Journal of Physics: Conference Series

PAPER • OPEN ACCESS

Drone Presence Detection by the Drone's RF Communication

To cite this article: Huan Lv *et al* 2021 *J. Phys.: Conf. Ser.* **1738** 012044

Drone Presence Detection by the Drone's RF Communication

Huan Lv[1*], Fang Liu[1] and NaiChang Yuan[1]

[1]School of Electronic Science and Engineering, National University of Defense Technology, Changsha, Hunan, 410073, China

[*]Corresponding author's e-mail: 68107745@qq.com

Abstract. Unmanned aerial vehicles (UAVs), also known as drones, are expected to play an essential role in future life. However, if drone technology is misused, it will bring unpredictable harm. For example, the use of drones to engage in illegal, criminal, and terrorist activities has brought new challenges to confidentiality, security, and counter-terrorism. The demand for anti-drone systems from all walks of life is rising. These systems can detect and prevent the activities of illegal drones, so that the technology of drones can be used well. This article introduces the current mainstream methods of UAV detection, and then uses the radio frequency (RF) control and map transmission signal exchanged between the drone and its remote controller to achieve a way of passive radio detection of drones.

1. Introduction

The use of civilian drones has increased dramatically in recent years due to lower costs. Similarly, drones are rapidly gaining popularity around the world. However, the way drones are being used has raised public concerns. For example, on July 9, 2020, in Shexian County, Anhui Province, two drones broke into the examination room; on June 17, 2020, there were people flying drones within the scope of Hangzhou Xiaoshan International Airport, which caused dozens of planes to fail; in January 2015, the invasion of the White House by a DJI drone caused a huge sensation; drones are accused of invading privacy and even engaging in illegal and criminal activities. These incidents provide numerous examples of the critical importance of developing surveillance systems for suspected drones.

The article is organized as follows. Section II introduces several mainstream UAV detection methods. Section III describes the signal characteristics of the drone and demonstrates the separation of a remote control signal and map transmission signal by morphological filtering. Section IV presents the detection principle of drone map transmission signal. Section V introduces a detection method of drone remote control signals. Section VI ends this article.

2. Related Works

As the equipment characteristics of different types of UAVs vary greatly, and there are many interferences in the environment, the reliable detection of UAVs is a challenging task. The literature provides many different methods of drone detection [1]. At present, researchers mainly detect UAVs from visual detection, acoustic detection, radar detection, and radio frequency (RF) passive detection.

2.1. Computer Vision

The computer vision detection method uses a dedicated camera and computer to replace the human eye to identify and track the target, and further performs graphic processing to make the computer processing an image more suitable for human eye observation or transmission to the instrument for detection[2].

Drone detection and tracking based on computer vision have significant advantages [3], including:

1. Capable of detecting drones without RF transmission
2. Use passive and inexpensive optical sensors
3. Excellent inherent directional accuracy

The main disadvantage of optical sensors is that they do not work well in bad weather conditions, and they are not applicable at night. They also cannot operate under NLOS conditions, such as in an urban environment. In addition, in practical applications, it is difficult to strictly distinguish drones from flying birds, balloons, etc., and it is easily blocked by obstacles in the environment. In order to detect at night, some scholars have developed infrared sensing technology through thermal imaging cameras [4]. The heat emitted by the drone is used for detection by analyzing thermal images. However, this method is difficult to effectively detect such small targets as drones, mainly because drones do not generate a lot of heat, and the heat radiation characteristics are not obvious, and they are greatly affected by the thermal radiation of the environment.

2.2. Acoustic Detection
Audio detection is mainly to collect the sound signal from the rotor or engine of the drone through the sound sensor, and extract the sound characteristic parameters for identification and detection. Audio detection has the advantages of detection and positioning. This method has advantages when the detected signal within the detection range has sufficient clarity, and the acoustic array can achieve high-precision drone sound source positioning at close range.

Several research groups [5][6] used acoustic sensors to detect drones, and have demonstrated the ability to detect small drones within a range of 20 meters [5] to 600 meters [6], with a detection probability of 99.5%, the false alarm rate is 3%.

However, it has two main shortcomings. One is the small detection range (<600 meters), and the other is that it cannot recognize the drone's sound in the presence of noise.

2.3. Active Radio Frequency Method (Radar)
Radar detection measures the speed, azimuth, etc. of the drone by emitting electromagnetic waves and using the echoes reflected by the drone. Meanwhile, the doppler frequency shift effect can also be used to estimate the drone's flight speed [8]. The detection range of the radar is about 3000 meters [9], which has the advantages of positioning and tracking, but requires the drone to be larger and move faster so that the radar echo is more obvious, and it is suitable for areas with relatively open environments. However, small consumer drones have the characteristics of low flying height, small size, and slow speed. Its flight concealment is high, and the effective reflection area of radar electromagnetic wave signals is very small [7], and complex electromagnetic environment in the urban environment, so radar detection is not a very effective means. At the same time, the accuracy of radar positioning and tracking is greatly reduced when the distance is relatively close, which affects its actual performance.

2.4. RF (passive)
The Radio Frequency (RF) based detection methods mainly use the communication or map transmission signal between the drone and the ground controller to detect the drone. Drone communication protocols usually use the same frequency bands used for WiFi transmissions, particularly in the 2.400–2.483 GHz and 5.725–5.825 GHz. A drone equipped with a camera usually transmits a video stream to its control unit through the same wireless channel.

A simple method is to monitor a wide range of RF signals, such as 1 MHz to 6.8 GHz in [12], and treat any transmitter of unknown RF signals as a drone. Since the unknown RF transmitter is not necessarily a drone, this method will lead to a high probability of false alarms. RF detection is detected by remote control signals or map transmission signals, but when the drone uses GPS navigation to fly autonomously, this method will fail.

Compared with active methods, passive detection has lower costs in terms of hardware and software requirements, operation and maintenance, portability and ease of deployment, and flexibility to interception. Therefore, this article focuses on the passive method, in which the drone sends a signal, and then we detect and recognize it.

3. Radio frequency passive surveillance drones

In the case that the drone sends radio frequency signals, the drone can be monitored by eavesdropping on the communication between the drone and the ground controller. Technically speaking, this method can detect the drone and estimate its angle of arrival by processing the data sent by the drone to the controller through the wireless receiver. Since most commercial drones often communicate with the controller to update status and receive commands, there is a data link between the drone and the controller. Therefore, the RF receiver can collect wireless data samples, analyze them, and detect the presence of drones.

3.1. Drone communication signal introduction

The major commercial drones in the market include DJI spirit, Mavic, and Xiaomi drones. To increase anti-interference capability, frequency-hopping communication systems are used. By controlling the variation of the carrier frequency, communication signals can hop across different channels over time to achieve normal communication in complex electromagnetic environments. The frequency band used for drone communication signals must meet the requirements of the radio frequency band management of the country where the drones are located.

Drones communication signals include remote control signals, navigation satellite signals, and map transmission signals used by some aircraft types. The remote control sends the upline control data to the drone host, and the host sends the map transmission signal to the remote control end.

For control signals, the remote controller is only responsible for sending data, and the host drone is only responsible for receiving data. There is no RF interaction between the two. In order to increase the stability of transmission, the mainstream of drone remote control signal using ISM frequency range of frequency hopping communication signals, in the process of drone flight, drone flight instruction sent by the remote control of frequency hopping signal control. Once out of control, the drone will execute the slow landing or return command according to the pre-set instructions. Figure 1 is a schematic diagram of the drone's communication signal and transmission direction.

Figure 1. Communication signal of UAV

An example of a drone signal is shown in the time-frequency diagram in Figure 2. The drone signal of interest is composed of 2MHz narrowband frequency-hopping remote control signal and 10MHz large-bandwidth video stream signal, as shown in Figure 2. Literature [13] uses morphological filtering scheme to process the power spectral density, and the remote control signal (Figure 2b) and the video stream signal (Figure 2c) were separated with proper length structural elements.

In this paper, multi-hop autocorrelation and power spectrum cancellation are used to detect drone signals.

Journal of Physics: Conference Series **1738** (2021) 012044 doi:10.1088/1742-6596/1738/1/012044

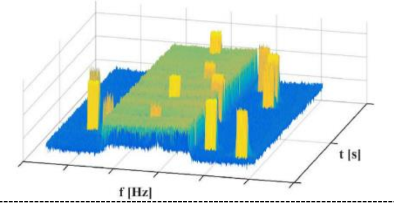

Figure 2(a). Drone signals composed of remote control and map transmission data

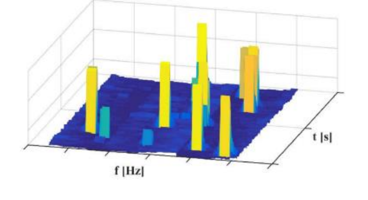

Figure 2(b). Extracted remote control signal

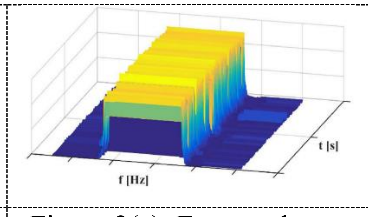

Figure 2(c). Extracted map transmission signal

3.2. RF signal characteristics of commercial drone

UAV signals are divided into remote control signals and image transmission signals. UAV remote control signals belong to a typical frequency hopping communication system, and the image transmission signals are fixed frequency signals. We tested the uplink remote control signal and downlink image transmission signal on the typical commercial drone platform-DJI Phantom 4.

In the time domain, the signal period of the UAV is about 14ms. The remote control signal and the image transmission signal alternately appear. First, the UAV uplink remote control signal is generated. This signal is a frequency hopping signal, and the dwell time of each hop signal is about 2.17ms, after the frequency hopping signal, a 9.75ms downlink image transmission signal will be generated. This signal belongs to a fixed frequency signal, and alternately forms the UAV communication system.

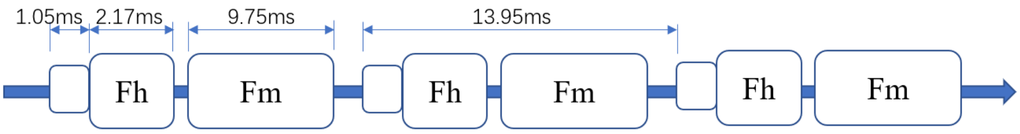

Figure 3.Drone signal timing obtained from the test

In the frequency domain, the test found that the UAV remote control signal has a total of 34 frequency points, ranging from 2404MHz to 2470MHz, with an interval of 2MHz between each hop frequency, and the signal bandwidth per hop is about 1.5MHz.

4. Detect map transmission signal

The map transmission system of the drone usually sends radio signals with a frequency of 2.4GHz or 5.8GHz to transmit the image information back to the ground control end. 2.4GHz and 5.8GHz are ISM band. ISM band is very crowded, and there are a lot of communication signals, so the electromagnetic environment is quite complex. Table 1 shows the frequency band and bandwidth characteristics of drone remote control signal, map transmission signal, and common WiFi signal [14]. It can be seen from Table 1 that the drone map transmission signal has a significant feature, with a bandwidth of about 9MHz. Therefore, the drone map transmission signal can be detected and identified through the bandwidth characteristics of the signal.

Table 1. Signal type of ISM frequency band

Signal Type	Frequency band	Bandwidth
Map transmission signal	2.404GHz~2.47GHz 5.725GHz~5.775GHz	9MHz
Remote signal	2.404GHz~2.47GHz	2MHz
WiFi signal	2.40GHz-2.483GHz 5.15GHz-5.85GHz	20MHz

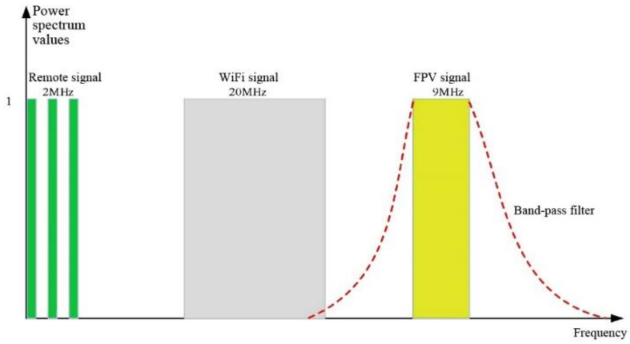

Figure 4. Map transmission signal recognition principle

4.1. Detect remote control signal

The remote control signal of drone belongs to frequency-hopping signal. There are many detection methods about the frequency-hopping signal at home and abroad. The current research focuses on two aspects: hardware detection based on front-end receiver and detection method based on back-end signal processing. The detection method based on back-end signal processing is of great effect and low false alarm probability, which mainly includes the detection method based on power spectrum cancellation, autocorrelation detection and remote control signal extraction method based on spectrum. This section demonstrates a blind detection method for drone remote control signals based on multi-hop autocorrelation and power spectrum estimation.

Suppose the received signal from the antenna is

$$x(t) = s_h(t) + n(t) \tag{1}$$

Among them, $s_h(t)$ represents the UAV remote control signal, $n(t)$ is the bandpass Gaussian white noise with the mean value of 0 and the unilateral power spectral density of $N_0/2$. Then the autocorrelation function of $x(t)$ is

$$R(\tau) = \int_0^T x(t)x(t-\tau)dt = R_{ss}(\tau) + R_{sn}(\tau) + R_{nn}(\tau) \tag{2}$$

Among them, $R_{ss}(\tau)$ is the autocorrelation function of the remote control signal, $R_{sn}(\tau)$ is the cross-correlation function of the remote control signal and noise, $R_{nn}(\tau)$ is the autocorrelation function of noise, and T is the time of receiving data, including multiple frequency hopping periods T_h. When the signal-to-noise ratio is small, the cross-correlation function of the signal to be detected and the noise signal can be ignored and is close to 0; or the signal is not correlated with the Gaussian white noise signal, and the cross-correlation function is also close to 0, so the above formula is simplified for

$$R(\tau) = R_{ss}(\tau) + R_{nn}(\tau) \tag{3}$$

Assuming that the received data contains signals with N hops, different hop signals are uncorrelated, that is, the cross-correlation function is 0, while ignoring the impact of not a complete frequency hopping period data included in the received data, we can get:

$$R_{ss}(\tau) = \sum_{j=1}^{N} R_{sjsj}(\tau),\ j \text{ is an integer} \tag{4}$$

The signal of the jth hop can be expressed as

$$s_j(t) = A\cos(2\pi f_j t + \varphi_j) \tag{5}$$

Then finally can be expressed as

$$\begin{aligned} R_{sjsj}(\tau) &= \frac{1}{T_h}\{\int_0^{T_j-\tau} A^2\cos(2\pi f_j t+\varphi_j)\cos[2\pi f_{j+1}(t+\tau)+\varphi_{j+1})dt \\ &+\int_{T_j-\tau}^{T_j} A^2\cos(2\pi f_j t+\varphi_j)\cos[2\pi f_{j+1}(t+\tau)+\varphi_{j+1})dt\} \\ &= \frac{A^2}{2}\cos(2\pi f_j\tau)\frac{T_h-\tau}{T_h},\tau\le T_h \end{aligned} \quad (6)$$

When the received signal contains a frequency hopping signal, the autocorrelation function is expressed as

$$R_x(\tau)=\begin{cases} \frac{A^2}{2}\cos(2\pi f_j\tau)\frac{T_h-\tau}{T_h}+R_{nn}(\tau), 0<\tau\le T_h \\ R_{nn}(\tau), T_h<\tau<T \end{cases} \quad (7)$$

When there is no frequency hopping signal in the received signal, the autocorrelation function is expressed as

$$R_x(\tau)=R_{nn}(\tau) \quad (8)$$

Therefore, when the time delay of the autocorrelation function of the received signal is different in $0<\tau\le T_h$ and $T_h<\tau<T$, the different function values can be used to determine the presence or absence of the frequency hopping signal.

Experimental results of measured UAV remote control signal data:

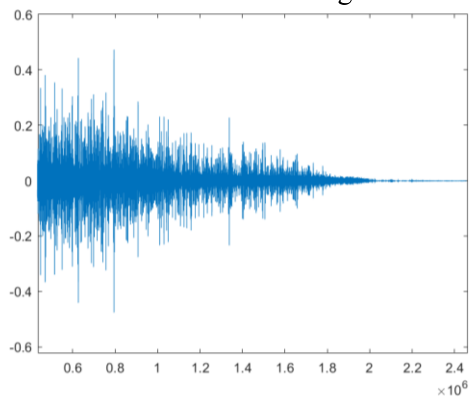

Figure 5. Autocorrelation of measured remote control signal data

The actual measured UAV remote control signal length is 3 hops. The autocorrelation function is shown in the figure. $R_x(\tau)$ oscillates up and down in the range of $0<\tau\le T_h$ (T_h=14ms), and is a very small value in the range of $T_h<\tau<T$, which is close to 0. of. In the actual processing process, the threshold setting needs to be set in conjunction with the actual received data length, signal-to-noise ratio, sampling frequency and other parameters. And when the signal contains a fixed frequency signal, it will greatly affect the values of the two segments of the autocorrelation function, leading to false alarms.

Because fixed-frequency interference has a strong correlation throughout the observation time, a certain method must be taken to remove the influence of fixed-frequency interference on multi-hop autocorrelation detection. The main idea of the UAV signal detection method based on power spectrum estimation is to use the difference between the power spectrum of the UAV remote control signal and the fixed frequency signal over time, and the power spectrum cancellation can eliminate the interference of the fixed frequency signal.

Suppose the received signal is

$$x_N(n)=\sum_{i=1}^{p}s_f^i(n)+\sum_{j=1}^{q}s_h^j(n)+z(n) \quad (9)$$

Among them, $s_f^i(n)(i=1,2,\cdots,p)$ represents p fixed frequency signals mixed in the signal, $s_h^j(n)(j=1,2,\cdots,q)$ represents q frequency hopping signals to be processed, z(n) is the noise signal, and N is the signal length. Divide the signal into L pieces of data that grow into M, namely $x_N^k(n)(k=1,2,\cdots,\mathrm{L})$, and then use FFT to find the power spectrum of each piece of data $x_N^k(n)$, expressed as

$$\hat{S}_{x_N^k}^k(\omega)=\frac{1}{M}\left|\sum_{n=0}^{M-1}x_N^k(n)e^{-j\omega n}\right|^2,1\le k\le L \tag{10}$$

Add the power spectrum obtained from each piece of data and average it, and the average power spectrum $\overline{S_{x_N}}(\omega)$ of the received signal can be obtained as

$$\overline{S_{x_N}}(\omega)=\frac{1}{L}\sum_{k=1}^{L}\hat{S}^k(\omega)=\frac{1}{ML}\sum_{k=1}^{L}\left|\sum_{n=0}^{M-1}x_N^k(n)e^{-j\omega n}\right|^2 \tag{11}$$

Assuming that the p fixed-frequency signals $s_f^i(n)(i=1,2,\cdots,p)$ always exist in the received $x_N(n)$ data, the power spectrum of the i-th fixed-frequency signal $s_f^i(n)$ in the k-th segment data signal is

$$\hat{S}_f^{ki}(\omega)=\frac{1}{M}\left|\sum_{n=0}^{M-1}S_f^{ki}(n)e^{-j\omega n}\right|^2,1\le k\le L,1\le i\le p \tag{12}$$

Therefore, the average power can be obtained by calculation as

$$\overline{S_f^i}(\omega)=\frac{1}{L}\sum_{k=1}^{L}\hat{S}_f^{ki}(\omega)=\frac{1}{ML}\sum_{k=1}^{L}\left|\sum_{n=0}^{M-1}S_f^{ki}(n)e^{-j\omega n}\right|^2,1\le i\le p \tag{13}$$

By observing the above two equations, we can see that the power spectrum contained in each segment of the fixed-frequency signal $\hat{S}_f^{ki}(\omega)$ and the average power spectrum $\overline{S_f^i}(\omega)$ is almost the same, but the variance of $\overline{S_f^i}(\omega)$ after averaging is $1/L$ of the original variance of each segment of data $\hat{S}_f^{ki}(\omega)$.

Assuming that the frequency of the FH signal $s_h^j(n)$ in the received signal is $f_j(j=1,2,\cdots,q)$, there are m_j times in the received signal of length L ($m_j=N_L/N_M$, N_L is the number of sampling points of the frequency hopping signal, N_M is the number of sampling points of each segment of the signal after segmentation) , The power spectrum of the frequency hopping signal $s_h^j(n)$ in the received signal is expressed as

$$\hat{S}_h^j(\omega)=\frac{1}{M}\left|\sum_{n=0}^{M-1}s_h^j(n)e^{-j\omega n}\right|^2,1\le j\le q \tag{14}$$

Perform FFT transformation on the segmented data, and get the average power spectrum of the frequency hopping signal $s_h^j(n)$ expressed as

$$\overline{S_h^j}(\omega)=\frac{1}{L}\sum_{k=1}^{m_j}\hat{S}_h^j(\omega)=\frac{1}{ML}\sum_{k=1}^{m_j}\left|\sum_{n=0}^{M-1}s_h^j(n)e^{-j\omega n}\right|^2,1\le j\le q \tag{15}$$

It can be seen from the above two formulas that in the average power spectrum, the power of the frequency hopping signal has become m_j/L times that of the original signal in each segment, so the average power spectrum of the entire segment of data can eliminate the power spectrum of the frequency hopping signal , Only the power spectrum of the fixed frequency signal is left.

According to this feature, the power spectrum of each piece of data is subtracted from the average power spectrum of the entire piece of data, accumulated and summed, the fixed frequency signal is cancelled, and the frequency hopping power is almost unchanged. Define the parameter power cancellation ratio as

$$\zeta = p_1 / p_2 \tag{16}$$

Where p_1 represents the power after segmentation, p_2 represents the power after cancellation, and the threshold Λ is set. Usually the threshold is set according to the selection of the window function, the signal-to-noise ratio SNR of the signal to be detected, and the number of segments of the received data , FFT length is set, if $\zeta > \Lambda$, the signal to be detected is a frequency hopping signal, otherwise it is a fixed frequency signal.

The detection steps are as follows:

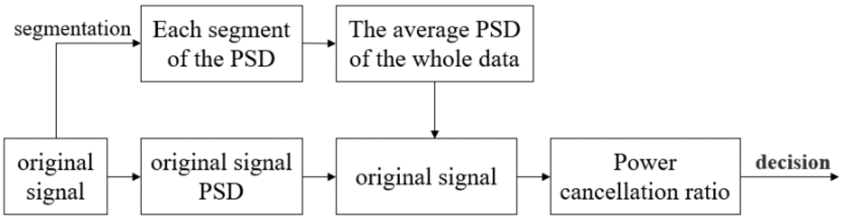

Figure 6. The flow chart of power spectrum estimation detection

Using the collected drone remote control signal data, the experimental results are shown in Figure 6. As can be seen from Figure 7a, the signal includes a 3-hop remote control signal, a map transmission signal, and many unknown fixed-frequency signals.

It can be seen from Figure 7b that the power of the FH signal can be obviously suppressed by calculating the average power spectrum in segments.

It can be seen from Figure 7c that the image can be well transmitted and the constant frequency signal can be cancelled, with good detection effect, and the remote control signal can be obtained.

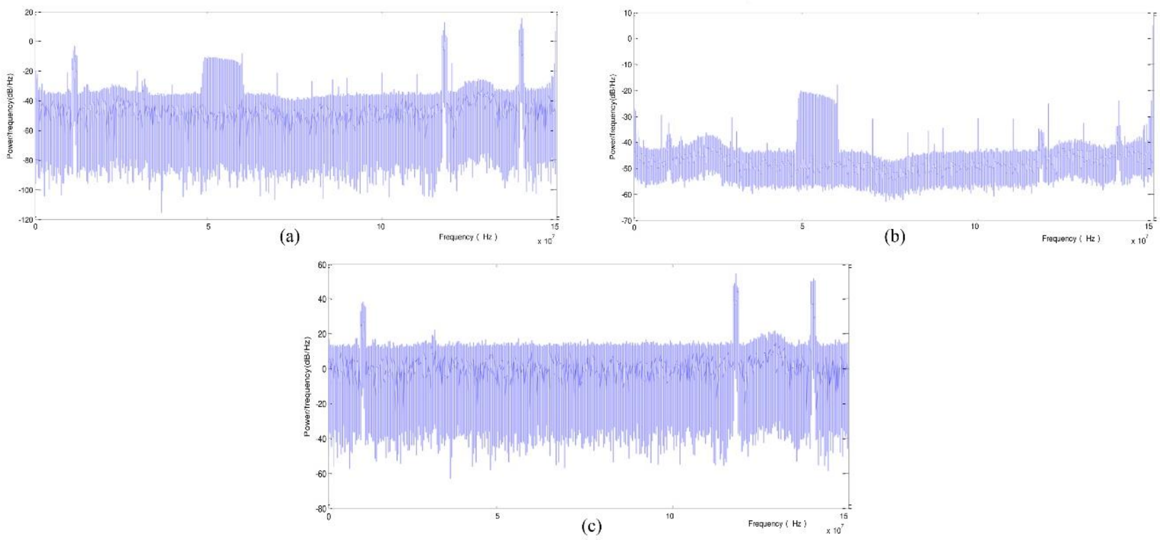

Figure 7. Power spectrum cancellation of the measured remote control signal. (a) The power spectrum of the original signal; (b) Average power spectrum; (c) Power spectrum after cancellation

5. Conclusion

This article first introduces several ways of drone presence detection. Through the detection and analysis of the drone communication signal, it can be judged whether there is a drone in the space, which is a promising direction. The advantage of the method proposed in this paper is that the amount of calculation is small and the implementation on hardware is relatively easy. It has good detection performance without knowing the characteristic parameters of the drone signal in advance, but the disadvantage is that it is in a complex electromagnetic environment. We can only eliminate the interference of fixed-frequency signals, and there are many other interference signals that cannot be solved. Our next plan is to continue our efforts in eliminating more interference. Then we can determine the position of the drone and the controller by analyzing the angle of arrival of the drone signal.

References

[1] I. Guvenc, F. Koohifar, S. Singh, M. L. Sichitiu, and D. Matolak, “Detection, tracking, and interdiction for amateur drones,” IEEE Commun. Mag., vol. 56, no. 4, pp. 75–81, Apr. 2018.
[2] Deng Z, Sun H, Zhou S, et al. Toward Fast and Accurate Vehicle Detection in Aerial Images Using Coupled Region-Based Convolutional Neural Networks[J]. IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing, 2017, PP (99):1-13.
[3] Fu H, Abeywickrama S, Zhang L, et al. Low-Complexity Portable Passive Drone Surveillance via SDR-Based Signal Processing[J]. IEEE Communications Magazine, 2018, 56(4):112-118.
[4] IEC, Banshee; http://www.iecinfrared.com/products/inte-grated-systems/banshee/, accessed 7 Nov. 2016.
[5] G. C. Birch, J. C. Griffin, and M. K. Erdman, “UAS Detection, Classification, an Neutralization: Market Survey,” prepared by Sandia Nat'l. Labs, 2015.
[6] M. Benyamin and G. H. Goldman, “Acoustic Detection and Tracking of a Class I UAS with a Small Tetrahedral Microphone Array,” Army Research Lab. tech. rep. (ARL-TR-7086), DTIC Doc., Sept. 2014.
[7] M. Ritchie, F. Fioranelli, H. Griffiths, and B. Torvik, “Micro-drone RCS analysis,” in Proc. IEEE Radar Conf., Oct. 2015, pp. 452–456.
[8] Hoffmann F , Ritchie M , Fioranelli F , et al. Micro-Doppler based detection and tracking of UAVs with multistatic radar[C]// 2016 IEEE Radar Conference (RadarConf). IEEE, 2016.
[9] Article in a journal: J. Farlik et al., “Radar Cross Section and Detection of Small Unmanned Aerial Vehicles,” Proc. 17th IEEE Int’l. Conf. Mechatronics--Mechatronika, Prague, Czech Republic, Dec. 2016, pp.1--7.
[10] S. Kamkar, “Skyjack: Autonomous drone hacking w/ Raspberry Pi,aircrack & Javascript,” Accessed: Apr. 18, 2017. [Online]. Available:http://www.samy.pl/skyjack/
[11] I. Bisio, C. Garibotto, F. Lavagetto, A. Sciarrone, and S. Zappatore, “Unauthorized amateur UA V detection based on WiFi statistical fingerprintanalysis,” IEEE Commun. Mag., vol. 56, no. 4, pp. 106–111, Apr. 2018.
[12] F. Tang, Z. M. Fadlullah, N. Kato, F. Ono, and R. Miura, “AC-POCA: Anticoordination game based partially overlapping channels assignment in combined UA V and D2D-based networks,” IEEE Trans. V eh. Technol., vol. 67, no. 2, pp. 1672–1683, Feb. 2018.
[13] Witschi M , Schild J , Nyffenegger B , et al. [IEEE 2016 24th European Signal Processing Conference (EUSIPCO) - Budapest, Hungary (2016.8.29-2016.9.2)] 2016 24th European Signal Processing Conference (EUSIPCO) - Detection of modern communication signals using frequency domain morphological filtering[J]. 2016.
[14] Yang Yanan. Research on detection and Recognition Method of UAV signal [D]. Chengdu: University of Electronic Science and Technology, 2018.