Identifying and Analyzing DJI Drone Signals

Vasil Andonov
NMU "Vasil Levski"
Veliko Tarnovo, Bulgaria
vasilandonov123@gmail.com

Yordan Shterev
dept. Communication and Information systems
NMU "Vasil Levski"
Veliko Tarnovo, Bulgaria
jshterev@abv.bg

***Abstract*—The widespread use of drones in commercial, industrial, military and security applications has led to a growing need for techniques to analyse their signals. Understanding the communication signals of drones is essential for applications such as airspace monitoring, counter-unmanned aerial vehicles technologies and electronic warfare. This defines the topicality of the topic. That is why the purpose of the study focuses on the identification and analysis of DJI drone signals using software defined radio. The research aims to find their frequencies usage, look for the drone activities in spectrogram, record them and characterize modulation types of drones, specifically the DJI Air 3 and Phantom 4. The working methods are based on using HackRF One software defined radio alongside the DragonOS operating system and HackRF Spectral Analyzer, SDR++ and Inspectrum software. Signal identification is performed in controlled urban and non-urban environments, allowing for the examination of telemetry signal. Different signal processing techniques are used including spectral analysis and modulation classification are applied to identify DJI drone ID. By analysing frequency bands, bandwidth requirements, and transmission structures, the study indicates how both drones communicate and adapt to environmental factors such as interference. Main conclusions from this paper are revealing that DJI drones use frequency hopping, orthogonal frequency division multiplexing modulation adapting itself with quadrature phase shift keying, 16 and 64 quadrature amplitude modulation depending on the enviroment. They also use Zadoff-Chu sequencies for synchronizing their drone ID packets. Having in mind this, the signal width and strength also chages based on the urban or no-urban environments that the drone is.**

Keywords*—*DJI drones, HackRF One, signal analysis, software-defined radio.

I. Introduction

The rapid advancement of drone technology has significantly impacted various industries, including commercial and recreational applications, security, law enforcement, and military operations [1], [6]. Drones or *UAVs* are widely used for tasks such as aerial photography, infrastructure inspection, agricultural monitoring, and disaster response [15]. Understanding the signals used by drones is crucial for monitoring their activity, ensuring regulatory compliance, and developing counter-drone strategies, when necessary [2], [8]. This defines the topicality of the topic.

DJI is one of the leading manufacturers of consumer and professional drones [4]. They use advanced wireless communication protocols to maintain stable control links and transmit telemetry data in real time [9], [11], [16]. These transmissions include essential information such as GPS coordinates, altitude, speed, battery levels, and other flight parameters [3], [13]. Analysing these signals can provide valuable insights of drone behaviour, operational patterns, and potential vulnerabilities. However, as drone communication protocols evolve, they become more secure by using encryption and frequency-hopping techniques, which make signal interception and analysis more complex [2], [8].

In [3], [8], [16] experiments are focused more on analysing drone communication protocols and their structures. Comparing to this paper, it is shown more practically visualisation of their signals.

SDRs are powerful tools for analysing drone signals due to their ability to capture a wide range of frequencies. Devices like the *HackRF One*, combined with operating systems such as *DragonOS*, allow to identify transmission characteristics, and classify different types of drone signals based on their frequency bands, modulation schemes, and bandwidth usage [10], [14], [19].

The purpose of the study aims to discuss the methodology applied in this research for spectrum analysis, pattern recognition, and frequency monitoring, providing a systematic approach to examining drone communication signals.

II. Materials and methods

To effectively analyse *DJI drone signals*, a combination of hardware and software tools are used. The

Online ISSN 2256-070X
https://doi.org/10.17770/etr2025vol5.8486

primary hardware used in this study was the *HackRF One* on *Fig. 1*. It is a versatile *SDR* capable of transmitting and receiving signals within a wide frequency range *(1MHz to 6GHz)*. This device was selected due to its affordability, open-source nature, and compatibility with multiple *SDR* software tools. *HackRF One* provides real-time access to the electromagnetic spectrum, allowing to capture and analyse drone transmissions.

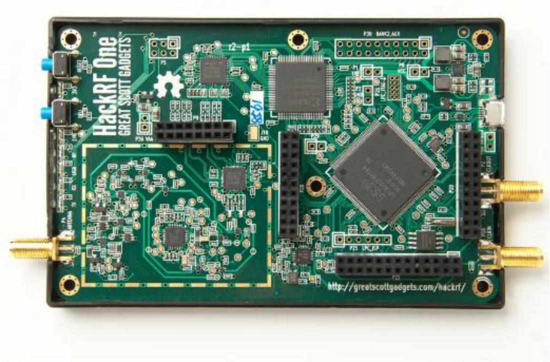


Fig. 1. HackRF One Board.

The *DragonOS* is Linux distribution. It was used as the operating environment for the *SDR-based* signal analysis. *DragonOS* is a pre-configured operating system that includes various open-source *SDR* tools. This is making it an ideal choice for researchers analysing wireless communications. It includes softwares for recording, processing and visualizing captured or live signals.

HackRF Spectrum Analyzer is a real-time spectrum monitoring software, is used to find drone activities and also to see a drone signal look like. After that a *DJI drone ID* with *SDR++ have been recorded.* Finally, with the help of *Inspectrum* software analyze the actual modulation characteristics.

A. Signal identification and visualization

DJI Air 3 and *Phantom 4* use *OcuSync* or *Lightbridge* radio protocols. OcuSync is used in *DJI drones* for transmitting video and control signals. It is part of the *Lightbridge* family and is designed to offer low-latency HD wireless video and control signals, allowing long-range transmission. OcuSync supports dual-frequency bands of *2.4 GHz* and *5.8GHz*, which gives it more flexibility in areas with interference [1], [3]. It can automatically switch between these frequencies to maintain a stable connection. It has a range of up to *4.3 miles (7 km)* and can transmit video at *1080p* resolution. On the other hand, *Lightbridge* is an older protocol with the same range but with a lower video resolution of *720p.*

Both radio protocols use *Orthogonal Frequency Division Multiplexing (OFDM)* modulation. This is a transmission technique that divides a data stream into multiple smaller subchannels, as you can see on *Fig. 2*, each carrying part of the information across closely spaced frequencies, rather than using a single wideband channel [9]. Unlike traditional single-channel modulation, where data bits are transmitted sequentially, *OFDM* allows multiple bits to be sent simultaneously across parallel subchannels. This reduces the required data rate per subchannel, making the system more resistant to interference and improving spectral efficiency [1]. While primarily used in wireless communication, *OFDM* is also applied in wired and fiber optic networks for reliable high-speed data transmission.

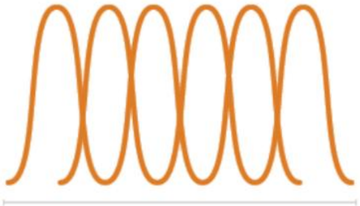


Fig. 2. OFDM subchannels overlapping.

Lightbridge is used in older *DJI* models like the *Phantom 4*, leverages *OFDM* to maintain stable video and telemetry transmission over extended distances. *OcuSync* is an evolution of *Lightbridge*, further optimizes *OFDM* by incorporating adaptive frequency hopping, improved error correction, and dynamic bandwidth allocation, allowing it to switch between *2.4GHz* and *5.8GHz* for better interference avoidance [3]. These enhancements make *OcuSync* more robust in complex *RF* environments, providing lower latency, higher data rates, and increased range compared to traditional single-carrier transmission methods.

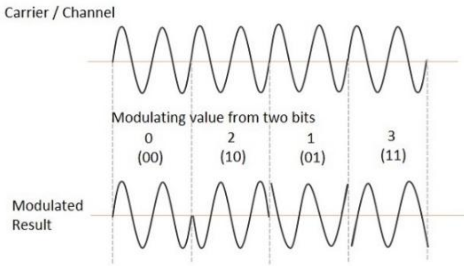


Fig. 3. QPSK waveform.

In the other hand, based on signal quality within *OFDM*, subcarriers use different modulation schemes. They are *Quadrature phase-shift keying (QPSK), 16 and 64 Quadrature amplitude modulation (QAM)*. *QPSK* is a modulation technique that allows the transmission of multiple bits simultaneously by representing possible states with different analog levels and phases *(Fig. 3)* [10]. It improves spectral efficiency by transmitting two bits using the same spectrum width as *Binary Phase Shift Keying (BPSK)*, with the *I (in phase)* and *Q (quadrature)* channels modulated onto carriers *90°* apart [7]. Both drones, *DJI Air 3* that uses *OcuSync 4.0* and *DJI Phantom 4* working with *Lightbridge* rely on *QPSK* to establish stable, long-range, and interference-resistant links between drones and controllers.

In *16-QAM*, each symbol is represented by *4 bits* of data, allowing for *16 different states*, while in *64-QAM*, each symbol is represented by *6 bits* of data, allowing for *64 different states - Fig. 4* [12]. The main difference between *16-QAM* and *64-QAM* lies in the number of bits per symbol and the number of states they can represent. *16-QAM* has *16* possible states, whereas *64-QAM* has *64* possible states [5]. This means that *64-QAM* can transmit more data per symbol than *16-QAM*, but it is also more susceptible to noise and interference, making it less robust in low *Signal-to-Noise Ratio (SNR)* conditions [18].

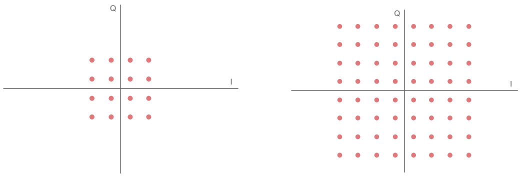


Fig. 4. 16 and 64 QAM constellation.

By combining *OFDM's* multi-carrier transmission with adaptive modulation, *DJI's Lightbridge* and *OcuSync* achieve low-latency, high-quality video streaming and robust control links. In strong signal conditions, *64-QAM* maximizes data throughput, while in weaker or noisier environments, the system can downgrade to *QPSK* to maintain a stable connection.

B. Recording a DJI drone ID

DJI drone ID is the identification system used by *DJI* drones to provide information about the drone and its operator [13]. This system is designed to comply with the Remote ID requirements set by the *Federal Aviation Administration (FAA)* and other regulatory people around the world. Remote ID allows drones to transmit identification and location data to other parties, enhancing safety and security in the airspace [1], [4]. *DJI* drones can use various methods to transmit this information, including Wi-Fi, Bluetooth, or cellular networks, depending on the model and the specific Remote ID requirements in their operating region. Center frequencies depend on the band that is used [3]. In *table 1* there are shown *2.4GHz* and *5.8GHz* bands.

SDR++ is an open-source, cross-platform *SDR* receiver application. It provides a powerful and flexible interface for tuning, demodulating, and analyzing radio signals from various SDR devices, including *HackRF One*. Using this software, *drone ID* can be recorded by selecting one of the center frequencies listed above. The recording file format needs to be *float32*. It is a *32-bit* floating-point format used in computer memory to represent a wide dynamic range of numeric values by using a floating radix point [17]. *Float32* is preferred due to its higher precision and dynamic range. This is crucial for capturing weak or noisy signals. *Float32* minimizes quantization errors, preserving fine details essential for accurate demodulation, especially for signals using *OFDM* or frequency hopping.

SDR++ is an open-source, cross-platform *SDR* receiver application. It provides a powerful and flexible interface for tuning, demodulating, and analyzing radio signals from various SDR devices, including *HackRF One*. Using this software, *drone ID* can be recorded by selecting one of the center frequencies listed above. The recording file format needs to be *float32*. It is a *32-bit* floating-point format used in computer memory to represent a wide dynamic range of numeric values by using a floating radix point [17]. *Float32* is preferred due to its higher precision and dynamic range. This is crucial for capturing weak or noisy signals. *Float32* minimizes quantization errors, preserving fine details essential for accurate demodulation, especially for signals using *OFDM* or frequency hopping.

TABLE 1 DJI DRONE ID CENTRE FREQUENCIES

Frequency Bands	
2.4GHz	**5.8GHz**
2399.5MHz	5741.5MHz
2414.5MHz	5756.5MHz
2429.5MHz	5771.5MHz
2444.5MHz	5786.5MHz
2459.5MHz	5801.5MHz
	5816.5MHz

C. Analyzing DJI drone ID packet

One of the main characteristics of a *drone ID* is the *Zadoff-Chu (ZC) sequence*. It is a special mathematical sequence used in transmissions for synchronization and signal detection. It has key properties like constant amplitude and zero cross-correlation, making it highly effective for timing alignment and interference resistance in wireless communication [19]. In *DJI* drones, the *ZC sequence* helps receivers accurately detect and decode *Drone ID* signals, even in environments with *RF* noise and interference [11], [13].

The *ZC sequence* enhances signal accuracy by reducing timing errors and improving synchronization. It minimizes interference and distortion, ensuring clear and reliable transmission [19]. Each *Drone ID* transmission consists of nine *OFDM* symbols, with the *ZC sequence* embedded in symbols *4* and *6* [3], [16]. These special symbols act as reference points, allowing the receiver to synchronize with the transmission. The remaining symbols contain identification and telemetry data, such as the drone's serial number, GPS position, and flight status.

III. RESULTS AND DISCUSSION

On *Fig. 5* is the experimental setup. There are both drones, on the left is *DJI Air 3* with the controller and on the right is *DJI Phantom 4* again with his controller. *HackRF One* works with a tri-band antenna, and it is connected to a laptop with *DragonOS* operating system.

A. Identifying drone signals

Based on the methodology, first experiment is identifying a drone signal in urban and non-urban environment. It is used a tri-band *(GSM, 4G and 5G)* antenna with frequency range from *600MHz* to *6GHz* connected to *HackRF One* working with *HackRF Spectre*

Analyzer software on *DragonOS*. At the beginning on *Fig. 6* and *Fig. 7* are the spectrograms in urban and non-urban environment with the *DJI Air 3* powered off. The frequency range is set to be *2300MHz–2600MHz* to have clear view of *2.4GHz* band.

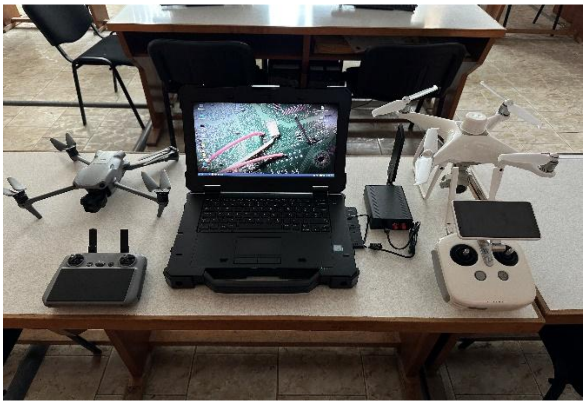


Fig. 5. Experimental setup softwares and hardwares.

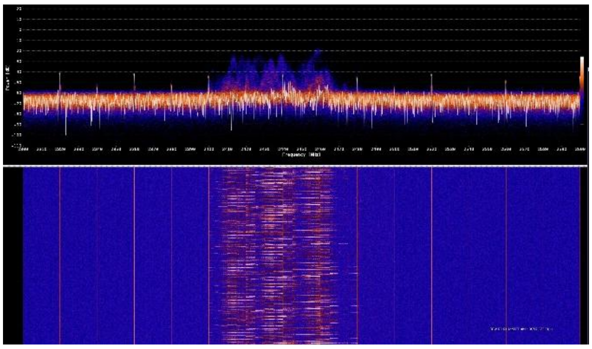


Fig. 6. The Spectrogram in urban environment with drone powered off. Power levels from -75dB to -50dB with PSD frequency range from 2405MHz to 2465MHz.

On *Fig. 6* the spectrogram has only short bursts that indicate the usage of *Wi-Fi*, *Bluetooth* and smart home devices. This is because the experiment is in an urban environment. After that on *Fig.7* is the same test but in non-urban environment. The differences are quite big. The spectrogram is much clearer because of there are fewer *Wi-Fi* routers, cellular towers, or other strong *RF* emitters in the *2.4GHz industrial, scientific and medical (ISM)* band. The few narrowband spikes are from distant sources, background noise, or minor reflections.

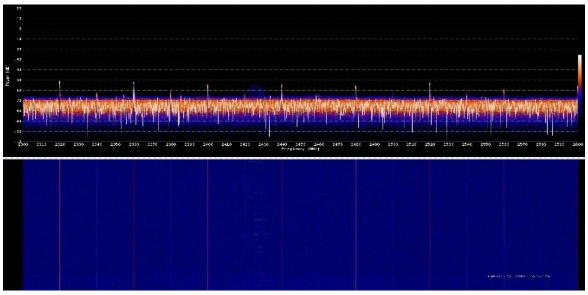


Fig. 7. The spectrogram in non-urban environment with drone powered off. Power levels from -100dB to -70dB with no frequency usage.

Then on *Fig. 8* and *Fig. 9* are the spectrograms with the drone powered on. The *RF* spectrum changed significantly due to the introduction of multiple wireless transmissions. Before the drone is powered on, the baseline spectrogram primarily shows background *RF* noise and interference from nearby *Wi-Fi*, *Bluetooth*, and other *ISM-band* devices. The signal power levels remain relatively low between -*100dB* and -*50dB*.

However, when the drone is powered on, it immediately begins broadcasting signals, which results in a higher *power spectral density (PSD)* in frequency range from *2360MHz* to *2500MHz* in urban environment *(Fig. 8)* and in non-urban environment from *2435MHz* to *2470MHz (Fig. 9)* with power levels reaching *-18dB*.

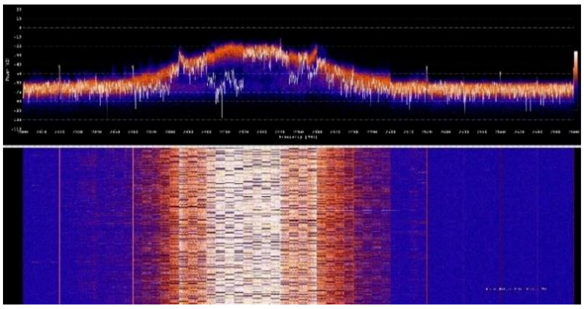


Fig. 8. The spectrogram in urban environment with DJI Air 3 powered on. Power levels from -70dB to -18dB with PSD frequency range from 2360MHz to 2500MHz.

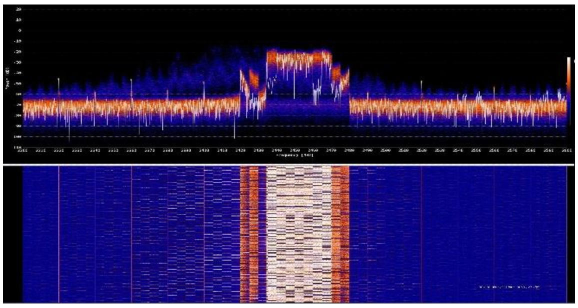


Fig. 9. The spectrogram in non-urban environment with DJI Air 3 powered on. Power levels from -75dB to -20dB and PSD frequency range from 2435MHz to 2470MHz.

The spectrum analyzer also displays wide, consistent, repeating signal bursts, suggesting for frequency hopping methods in *OFDM* modulation. The drone adapts by dynamically adjusting its power levels and switching channels frequently in an attempt to maintain a stable connection. The hopping behavior is more structured and predictable in non-urban environments as can be seen on *Fig. 9* but becomes more irregular and adaptive in urban environments where interference levels are higher, *Fig. 8*.

Comparing the *DJI Phantom 4* signals to the *Air 3* ones the differences are visually big - *Fig.10*. Phantom *4's* signal appears more structured and concentrated within a specific range from *2415MHz* to *2425MHz*. This is because this drone uses the Lightbridge radio protocol which is not so adaptive as OcuSync used in DJI Air 3. It has strong, periodic peaks in the waterfall display, meaning it follows a fixed frequency hopping pattern rather than dynamically adjusting its transmission as *Air 3* on *Fig. 8*.

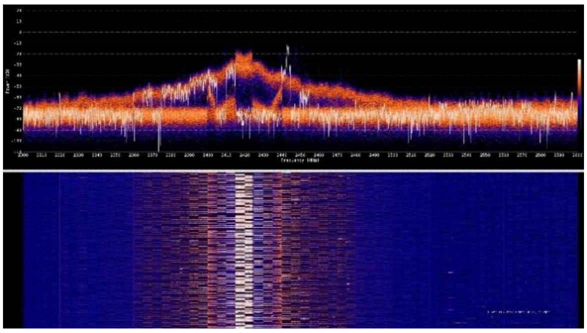


Fig. 10. The spectrogram in urban environment with DJI Phantom 4 powered on. Power levels from -90dB to -18dB with PSD frequency range from 2400MHz to 2440MHz.

Overall, the *Phantom 4* uses an effective but less adaptive communication system compared to the *Air 3*, which employs a wider and more interference-resistant transmission method. The *Air 3's* spectrum characteristics make it better suited for urban conditions with high *RF* congestion, while the *Phantom 4* may function more reliably in less crowded *RF* environments, where fixed frequency hopping patterns are less likely to be disrupted by external interference sources.

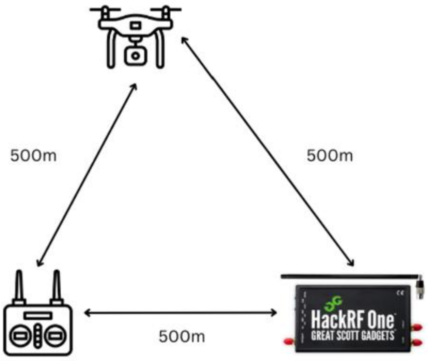


Fig. 11. Real-life scenario of detecting a drone.

The next experiment is a more real-life scenario of detecting a drone signal in big distances. On *Fig. 11* is an illustration of the experimental setup. The drone controller is *500m* from *HackRF One*. The drone is *500m* hight and *500m* from *HackRF* too.

The spectrogram on *Fig. 12* shows the usage of a drone around. The *PSD* is from *2435MHz* to *2470MHz,* and the power levels are reaching *-50dB*. The signals are not so strong but because there are repeating signal bursts and frequency hopping can say that these are drone signals. By this experiment it can be said that *HackRF* can be used also as a drone detector on a not so small distance in real-life implementations.

B. Recording a DJI drone ID packet

The next experiment is recording a drone ID using again *HackRF One*, *the tri-band antenna* and *SDR++* software on *DragonOS*.

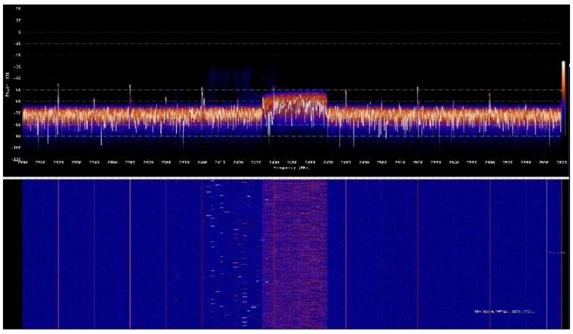


Fig. 12. The spectrogram of the real-life scenario experiment. Power levels from -80dB to -55dB with PSD frequency range from 2435MHz to 2470MHz.

Having in mind the center frequencies of *drone ID* in *table 1* one of them is set and make a *float32* record. In the example it is used *2444.5Mhz - Fig. 13* and the duration of the recording is *10 seconds*. *DJI drone ID* is transmitted *10 times per second* and the adaptation of frequency that is used on because of frequency hopping adjustments. That is why a *10sec.* recording is enough for the experiment.

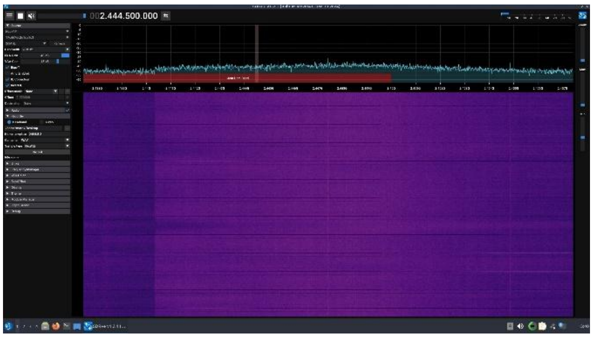


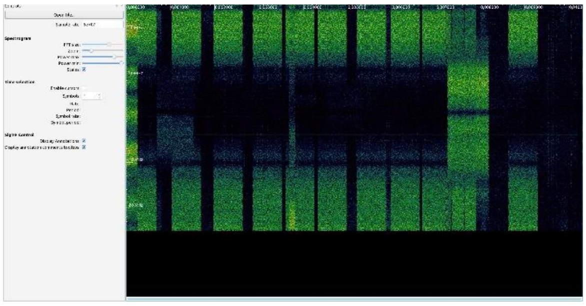
Fig. 13. SDR++ recording a DJI drone ID on 2444.5MHz center frequency.

This can be done with every of the frequency shown in *table 1*. Transition of *drone ID* depends on the environment that you are in. In non-urban environments, *ID* transmission remains stable with minimal interference but in urban environments, signal congestion and multipath effects can cause packet loss or frequency hopping adjustments, leading to slight variations in transmission timing and frequency usage.

It has been observed that even when a user manually sets the *DJI OcuSync* downlink to operate strictly within the *2.4GHz* or *5.8GHz* range, the *DJI drone ID* signal does not conform to these settings and continues transmitting on the frequencies in *table 1* [3].

A. Analyzing a DJI drone ID

Finally, when the recording of center frequencies listed in *table 1* is made, open it in *Inspectrum* on *DragonOS* to analyze the specter deeply. In our example the recording of 2.444.5MHz frequency is used.



Controls

Open file...

Sample rate: 5e+07

Spectrogram

FFT size:

Zoom:

Power max:

Power min:

Scales: ☒

Time selection

Enable cursors: □

Symbols:

Rate:

Period:

Symbol rate:

Symbol period:

Signal control

Display Annotations ☒

Display annotation comments tooltips ☒

Fig. 14. Analysis of drone IDs on Inspectrum software.

The spectrogram on *Fig. 14* captures *RF* signals over time and shows their frequency characteristics. The sample rate of *5e+07 (or 50 MHz)* is used to capture signals at a high enough resolution to analyze the details of *RF* transmissions. The frequency range spans from *0MHz* to *20MHz*, as indicated by the *Y-axis*, with signal bursts appearing throughout this range. These bursts, separated by quiet periods, are characteristic of the *Drone-ID RF* frame structure. This pattern is consistent with the expected behavior of a communication system used for *Remote ID*, where data packets are transmitted in structured bursts at regular intervals.

The time window captured by the spectrogram spans about *10 milliseconds*. Each vertical group of lines in the spectrogram corresponds to one of these signal bursts, suggesting that each burst represents a packet of data being transmitted at specific intervals. Each frame's bandwidth range from *9.38MHz* to *10.91MHz*. In the spectrogram, the signal shifting slightly across the frequency domain, which corresponds to the *CFO* variations in the packet analysis. These shifts are visible as slight changes in the positioning of the bursts on the frequency axis. The regular pattern of bursts observed also in the spectrogram in *Fig. 14* suggests the usage of *Zadoff-Chu (ZC)* sequences. These bursts occur at precise intervals, which is typical of systems using *ZC sequences* to maintain synchronization.

IV. Conclusion

The methodology applied in this research integrates spectrum analysis, pattern recognition, and frequency monitoring, providing a systematic approach to examining drone communication signals. By SDR technology like HackRF One with tools such as HackRF Spectrum Analyzer, SDR++ and Inspectrum, it was capture, visualize, and analyze the behaviour of DJI Air 3 and Phantom 4 signals across urban and non-urban environments. Also, it is demonstrated capabilities of the methodology that reach up to 500m drone signal detection. Theoretically, the ability to study drone signals at the raw RF level allows for a detailed examination of frequency utilization, modulation schemes, bandwidth variations, and transmission stability.

Spectrum analysis plays a critical role in identifying occupied frequency bands, signal strength variations, and interference levels. By monitoring the 2.4GHz band, it is determined which frequencies are used for telemetry data, as it shown in table 1. The application of spectrogram visualization enables researchers to track signal evolution over time, revealing patterns such as frequency hopping, channel allocation, and power adjustments in response to environmental conditions.

Pattern recognition techniques help distinguish recurring structures in drone transmissions, allowing to differentiate between control commands, telemetry bursts, and video signals. It is discovered that each DJI Remote ID bandwidth ranges from 9.38MHz to 10.91MHz with precise intervals, which is typical of systems using ZC sequences to maintain synchronization. The identification of repeated frequency hopping intervals and unique transmission signatures provides deeper insight into how DJI drones maintain stable communication links

Practically, findings of this study significantly contribute to counter-drone measures, regulatory enforcement, and spectrum management. Understanding the characteristics of UAV communications enables researchers, security professionals, and regulatory agencies to develop effective detection and mitigation strategies. For instance, identifying distinct frequency hopping patterns and modulation schemes allows the creation of automated drone detection systems, which can track UAV activity based on its unique RF footprint. Future research could focus on analysing 5.8GHz signal characteristics, evaluating long-range signal propagation, and investigating encryption methods within DJI transmissions. Expanding these studies will further enhance ability to detect, monitor, and regulate drone activity in both civilian and military applications.

Acknowledgments:

This report is supported by the National Scientific Program "Security and Defence", approved by Decision No. 171/21.10.2021 of the Council of Ministers of the Republic of Bulgaria.

References

[1] D. Aouladhadj, E. Kpre, V. Deniau, A. Kharchouf, C. Gransart, C. Gaquière, "Drone Detection and Tracking Using RF Identification Signals", Sensors, 2023, 23, 7650. https://doi.org/10.3390/s23177650.

[2] A. Bello, Radio Frequency Toolbox for Drone Detection and Classification. Master of Science (MS), Thesis, Electrical & Computer Engineering, Old Dominion University, 2019. DOI: 10.25777/9gkmjd54. Available: https://digitalcommons.odu.edu/ece_etds/160. [Accessed Feb. 23, 2025].

[3] C. Bender, DJI Drone IDs Are Not Encrypted. *arXiv*, 2022. https://doi.org/10.48550/arXiv.2207.10795.

[4] D. Clark, C. Meffert, I. Baggili, F. Breitinger, DROP (DRone Open Source Parser) Your Drone: Forensic Analysis of the DJI Phantom III. *Digital Investigation* 2017, 22, S3-S14. https://doi.org/10.1016/j.diin.2017.06.013.

[5] Constellation Diagram. *Wikipedia*. Available: https://en.wikipedia.org/wiki/Constellation_diagram. [Accessed Feb. 23, 2025].

[6] DJI Drone Operators' Location Intercepted. *DroneXL*, 2 March 2023. Available: https://dronexl.co/2023/03/02/dji-drone-operators-location-intercepted/. [Accessed Feb. 23, 2025].

[7] Digital Communication: Quadrature Phase Shift Keying. TutorialsPoint. Available: https://www.tutorialspoint.com/digital_communication/digital_communication_quadrature_phase_shift_keying.htm. [Accessed Feb. 23, 2025].

[8] Master Thesis on DJI Protocol Reverse Engineering. Digidow, Available: https://www.digidow.eu/publications/2021-christof-masterthesis/Christof_2021_MasterThesis_DJIProtocolReverseEngineering.pdf. [Accessed Feb. 23, 2025].

[9] Orthogonal Frequency Division Multiplexing. TechTarget. Available: https://www.techtarget.com/searchnetworking/definition/orthogonal-frequency-division-multiplexing. [Accessed Feb. 23, 2025].

[10] Phase Shift Keying: Implementation. Wikipedia. Available: https://en.wikipedia.org/wiki/Phase-shift_keying#Implementation_2. [Accessed Feb. 23, 2025].

[11] Phase Shifting Techniques in Communication. *arXiv*, 2022. Available: https://arxiv.org/abs/2211.05702. [Accessed Feb. 23, 2025].

[12] Quadrature Amplitude Modulation. Wikipedia. Available: https://en.wikipedia.org/wiki/Quadrature_amplitude_modulation. [Accessed Feb. 23, 2025].

[13] Research Square: RF Toolbox for Drone Detection. Available: https://assets-eu.researchsquare.com/files/rs-5827543/v1_covered_58ee4e7b-b0e4-4d34-b0d9-4d5fbac723d7.pdf. [Accessed Feb. 23, 2025].

[14] RTL-SDR: Drones. Available: https://www.rtl-sdr.com/tag/drone/. [Accessed Feb. 23, 2025].

[15] S. Kreps, Drones: What Everyone Needs to Know, ISBN 978–0–19–023535–2, Oxford University Press 2016.

[16] N.Schiller, M. Chlosta, M. Schloegel, N.Bars, T. Eisenhofer, T. Scharnowski, L. Schönherr, T. Holz, Drone Security and the Mysterious Case of DJI's DroneID. ISBN 1-891562-83-5, 3 March 2023. Available: https://dx.doi.org/10.14722/ndss.2023.24217.

[17] Single-Precision Floating-Point Format. *Wikipedia*. Available: https://en.wikipedia.org/wiki/Single-precision_floating-point_format. [Accessed Feb. 23, 2025].

[18] Types of Quadrature Amplitude Modulation. Electronics *Notes*. Available: https://www.electronics-notes.com/articles/radio/modulation/quadrature-amplitude-modulation-types-8qam-16qam-32qam-64qam-128qam-256qam.php. [Accessed Feb. 23, 2025].

[19] Zadoff–Chu Sequence. Wikipedia. Available: https://en.wikipedia.org/wiki/Zadoff%E2%80%93Chu_sequence#cite_note-Zepernick-1. [Accessed Feb. 23, 2025].