Research and Experiments on Anti-UAV Technology

Hongbo Wei, Xinhuai Wang*, Xiaowei Shi, and Bo Liang

National Key Laboratory of Science and Technology on Antennas and Microwave
Xidian University, Xi'an, Shaanxi, 710071, China
w5918666@vip.qq.com, *xinhuaiwang@xidian.edu.cn,
xwshi@mail.xidian.edu.cn, Seeker93@outlook.com

Abstract ─ Unregistered flight of Unmanned Aerial Vehicle (UAV) has been a severe challenge to the security of low-altitude airspace. Illegal elements may use UAV to carry dangerous goods or steal privacy. More and more conferences and large-scale activities pay attention to the security and privacy of the air defense. This paper focuses on two kinds of UAV interference solutions, traditional full-band suppression and targeted spectrum suppression. Experiments show that the target spectrum suppression scheme can reduce 4.61dB transmission power compared with traditional full-band suppression for a certain UAV at the same attack distance. The novelty of paper is that we use artificial intelligence method to analyze the spectrum of UAV signal and the new scheme can reduce power transmission by more than half at the same attack distance. This paper also carry out comparative experiments on different types of UAVs, demonstrating its excellent performance. In addition, for some WiFi UAVs, this paper can even steal their password to acquire the UAVs' control.

Index Terms ─ Control password, low transmission power, targeted spectrum suppression, traditional full-band suppression, Unmanned Aerial Vehicle (UAV).

I. INTRODUCTION

The number of civilian UAVs had grown tremendously in the past years. There is a huge potential that UAV offers in as far as revolutionizing approaches to handling tasks that require precision, accuracy and risk are concerned. As a result, there is a growing application of UAV in running recreational and commercial tasks. "Aerial photography", for instance, has gradually become a trend in society. Policies and guidelines exist on the registration and operational conduct of UAV for commercial purposes. However, there is lack of complete and rigorous management practices for civilian UAV, and most consumers do not receive any professional training [1-2].

The security control of large-scale activities is becoming more and more strict. Therefore, the anti-UAV technology is becoming more critical. UAV poses a threat to the security of society. Implementing mandatory dispersal ways is necessary. Based on the analysis of the existing UAV interference technology and its application status, this paper proposed traditional full-band suppression and targeted spectrum suppression methods. The full-band suppression interference is based on frequency sweeping. The targeted spectrum suppression interference is based on spectrum analysis. Both methods could suppress UAV communication signal by high-power noise signal. In this paper, a certain UAV is experimentally validated and the advantages and disadvantages are compared [3-4].

II. OVERVIEW OF UAV JAMMING TECHNOLOGY

Given the difficulty in regulating the airspace for unregistered and unexpected UAV, the remaining approach is to jam the signal communication so as to disable pesky ones. To understand how unregistered UAV can be stopped from accessing the airspace, we first need to understand their functioning. UAVs are piloted via RF technology and two frequency bands exist which assist in their communications: the 2.4GHz and the 5.8 GHz. Devices such as UAV represent modem application of tight frequency reuse and adaptive modulation. Using their communications technology, some expensive UAVs can easily control from far away and perform video recording functions. Even some UAVs can carry light dangerous items and Fig. 1 shows the dangerous UAV captured by military [5-7]. The following will introduce the interference methods.

A. Traditional full-band suppression interference

UAV suppression interference entails sending out noise interference signals on the target frequency band. Civilian UAV operates within known bands, if experimentally interrupted, the communication in this frequency band will interfere, and therefore the electronic device will not work correctly. In this design, the spectrum suppression signal is directly generated by frequency sweeping.

Submitted On: February 25, 2020
Accepted On: April 4, 2020

Fig. 1. Hazardous UAV.

Firstly, the traditional scheme is introduced. In the wide spectrum range, the signal jamming transmitter generates a periodic linear frequency sweep interference signal in a certain way. Therefore, the bit error rate of UAV communication receiver increases or even saturates directly. The UAV will disconnect with the remote controller and not able work properly. A communication breakdown between the device pilot and the device will make it impossible for the device to operate and to make any significant exploration of the airspace. This way, any targeted UAV can be eliminated from the airspace and only registered ones can operate.

B. Targeted spectrum suppression interference

The previous method requires a lot of transmission power, but the targeted spectrum scheme is a new scheme which can reduce unnecessary energy loss. This scheme is also the core innovation of this paper. The targeted spectrum interference adopts an idea of "interception-analysis-interference". Above all, this project needs to intercept the UAV communication signal, then analyze and process the UAV communication signal to get the signal communication frequency point, and finally suppress the UAV by transmitting the targeted frequency signal. Targeted spectrum suppression can theoretically saturate the UAV receiver efficiently, thus reducing the ability of the receiver to process normal signals and ultimately cutting off the communication of the target UAV.

In the case of losing the control signal, the UAV will return, hover or make a forced landing according to the original program, and ultimately achieve the purpose of intercepting the UAV.

III. DESIGN SCHEME

A. Overall design

The ultimate goal of both UAV interference plans is blocking the UAV receiver and paralyzing the coordination which would result in the successful piloting of the device illegally over an airspace. The Full-band suppression interference is based on the frequency sweeping method to spread the noise signal over a wider frequency band, and need not know the specific frequency. With the high-power interference transmitter, the interference can be performed within the communication band of the UAV. Targeted spectrum suppression interference takes the software radio technology as the core to form the frequency reconfigurable UAV interference platform. This platform can intercept the spectrum of the UAV communication signal, and analyze the communication frequency point to carry out targeted interference [8-10].

UAV communication signal includes control signal and image transmission signal, which can be in 2.4 GHz band or 5.8 GHz band. Due to the similarity between the 2.4 GHz band and the 5.8 GHz band, this paper takes the 2.4 GHz band as an example for specific analysis. Both plans block the UAV receiver by transmitting high-power suppression signals. The power amplifier and the antenna are the same except for the signal source. The whole system is shown in Fig. 2.

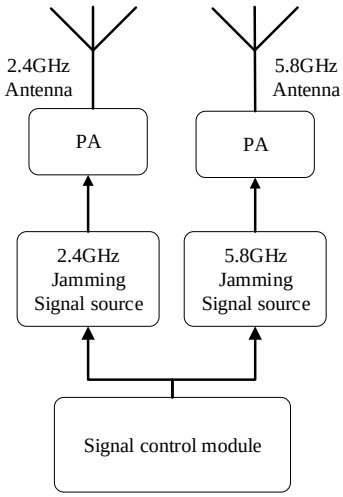

Fig. 2. The block diagram of whole system.

B. Design of traditional full-band suppression interference

The full-band suppression interference design consists of a sawtooth signal source, a voltage-controlled oscillator (VCO), a driver amplifier, and a power amplifier. The sawtooth signal is provided by the Agilent 33600A waveform generator. A sawtooth/triangle signal also could be generated by either a microcontroller or two operational amplifiers circuity. The waveform generator control VCO generates the frequency sweeping signal in the 2.4GHz~2.47GHz frequency band. VCO

selects chip MVE2400 and power amplifier selects chip SKY65135.

C. Design of targeted spectrum suppression interference

Targeted spectrum suppression interference is based on software radio and select USRP platform to design. The USRP is consisted of a Xilinx Kintex-7 FPGA and the AD9361, whose transmit frequency up to 6 GHz. Based on the Linux system, the USRP is used as the RF signal sources. USRP analyzes the spectrum of the UAV to obtain the frequency hopping frequency of the UAV communication signal and generates targeted suppression signals for these frequencies. By controlling and adjusting the RF parameters of USRP on the Linux system, the noise signal is transmitted through the power amplifier to block the UAV communication receiver, causing the UAV to be disconnected from the remote controller.

IV. EXPERIMENTAL RESULTS AND DISCUSSION

A. Module signal generation

The full-band suppressed interference signal module is connected to the spectrum analyzer, and the interference signal is observed to be distributed from 2.4 GHz to 2.47 GHz, and the power is about -1.56 dBm. The test result is shown in Fig. 3.

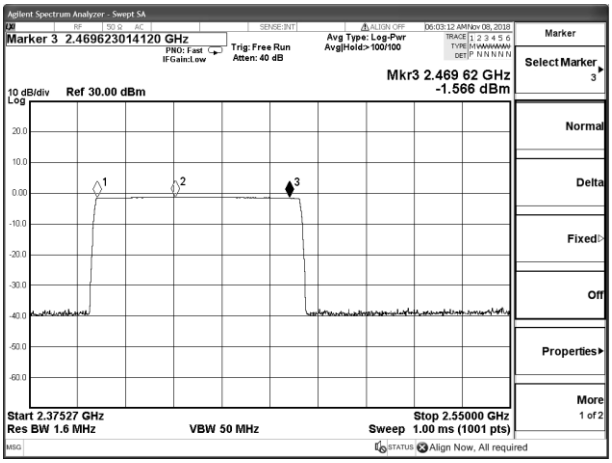

Fig. 3. Full-band suppressed spectrogram.

In this article, we chose DJI GO as the experimental object. DJI GO is a universal RF-controlled UAV that sells for about $1,500 in online mall. The specific parameters of the specific UAV can be found on the official website. The picture of DJI GO is shown in Fig. 4.

Fig. 4. DJI GO.

DJI GO communicates based on OFDM, which is an orthogonal frequency division multiplexing technology and a Multi-carrier modulation (MCM) technology. The basic idea of MCM technology is to convert the serial data stream to parallel data stream by decomposition, and then modulate these parallel data stream to several carriers of different frequencies. The targeted spectrum suppression interference scheme needs to know the hopping frequency point of the UAV communication signal [11]. Above all, receive the transmission signal from the UAV remote controller and then the signal is connected to the USRP platform. The communication signal of a certain UAV is analyzed to obtain the spectrum data, as shown in Fig. 5. It can be seen from the figure that the communication frequencies of UAV are constantly changing.

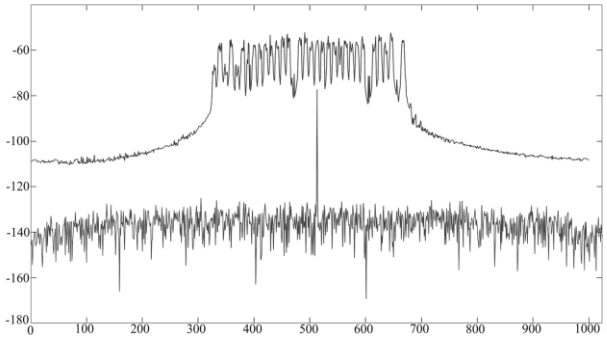

Fig. 5. Spectrum of UAV Communication Signal.

In this paper, we use the Long Short Term Memory model (LSTM) to recognize the frequency hopping sequence of UAV. The network structure schematic and network parameter model of long short term memory model are shown in Fig. 6.

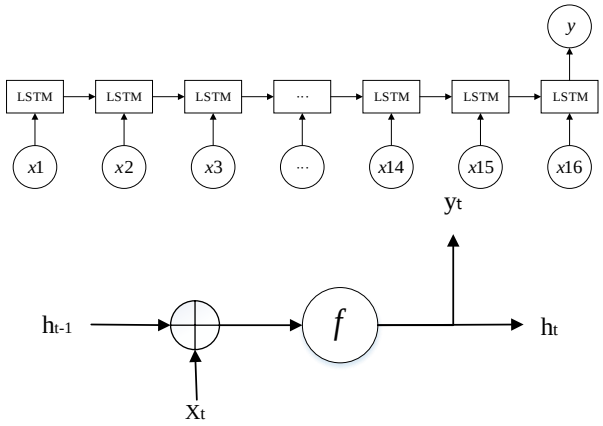

Fig. 6. LSTM model.

The spectrum difference of UAV communication signal is used as the feature of signal, so feature extraction is to transform the time domain data of UAV communication signal into frequency domain data. Formula transformation is expressed as (1):

$$X(k)=\sum_{n=0}^{N-1}x(n)e^{-j\frac{2\pi}{N}kn}(k=0,1,2\cdots,N-1), \quad (1)$$

The formula for calculating the neuron cell structure of LSTM neural network can be expressed as follows:

$$\begin{aligned} h_t &= f(W_{xh}x_t+W_{hh}x_{t-1}+b_h) \\ \mathrm{y}_t &= W_{hy}\mathrm{h}_t+b_y \end{aligned} . \quad (2)$$

For the given time series x_t, using the RNN model, equations (1) can be used to calculate h_t and the output sequence y_t. In the formula, *W* represents the weight coefficient matrix, *b* represents the offset vector, and *f* represents the activation function.

Using the LSTM model to train the drone signal, the project can get the accuracy rate and loss value with the training rounds [12]. The loss function can be expressed as the formula (3):

$$\begin{aligned} loss &= \frac{1}{N}\sum_{i=1}^{N}DL(y^i\|\overline{y^i}) = -\frac{1}{N}\sum_{i=1}^{N}\sum_{j=1}^{C}y_j^i\log\overline{y_j^i} \\ &= -\frac{1}{N}\sum_{i=1}^{N}\log\overline{y_k^i} \end{aligned} . \quad (3)$$

The LSTM model originally used the gradient descent method to optimize the neural network, but if the amount of data is large or the structure of the network is more complicated, the operation will take more time. In order to accelerate the analysis of loss value, this paper finally adopted Stochastic Gradient Descent method. This method can quickly complete the processing of UAV signals, and the formula is shown in (4):

$$w^{\tau+1}=w^{\tau}+\eta(t_n-(w^t)^{\mathrm{T}}x^{(n)})x^n. \quad (4)$$

The LSTM model test results are shown in Fig. 7. The accuracy rate increases with the number of training rounds, and the accuracy rate gradually approaches 100%. At the beginning, the loss value will slightly jitter up and down, but similar to the accuracy rate, the loss value eventually approaches 0. In addition, the project also uses different signal-to-noise ratio signals for artificial intelligence recognition, which can obtain the accuracy curve with different signal-to-noise ratio signals.

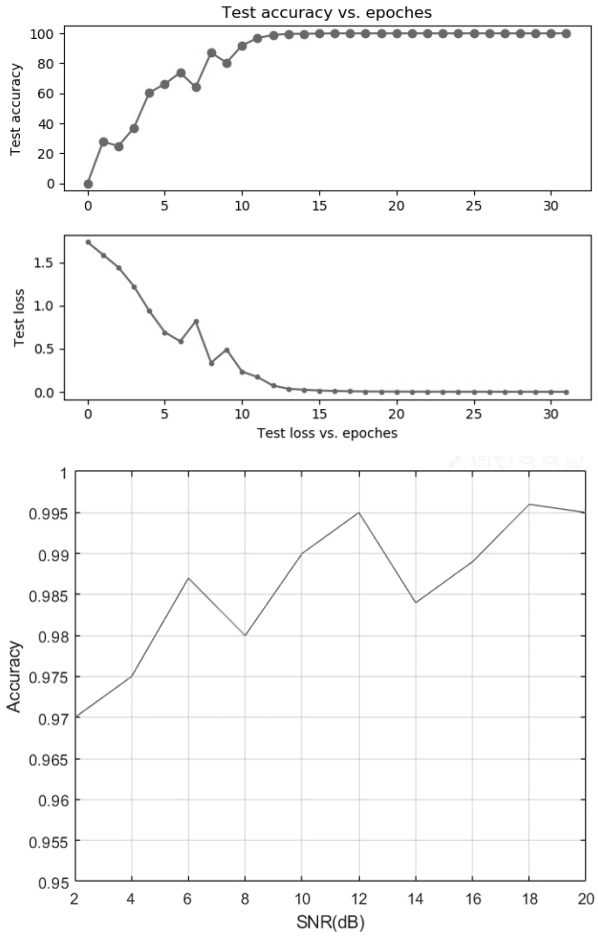

Fig. 7. LTSM training process.

The change of signal-to-noise ratio has a certain impact on the accuracy of UAV signal recognition. With the increase of signal-to-noise ratio, the accuracy has a trend to improve, but the improvement is actually small. It can be seen from the figure that the SNR increases from 2dB to 20dB, and the recognition rate increases by about 2.5%, so the recognizer has certain anti-interference ability Power.

By further analyzing the spectrum data of the UAV communication signal received once, the hopping frequency points of the signal spectrum can be obtained. The hopping frequency signal has 28 points, the hopping interval is 14ms, the frequency point bandwidth is 1.2MHz, and the spectrum range is 2404MHz~2470MHz.

USRP generates a targeted spectrum suppression signal with this data, the frequency hopping sequence and point is shown in Table 1 and Fig. 8.

Table 1: Frequency hopping point

Hopping Sequence	1	2	3	4	5	6
Frequency hopping point	2424	2470	2448	2425.8	2404	2456
Hopping Sequence	7	8	9	10	11	12
Frequency hopping point	2428	2405.8	2452	2430	2408	2454
Hopping Sequence	13	14	15	16	17	18
Frequency hopping point	2431.8	2412	2458	2436	2414	2460
Hopping Sequence	19	20	21	22	23	24
Frequency hopping point	2437.8	2416	2464	2442	2420	2466
Frequency hopping point	25	26	27	28		
Hopping Sequence	2444	2422	2468	2445.8		

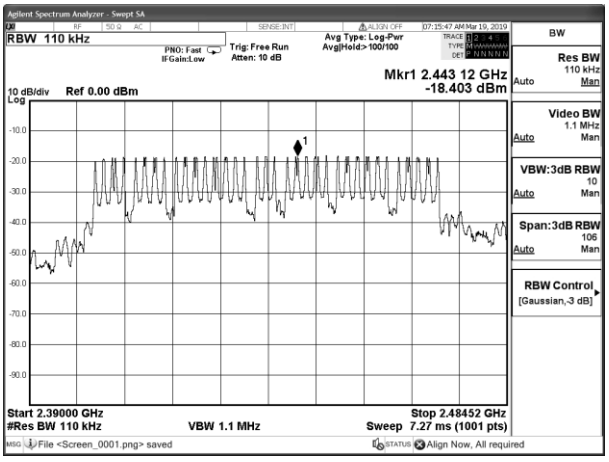

Fig. 8. Targeted Spectrogram.

B. Experiment and comparison of jamming UAV

The traditional full-band suppressed interference output signal is in the 2.4GHz~2.47GHz band and connect the signal source to the power meter to measure its average output power is -0.86dBm, as shown in Fig. 9.

Fig. 9. Full-band suppressed output average power.

The full-band suppressed signal source is connected to the power amplifier, with an average output gain of 36dB. The antenna is a well-directed Yagi antenna with a gain of 15 dBi. What's more, the remote controller is 50 meters away from the UAV and ensures that the remote controller is not affected by interference signals. The schematic diagram of the experimental test is shown in the Fig. 10.

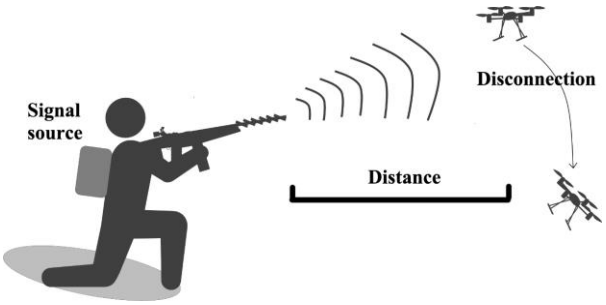

Fig. 10. Schematic diagram of the experiment.

Experiments show that the maximum distance of full-band suppression interference attack UAV can reach 380 meters. Replacing high power amplifier and high gain antenna can increase the attack distance.

Next, experiments are carried out on the targeted spectrum suppression jamming scheme. The average output power of the targeted spectrum interference signal source is set the same as the full-band suppression interference signal source, which is about -0.86 dBm.

When the transmit power is similar, targeted spectrum suppression interference scheme can attack UAV up to 670 meters. The critical point of test result is that the UAV remote controller changes from weak signal state to unconnected aircraft state. At this time, UAV communication receiver is blocked and cannot receive control and image transmission signals. The unconnected state of the aircraft is shown in Fig. 11.

Fig. 11. The state of UAV being disconnected.

The average output power of the targeted spectrum suppressed signal source is set as a variable and the standard is 0.86 dBm. The experiment measures when the average output power is reduced by 3 dB and the attack distances of the two schemes are the same. The test results is shown in Table 2.

Table 2: Experimental results of targeted spectrum suppression

Average Power of Signal Source/dBm	-0.86	-3.83	-5.47
Attack distance/m	670	500	380

What should be emphasized in this table is that the signal source does not include the power amplifier. The power amplifier and antenna uses the same modules and have the same gain as the previous experiment.

Free space loss describes the energy loss when electromagnetic waves propagate in air. The free space loss formula is expressed as follows:

$$Ls = 20\lg(F) + 20\lg(D) + 32.4 \quad (4)$$

$$Pr = Pt + Gt - Ls + Gr$$

F is the frequency, D is the distance, Pt is the transmit power, Gt is the transmit antenna gain, Ls is the free space loss, and Gr is the receive antenna gain. In this paper, the control variable only modifies P in the design process, and the other influences are the same.

According to the free transmission loss formula, when other factors are determined, the transmitting power is the most important factor affecting the attack distance of UAV [13-14]. On the basis of the test results, with the same power amplifier and Yagi antenna, the attack distance of the targeted spectrum suppression scheme is approximately 1.76 times that of the full-band suppression scheme. At the same attack distance, the average output power of the targeted spectrum suppression scheme is reduced by approximately 4.61 dB. The average output power is -5.47dBm, as shown in Fig. 12.

Through the above experimental tests, it is proved that the targeted spectrum suppression scheme has superior performance compared with the traditional full-band suppression scheme.

In addition, data acquisition and attack experiments of other types of UAVs are also carried out. For the DJI GO series UAVs, the power consumption can be saved to varying degrees by suppressing attacks. The following is a data acquisition chart of different series of UAVs, as shown in Fig. 13.

Fig. 12. Targeted spectrum suppression output average power.

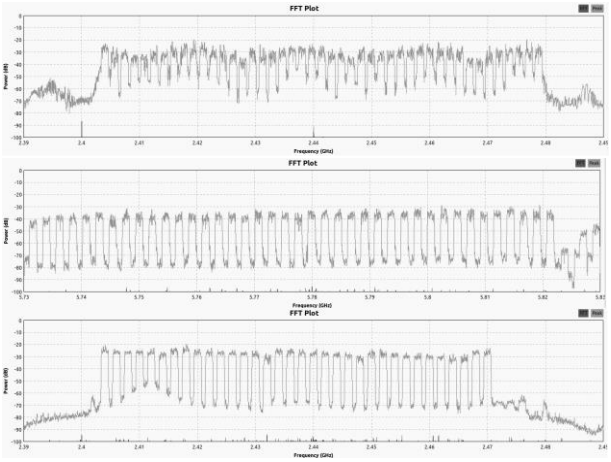

Fig. 13. DJI GO Series UAVs Signal Data.

The project carries out comparative experiments for different series of UAVs. By using neural network to analyze the UAV OFDM data signal and suppress the UAV OFDM signal in real time. In the experiments of different series of UAVs, the experimental results of the project are similar to the above table data. Under the same attack distance, the power consumption is saved about 4.6dB or the same transmit power, the attack distance is about 1.7 times.

In addition, the project also studies the WiFi-controlled UAV with the scheme of De-authentication Flood Attack. Some UAVs can even decipher WiFi passwords to gain control of the UAV. By sending forged cancellation authentication frames, De-authentication Flood attack makes the access point mistakenly think that the client wants to disconnect from it, and then the WiFi type UAV is out of control. Attack experiments for WiFi UAV are shown in Fig. 14.

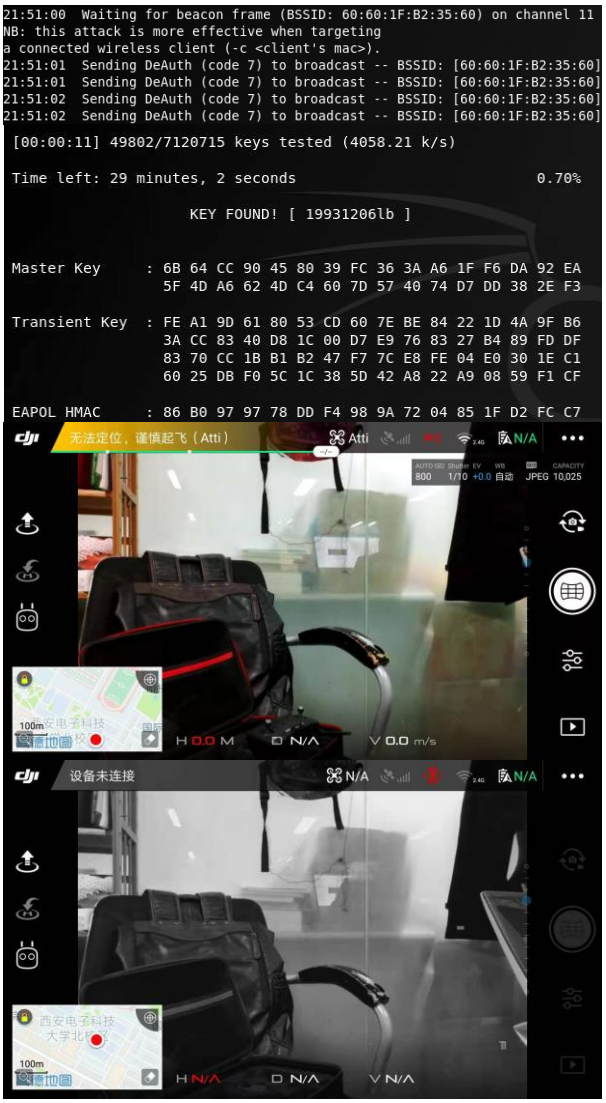

Fig. 14. Attack experiment process of WiFi UAV.

V. CONCLUSION

The Unregistered flight of UAV poses a serious threat to the security work in large-scale events. Whereas there is widespread adoption of UAV in recreational activities, there is record of inappropriate use of UAV to access highly sensitive information areas. Besides their size, the fact that UAV are remotely piloted provides a certain anonymity that can breed insecurity and inappropriate use of airspace. This paper proposes two solutions to this problem, traditional full-band suppression and targeted spectrum suppression. The experiments show that traditional full-band suppression scheme consumes more energy and has a shorter attack distance. In order to solve this problem, this paper proposes a targeted spectrum suppression scheme, and the novelty of this scheme lies in that the targeted spectrum suppression scheme can reduce the average output power by 4.61dB or can attack longer distances, which has a very good application prospect [15-18]. This experiment has tested other common UAVs on the market, and the experimental results are in line with expectations. For some WiFi UAVs, this experiment can even get their control passwords. This paper provides a new direction for the design of anti-UAV jammers and electromagnetic countermeasure system.

ACKNOWLEDGMENT

This work is supported by the The National Key Laboratory of Antennas and Microwave Technology from Xidian University, the Fundamental Research Funds for the Central Universities, the Innovation Fund of Xidian University and the National Natural Science Foundation of China (61405152).

REFERENCES

[1] S. S. Guo, "Development status of anti-UAV technology and products," *Military Digest*, vol. 19, pp. 36-39, 2016.

[2] D. Mei and L. Gao, "Application of directional energy weapon in anti-UAV operation," *China Plant Engineering*, vol. 7, pp. 40-42, 2017.

[3] Y. Fan and W. M. Li, "The impact of UAV on future air defense operations and countermeasures," *Modern Defense Technology*, [D], 2003.

[4] Y. Yang, C. Wang, and Y. Wu, "Current situation and development trend of anti-UAV strategy and weapon equipment," [J]. *Aerial Missile*, vol. 8, no. 8, pp. 27-31, 2013.

[5] X. H. Pan and Z. Q. Qin, "Brief analysis of anti-UAV system," [J]. *Scientific Chinese*, vol. 2Z, p. 29, 2016.

[6] M. Y. Xia, K. Zhao, and W. Ni, "Key technologies for the prevention and control of anti-UAV systems," [J]. *Command and Control and Simulation*, vol. 40, no. 2, pp. 53-60, 2018.

[7] F. L. Hui, "Research on anti-UAV industry," [J]. *China's Strategic Emerging Industries*, vol. 16, p. 9, 2018.

[8] L. Liu, Y. F. Wei, and Y. H. Zhang, "Analysis of the development of US anti-UAV technology and equipment," [J]. *Aerospace Electronic Countermeasure*, vol. 33, no. 1, p. 60, 2017.

[9] Y. Zhi and S. Lan, "Development of non-destructive anti-UAV technology abroad," [J]. *Light Weapons*, vol. 2018, no. 07, pp. 18-23, 2018.

[10] B. Luo, Y. C. Huang, and H. Zhou, "Overview of the development status of foreign anti-UAV systems," [J]. *Aerial Missiles*, vol. 2017, no. 09, pp. 24-28, 2017.

[11] M. Saber, A. El Rharras, R. Saadane, et al., "Artificial neural networks, support vector

machine and energy detection for spectrum sensing based on real signals," [J]. *International Journal of Communication Networks and Information Security*, vol. 11, no. 1, pp. 52-60, 2019.

[12] M. Saber, A. El Rharras, R. Saadane, et al., "Transmit-power and interference control algorithm in cognitive radio network based on non-cooperative game theory, [C]. *The Proceedings of the Third International Conference on Smart City Applications*. Springer, Cham, pp. 647-662, 2019.

[13] D. Me and L. Gao, "Application of directional energy weapons in anti-UAV operations," [J]. *China Equipment Engineering*, 7:40, 2017.

[14] Q. H. Zhu, *Technique of Communication Jamming and its Application in Spectrum Management*, Beijing: Posts & Telecom Press, 2010.

[15] Y. W. Liu and X. B. Liao, "Construction of basic framework for anti UAV technology system," *Journal of Weapon Industry*, 10:E926.3, 2015.

[16] J. Chen and D. S. Chen, "Analysis of effectiveness index system of microwave weapon anti UAV," *Journal of Guilin College of Aerospace Technology*, 2010.

[17] C. Liang, "Research on UAV detection and jamming method based on wireless signal," *Zhejiang University*, 2018.

[18] H. Liu, "Development and application of anti aircraft system for security enterprises," *China Security*, 2018.

Hongbo Wei was born in 1995 and received the B. S. degree in Electrical Engineering from Xidian University, Xi'an, China, in 2017. He is currently working toward the M.S. degree in Electromagnetic Field and Microwave Technology from Xidian University. His recent research interests are mainly in the design of circuits and algorithms.

Xinhuai Wang received the B. Eng. degree, M.Eng. and Ph.D. degrees in Electrical Engineering from Xidian University, Xi'an, China, in 2004, 2007, and 2011, respectively. Since 2011, he has been with Collaborative Innovation Center of Information Sensing and Understanding at Xidian University and Science and Technology on Antenna and Microwave Laboratory, Xidian University, as a Lecturer and Associate Professor. He has authored or coauthored over 60 international and regional refereed journal papers. His recent research interests are mainly in the design of microwave components system. He is a member of IEEE and senior member CIE.

Xiaowei Shi received the B.Eng. degree and Ph.D. degrees in Electrical Engineering from Xidian University, Xi'an, China, in 1982 and 1995, respectively. He has authored or coauthored over 200 international and regional refereed journal papers. He is IEEE Senior Member and the Chairman of the IEEE Microwave Society Xi'an Chapter.

Bo Liang was born in 1993 and received the M.S. degree in Electro-magnetic Field and Microwave Technology from Xidian University, Xi'an, China, in 2019. His field of expertise is related to drones, and research interests are mainly in the embedded system and algorithms.