the drone is physically in motion. Figure 7 presents a UAV flight path map resulting from a dynamic spoofing attack. In this case, the blue line indicates the initial and final position of the GNSS receiver, while the green line indicates the initial and final spoofed location generated by the spoofer.

5.3 *Estimation Spoofing Attack*

Estimation spoofing targets certain civilian satellite signals by estimating unknown security codes. The method predicts satellite information and generates spoofed GNSS signals based on the estimated values intended for the GNSS receiver.

5.3.1 *Security Code Estimation and Replay*

Security code estimation and replay is a method involving the emulation of satellite signals using an artificially generated encryption algorithm. In practice, this method is not commonly used due to its high implementation complexity [47].

5.3.2 *Forward Estimation Attack*

Forward estimation attack targets the portion of GNSS messages that contains authorization data. It is rarely used in practice because of the difficulty of implementation, similarly to security code estimation and replay technique [48].

5.4 *Advanced Spoofing Attack*

Advanced spoofing targets more sophisticated GNSS receivers equipped with spoofing prevention mechanisms. This method generates spoofed signals based on combinations of characteristics of potentially received signals for more effective deception. It often involves multiple spoofing modules working together.

5.4.1 *Nulling Attack*

Nulling attack is an advanced technique that involves simultaneously transmitting a copy of the signal expected to be received by the GNSS receiver from multiple transmitting units. These transmitted copies have an inverted signal phase, which, when reaching the receiver, causes destructive interference with the satellite signal, effectively preventing reception. This method is known for its exceptional effectiveness [40].

5.4.2 *Cooperative Interference Attack*

Cooperative interference attack is a complex combination of multiple jamming techniques using several coordinated jamming systems. Even when sophisticated anti-spoofing techniques are employed, this method can prevent the end user from receiving valid data or ensuring data integrity [49].

5.5 *Summary of GNSS Spoofing Techniques*

Table 2 presents a summary of all discussed jamming and spoofing methods based on their implementation difficulty and operational effectiveness [32].

6 EXAMPLES OF COMMERCIAL HARDWARE SOLUTIONS FOR JAMMING UAV RADIO LINKS AND SPOOFING GNSS RECEIVERS

With the growing use of UAVs in both commercial and recreational applications, there is an increasing need to ensure security and privacy. As a result, there is a rising demand for technological solutions that can control and restrict UAV operations in designated areas. One such solution involves commercial systems designed to jam GNSS signals and UAV communication links.

In this section, we present three examples of C-UASs with significantly focusing on radio frequency (RF) sensors and effectors. Broader overviews of C-UASs, including other types of sensors and effectors, are included in [4], [12].

6.1 *DRONESHIELD DroneGun Tactical*

The DRONESHIELD DroneGun Tactical [50] is a non-kinetic C-UAS that uses jamming emitters. It is a portable, rifle-shaped device equipped with wide-range directional antennas and a control panel that allows the operator to select the frequencies to be jammed. By emitting targeted interference, the system forces the UAV to either land at a designated location or return to its take-off point. Figure 8 shows the DRONESHIELD system [50].

Figure 8. Handheld DRONESHIELD DroneGun Tactical system [50].

Table 2. Advantages and limitations of GNSS spoofing methods [32].

Type of spoofing attack	Implementation difficulty	Effectiveness
Replay spoofing attack (RSA):	Low	Moderate
Direct replay interference	Low	Low
High power replay interference	Low-medium	Moderate
Selective delay replay interference	Low-medium	Moderate
Multi-antenna receiver replay interference	High	Moderate-good
Forgery spoofing attack (FSA):	Medium	Moderate-good
Direct-generation forgery	Medium	Moderate
Analysis-eneration forgery	Medium-high	Moderate-good
Denial environment forgery	Medium	Moderate
Full-channel forgery	High	Good
Estimation spoofing attack (ESA)	Medium-high	Good
Forwarding spoofing attack	Medium-high	Good
Generation spoofing attack	Medium-high	Good
Advanced spoofing attack (ASA):	High	Good
Nulling attack	High	Moderate-good
Cooperative inference attack	High	Good

6.2 *Anti-UAV Defence System (AUDS)*

Figure 9. AUDS system in stationary configuration [51].

Anti-UAV Defence System (AUDS) [51] is a C-UAS developed by British companies Blighter Surveillance Systems, Chess Dynamics, and Enterprise Control Systems. It is intended for use by the military, governments, and homeland security forces to detect, track, classify, and disrupt threats posed by micro, mini, and large UAVs. The system features a directional radio frequency jammer used to disrupt the UAV's control signal. It employs four high-gain antennas and covers the frequency bands of the GNSS. AUDS can be deployed in various terrains and can operate from fixed installations or mobile platforms. Figure 9 depicts the AUDS in its stationary configuration.

6.3 *DRONE DOME*

The DRONE DOME system [52] provides a complete and comprehensive solution aimed at restricting unauthorized UAV flights within designated zones. DRONE DOME is capable of identifying unknown targets, generating alerts (based on a customizable rule engine), and operating without interfering with non-targeted aircraft by utilizing a defined jamming bandwidth and an advanced directional antenna. This feature makes DRONE DOME particularly effective in highly congested airspaces (civilian or military). DRONE DOME is a modular C-UAS that can be deployed in stationary, mobile, or customized configurations. Figure 10 presents the DRONE DOME system.

Figure 10. DRONE DOME system [52].

7 SUMMARY

The rapid development and growing ubiquity of UAV have necessitated the advancement of countermeasures capable of neutralizing potential threats posed by unauthorized or hostile drone operations. This survey presented a comprehensive overview of intentional interference techniques targeting UAV communication links and GNSSs, which are critical for drone control and positioning.

Key aspects of the radio spectrum used by UAVs were analyzed, emphasizing the dominant use of unlicensed ISM bands and the dependence on multiple GNSS constellations. A detailed examination of radio emissions revealed the typical structure and bandwidth characteristics of UAV control and video transmission links, underscoring their susceptibility to various forms of jamming. The paper classified multiple radio jamming methods, ranging from basic noise jamming to more advanced intelligent and response-based spoofing techniques. Similarly, GNSS spoofing was categorized into replay, forgery, estimation, and advanced attack strategies, each evaluated in terms of implementation difficulty and operational effectiveness. The final section presented real-world C-UAS solutions. These examples demonstrate how commercially available technologies can detect, track, and disable UAVs by targeting their radio and navigation links without physical destruction.

Overall, the paper highlights that as UAVs continue to evolve, so must the techniques and technologies used to counteract them. Future efforts should focus on the development of adaptive, intelligent, and minimally invasive countermeasures capable of responding dynamically to emerging UAV technologies and increasingly sophisticated communication protocols.

ABBREVIATIONS

5G	–	fifth-generation
AI	–	artificial intelligence
ASA	–	advanced spoofing attack
AUDS	–	Anti-UAV Defence System
BDS	–	BeiDou Navigation Satellite System
C-UAS	–	counter-unmanned aerial system
DSP	–	digital signal processor
DSSS	–	direct sequence spread spectrum
ESA	–	estimation spoofing attack
FFT	–	fast Fourier transform
FHSS	–	frequency-hopping spread spectrum
FPGA	–	field-programmable gate array
FPV	–	first person view
FSA	–	forgery spoofing attack
GNSS	–	global navigation satellite system
GPS	–	Global Positioning System
RF	–	radio frequency
RSA	–	replay spoofing attack
SDR	–	software-defined radio
UAV	–	unmanned aerial vehicle

UWB – ultra-wideband

ACKNOWLEDGEMENTS

This work was developed within the framework of the research grant no. UGB/22-059/2025/WAT, sponsored by the Military University of Technology (WAT), Poland.

REFERENCES

[1] S. A. H. Mohsan, N. Q. H. Othman, Y. Li, M. H. Alsharif, and M. A. Khan, "Unmanned aerial vehicles (UAVs): Practical aspects, applications, open challenges, security issues, and future trends," *Intel Serv Robotics*, vol. 16, no. 1, pp. 109–137, Mar. 2023, doi: 10.1007/s11370-022-00452-4.

[2] K. Bednarz, J. Wojtuń, J. M. Kelner, and K. Różyc, "Frequency instability impact of low-cost SDRs on Doppler-based localization accuracy," *Sensors*, vol. 24, no. 4, Art. no. 4, Jan. 2024, doi: 10.3390/s24041053.

[3] G. E. Jeler, "Military and civilian applications of UAV systems," in *2019 International Scientific Conference Strategies XXI. The Complex and Dynamic Nature of the Security Environment*, Bucharest, Romania, Nov. 2019, pp. 379–386. Accessed: July 24, 2025. [Online]. Available: https://www.ceeol.com/search/chapter-detail?id=824918

[4] D. Zmysłowski, P. Skokowski, and J. M. Kelner, "Anti-drone sensors, effectors, and systems – A concise overview," *TransNav Int. J. Mar. Navig. Saf. Sea Transp.*, vol. 17, no. 2, pp. 455–461, June 2023, doi: 10.12716/1001.17.02.23.

[5] M. Specht, S. Widźgowski, A. Stateczny, C. Specht, and O. Lewicka, "Comparative analysis of unmanned aerial vehicles used in photogrammetric surveys," *TransNav, International Journal on Marine Navigation and Safety od Sea Transportation*, vol. 17, no. 2, pp. 433–443, June 2023, doi: 10.12716/1001.17.02.21.

[6] J. Skóra, "The use of unmanned aerial vehicles in the context of ensuring security in the state," *Aviation and Security Issues*, vol. 1, no. 1, Art. no. 1, July 2022, doi: 10.55676/asi.v1i1.7.

[7] W. Shin and M. Vaezi, "UAV-enabled cellular networks," in *5G and beyond: Fundamentals and standards*, X. Lin and N. Lee, Eds., Cham, Switzerland: Springer International Publishing, 2021, pp. 165–200. doi: 10.1007/978-3-030-58197-8_6.

[8] H. Jinke, F. Guoqiang, and Z. Boxin, "Research on autonomy of UAV system," in *2021 IEEE 4th International Conference on Automation, Electronics and Electrical Engineering (AUTEEE)*, Shenyang, China, Nov. 2021, pp. 745–750. doi: 10.1109/AUTEEE52864.2021.9668730.

[9] I. Al-Darraji *et al.*, "A technical framework for selection of autonomous UAV navigation technologies and sensors," *Computers, Materials & Continua*, vol. 68, no. 2, pp. 2771–2790, 2021, doi: 10.32604/cmc.2021.017236.

[10] P. R. Sriram, S. K. Ramani, R. V. Shrivatsav, M. M.Mankiandan, and N. Ayyappaa, "Autonomous drone for defence machinery maintenance and surveillance," in *2019 3rd World Conference on Smart Trends in Systems Security and Sustainablity (WorldS4)*, London, UK, July 2019, pp. 288–292. doi: 10.1109/WorldS4.2019.8904014.

[11] A. Cheranyov and E. Dukhan, "Methods of detecting small unmanned aerial vehicles," in *2021 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT)*, Yekaterinburg, Russia, May 2021, pp. 0218–0221. doi: 10.1109/USBEREIT51232.2021.9455043.

[12] S. Park, H. T. Kim, S. Lee, H. Joo, and H. Kim, "Survey on anti-drone systems: Components, designs, and challenges," *IEEE Access*, vol. 9, pp. 42635–42659, 2021, doi: 10.1109/ACCESS.2021.3065926.

[13] R. Di Pietro, G. Oligeri, and P. Tedeschi, "JAM-ME: Exploiting jamming to accomplish drone mission," in *2019 IEEE Conference on Communications and Network Security (CNS)*, Washington, DC, USA, June 2019, pp. 1–9. doi: 10.1109/CNS.2019.8802717.

[14] M. A. Jasim, H. Shakhatreh, N. Siasi, A. H. Sawalmeh, A. Aldalbahi, and A. Al-Fuqaha, "A survey on spectrum management for unmanned aerial vehicles (UAVs)," *IEEE Access*, vol. 10, pp. 11443–11499, 2022, doi: 10.1109/ACCESS.2021.3138048.

[15] D. Zmysłowski, M. Kryk, and J. M. Kelner, "Testing GNSS receiver robustness for jamming," *Aviation and Security Issues*, vol. 4, no. 2, Art. no. 2, Dec. 2023, doi: 10.55676/asi.v4i2.64.

[16] X. Liu, H. Wang, X. Yang, and J. Wang, "Quad-band circular polarized antenna for GNSS, 5G and WIFI-6E applications," *Electronics*, vol. 11, no. 7, Art. no. 7, Jan. 2022, doi: 10.3390/electronics11071133.

[17] H. Lv, F. Liu, and N. Yuan, "Drone presence detection by the drone's RF communication," *J. Phys.: Conf. Ser.*, vol. 1738, no. 1, p. 012044, Jan. 2021, doi: 10.1088/1742-6596/1738/1/012044.

[18] J.-C. Juang, C.-T. Tsai, and Y.-H. Chen, "Development of a PC-based software receiver for the reception of Beidou navigation satellite signals," *The Journal of Navigation*, vol. 66, no. 5, pp. 701–718, Sept. 2013, doi: 10.1017/S0373463313000271.

[19] N. M. Stojanović, B. M. Todorović, and V. B. Ristić, "Analysis of repeater jamming of a slow frequency hopping radio," *Vojnotehnicki glasnik/Military Technical Courier*, vol. 70, no. 3, pp. 664–679, 2022, doi: 10.5937/vojtehg70-37535.

[20] O. Šimon and T. Götthans, "A survey on the use of deep learning techniques for UAV jamming and deception," *Electronics*, vol. 11, no. 19, Art. no. 19, Jan. 2022, doi: 10.3390/electronics11193025.

[21] P. Skokowski *et al.*, "Practical trial for low-energy effective jamming on private networks with 5G-NR and NB-IoT radio interfaces," *IEEE Access*, vol. 12, pp. 51523–51535, 2024, doi: 10.1109/ACCESS.2024.3385630.

[22] Y. Bai, "Research on GNSS spatial signal interference evaluation and suppression method," PhD thesis, University of Chinese Academy of Sciences., Beijing, China, 2014.

[23] Z. Chong *et al.*, "Research on the mechanism and the impact of jamming on Beidou software receiver," in *2016 IEEE Chinese Guidance, Navigation and Control Conference (CGNCC)*, Nanjing, China, Aug. 2016, pp. 198–202. doi: 10.1109/CGNCC.2016.7828783.

[24] V. Chamola, P. Kotesh, A. Agarwal, Naren, N. Gupta, and M. Guizani, "A comprehensive review of unmanned aerial vehicle attacks and neutralization techniques," *Ad Hoc Networks*, vol. 111, p. 102324, Feb. 2021, doi: 10.1016/j.adhoc.2020.102324.

[25] H. Paik, N. N. Sastry, and I. SantiPrabha, "Effectiveness of noise jamming with white Gaussian noise and phase noise in amplitude comparison monopulse radar receivers," in *2014 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT)*, Bangalore, India, Jan. 2014, pp. 1–5. doi: 10.1109/CONECCT.2014.6740286.

[26] O. Šimon, T. Götthans, and M. Popela, "Commercial UAV jamming possibilities," in *2022 32nd International Conference Radioelektronika (RADIOELEKTRONIKA)*, Kosice, Slovakia, Apr. 2022, pp. 1–6. doi: 10.1109/RADIOELEKTRONIKA54537.2022.9764904.

[27] P. Skokowski and J. Dułowicz, "Autonomous mobile system for detecting and jamming cellular network signals using a software defined radio integrated into a UAV platform," in *2023 Signal Processing Symposium (SPSympo)*, Karpacz, Poland, Sept. 2023, pp. 149–151. doi: 10.23919/SPSympo57300.2023.10302702.

[28] A. Brito, P. Sebastião, and N. Souto, "Jamming for unauthorized UAV operations-communications link," in *2019 International Young Engineers Forum (YEF-ECE)*,

Costa da Caparica, Portugal, May 2019, pp. 94–98. doi: 10.1109/YEF-ECE.2019.8740828.
[29] K. Pärlin, M. M. Alam, and Y. Le Moullec, "Jamming of UAV remote control systems using software defined radio," in *2018 International Conference on Military Communications and Information Systems (ICMCIS)*, Warsaw, Poland, May 2018, pp. 1–6. doi: 10.1109/ICMCIS.2018.8398711.
[30] E. Horton and P. Ranganathan, "Development of a GPS spoofing apparatus to attack a DJI Matrice 100 quadcopter," *J. Glob. Position. Syst.*, vol. 16, no. 1, p. 9, July 2018, doi: 10.1186/s41445-018-0018-3.
[31] M. Haluza and J. Čechák, "Analysis and decoding of radio signals for remote control of drones," in *2016 New Trends in Signal Processing (NTSP)*, Demanovska Dolina, Slovakia, Oct. 2016, pp. 1–5. doi: 10.1109/NTSP.2016.7747781.
[32] Z. Wu, Y. Zhang, Y. Yang, C. Liang, and R. Liu, "Spoofing and anti-spoofing technologies of global navigation satellite system: A survey," *IEEE Access*, vol. 8, pp. 165444–165496, 2020, doi: 10.1109/ACCESS.2020.3022294.
[33] E. Schmidt, Z. Ruble, D. Akopian, and D. J. Pack, "Software-defined radio GNSS instrumentation for spoofing mitigation: A review and a case study," *IEEE Transactions on Instrumentation and Measurement*, vol. 68, no. 8, pp. 2768–2784, Aug. 2019, doi: 10.1109/TIM.2018.2869261.
[34] L. Huang, Z. C. Li, and F. X. Wang, "Spoofing pattern research on GNSS receivers," *Journal of Astronautics*, vol. 33, no. 7, pp. 884–890, July 2012.
[35] K. Wesson, M. Rothlisberger, and T. Humphreys, "Practical cryptographic civil GPS signal authentication," *NAVIGATION*, vol. 59, no. 3, pp. 177–193, 2012, doi: 10.1002/navi.14.
[36] S. Wang, J. Gao, Y. Wang, J. Liu, and H. Li, "GPS repeater deception jamming technology based on delay control," *Missiles Space Vehicles*, vol. 352, no. 2, pp. 103–106, 2017.
[37] J. Zidan, E. I. Adegoke, E. Kampert, S. A. Birrell, C. R. Ford, and M. D. Higgins, "GNSS vulnerabilities and existing solutions: A review of the literature," *IEEE Access*, vol. 9, pp. 153960–153976, 2021, doi: 10.1109/ACCESS.2020.2973759.
[38] Z. Gao and F. Meng, "Principle and simulation research of GPS repeater deception jamming," *Journal of Telemetry, Tracking and Command*, vol. 32, no. 6, pp. 44–47, Nov. 2011.
[39] L. Huang, H. Gong, X. Zhu, and F. Wang, "Research of re-radiating spoofing technique to GNSS timing receiver," *Journal of National University of Defense Technology*, vol. 35, no. 4, pp. 93–96, Aug. 2013.
[40] M. L. Psiaki and T. E. Humphreys, "GNSS spoofing and detection," *Proceedings of the IEEE*, vol. 104, no. 6, pp. 1258–1270, June 2016, doi: 10.1109/JPROC.2016.2526658.
[41] M. Shi, S. Chen, and Z. Liu, "Analysis and optimizing of time-delay in GPS repeater deception," *Journal of Chongqing University of Posts and Telecommunications*, vol. 29, no. 1, pp. 56–61, Feb. 2017.
[42] L. Scott, "Anti-spoofing & authenticated signal architectures for civil navigation systems," in *2003 16th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS/GNSS)*, Portland, OR, USA, Sept. 2003, pp. 1543–1552. Accessed: July 25, 2025. [Online]. Available: http://www.ion.org/publications/abstract.cfm?jp=p&articleID=5339
[43] S. F. Bian, Y. F. Hu, C. Chen, Z. M. Li, and B. Ji, "Research on GNSS repeater spoofing technique for fake position, fake time & fake velocity," in *2017 IEEE International Conference on Advanced Intelligent Mechatronics (AIM)*, Munich, Germany, July 2017, pp. 1430–1434. doi: 10.1109/AIM.2017.8014219.
[44] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, and P. M. Kintner, "Assessing the spoofing threat," *GPS World*, vol. 20, no. 1, pp. 28–39, Jan. 2009.
[45] B. S. Margana, D. S. Achanta, K. K. Songala, and S. R. Ammana, "A simple SDR based method to spoof low-end GPS aided drones for securing locations," in *2021 IEEE International Conference on Robotics, Automation, Artificial-Intelligence and Internet-of-Things (RAAICON)*, Dhaka, Bangladesh, Dec. 2021, pp. 32–36. doi: 10.1109/RAAICON54709.2021.9929965.
[46] B. Dai, M. Xiao, and S. Huang, "GPS spoofing and inducing model of UAV," *Communication Technology*, vol. 50, no. 3, pp. 496–501, Mar. 2017.
[47] S. Han, D. Luo, W. Meng, and C. Li, "Antispoofing RAIM for dual-recursion particle filter of GNSS calculation," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 52, no. 2, pp. 836–851, Apr. 2016, doi: 10.1109/TAES.2015.140297.
[48] H. Wang, Z. Yao, Z. Fan, and T. Zheng, "Experiment study of spoofing jamming on GPS receiver," *Fire Control and Command Control*, vol. 41, no. 7, pp. 184–187, July 2016.
[49] K. Ma, X. Sun, and Y. Nie, "Research on key technologies of GPS generated spoofing," *Aerospace Electronic Confrontation*, vol. 30, no. 6, pp. 24–26, 34, 2014.
[50] "DRONESHIELD DroneGun Tactical," MSS Defence. Accessed: July 25, 2025. [Online]. Available: https://mssdefence.com/product/droneshield-dronegun-tactical/
[51] "Counter Drone Technology and Anti-UAV Defence Systems," AUDS. Accessed: July 25, 2025. [Online]. Available: https://www.auds.com/
[52] "Rafael : DRONE DOME™ | Anti Drone System - Counter UAS," Rafael. Accessed: July 25, 2025. [Online]. Available: https://www.rafael.co.il/system/drone-dome-family/