Fixed Detection 、Jamming& Decoy Anti Drone Device

Drone detection defense system, is the cognitive radio protocol reverse parsing technology (CognitiveRadio ProtocolCracking, CRPC), solve the domestic and foreign civil uav detection, identification, orientation, defensive low security system. The system can detect and identify, omnidirectional interference or precision strike the drones in the protected area, and is widely used in low-altitude security defense of public security, airports, prisons, impor tant facilities, large venues and major event venues.

Cognitive radio protocol reverse analysis technology is the fourth generation UAV defense method. This technology monitors the radio environment in the target defense area through the antenna array, collects radio signals in the defense area 24 hours a day, and transmits the collected signals to the signal processing unit to accurately demodulate and reverse analyze the UAV signals. Then the analyzed UAV signals are transmitted to the data server through the network, and the data server identifies the received UAV signals and guides the interference module to strike and defend the UAV.

The decoy technology adopts generative decoy interference. The product calculates the necessary parameters such as GPS, BDS, GLONASS and Galileo signals that the target needs to receive at the desired target position in real time according to the pre-specified target position, builds the corresponding mathematical simulation model and signal synthesis module, and generates the corresponding navigation satellite decoy signals in real time.

1. Summarize

The fixed UAV detection and decoy equipment is a kind of UAV detection and decoy countermeasure equipment equipped with UAV integrated control system. Through the indepth analysis and data mining of UAV signals, the device can monitor multi-dimensional information such as serial number, model, position (latitude and longitude, azimuth), speed , altitude, altitude, take-off point, return point, track, remote control position (latitude and longitude, azimuth) of the UAV within the monitoring range.

The device is suitable for low-altitude security in political core areas, border defense , military restricted zones, military management zones, power and petrochemical parks and airports, etc. It can work independently offline, deploy flexibly and rapidly, and respond flexibly to meet the needs of various scenarios to form a tight low-altitude protection network.

2. Performance parameter

No	Name	Parameter	Note
1	Detection range	100MHz~6200MHz	
2	Scan time	120M bandwidth scanning time ≤0.25s	
3	Detection distance	1~5km	
4	Detectable drone model	Common models, such as DJI Avata 2, mini4pro, Dao EVO Ⅱ pro v3, EVO lite+ and other 220+; Homemade class or traversal machine 110+; WiFi machine, such as Youdi, Haoxiang, Sima, etc	
5	Locatable drone model	Some models of DJI	
6	Trajectory detection	The farthest detection and positioning distance of the existing brand and model UAV in the feature database is >3km in the open area without shelter	
7	Detection angle	Less than 15°	
8	Recognition time	≤1s	
9	Recognition quantity	≥60	
10	Connection mode	Ethernet /WiFi	
11	Operating temperature	-40℃~ 70℃	
12	Power supply	AC220V	
13	Black and white list	Support	
14	Hd GIS system	Displays information about the surrounding environment and device layout points	

15	Log and playback functions	No intrusion log, log display Angle, alarm time, frequency information, can play back UAV intrusion records	
16	Statistical statement	The statistical report of UAV intrusion can be provided, and the system can provide sound and light alarm	
17	orientation	The system has GPS positioning function, which can mark the location on the map	
18	Automatic north correction	The system should be able to automatically calibrate the north	
19	Machine weight	Single detection ≤15KG, Single jammer <22KG	
20	Working hours	All the time	
21	Software database	Support DJI's full range of drone detection and other brands - later upgradable	
22	Working mode	Spectrum + database protocol analysis technology, using radio silence monitoring,Real-time automatic monitoring, no electromagnetic radiation, and compatible with electromagnetic sensitive areas	
23	Peculiarity	Pinpoint the drone, identify the serial number	
24	Fixed refresh time	≤3-10s	
25	Operating system	Android/Windows	
26	Class of protection	IP68	
27	Display screen	The size of a tablet or laptop	
28	Reconnaissance sensitivity	Better than -95dBm (25kHz)	
29	Frequency measurement accuracy	≤1KHz	
30	Withdrawal time	≤3min	
31	Detection success rate	99%	
32	Defensive radius	≥2km	
33	Intercept response time	≤1s	

34	Interception quantity	≥35 units	
35	Interference mode	Evictions and forced landings	
36	Defense success rate	≥99%	
37	Jamming frequency	Output end 400-450MHz 50w 840-930MHz 50w 1160-1280MHz 50w 1550-1630MHz 50w 2380-2500MHz 50w 5150-5300MHz 50w 5720-5880MHz 50w	Average output power (total jamming power 350W)
38	Materials	Aluminum alloy + high performance glass steel	
39	Antenna type	Omnidirectional antenna + directional antenna complex	
40	Automatic defense	unattended	
41	System linkage	The extension interface is provided to facilitate the linkage with jammer devices	
42	Trick the frequency point	GPS LI 1575.42±1.023 BDS B1 1561.098±2.046 GLONASS LI 1602±4.17 GPS L21227.6±1.023 Galileo E1 1575.42±12.276	
43	Peculiarity	It can achieve a variety of ways to lure drones, including: drive away, smooth crash landing, rapid crash, etc	
44	Active defensive range	Greater than 2000 meters, less than 25,000 meters and the distance is adjustable	
45	Trick the number of drones at the same time	unlimited	
46	Effective decoy Angle	Horizontal: 360°, vertical: 90°	

Schematic drawing

Equipment composition

No.	Name	Quantities	Description	Photo
1	Fixed detection and decoy equipment	1pcs	Detect & decoy device host	
		1pcs	Computer link cable	
		1set	Host antenna array	
		1pcs	Power cable	
2	Fixed jamming equipment	1set	The main machine is equipped with fiberglass antenna	
		1pcs	Power cable	
		1pcs	Detect decoy and jammer link cables	
		1pcs	Jamming device host	

3. Installation and deployment

3.1 Check the equipment list

Before assembling and installing the equipment, check the specifications and quantity of all spare parts and standard parts according to the equipment packing list, read the equipment user manual and other supporting documents, and get familiar with the installation points of the equipment.

3.2 Survey and select a site

The device is usually deployed outdoors. Before installing and deploying the device, conduct a thorough site survey. Site investigation should pay attention to the following factors:

(1) Visibility environment: should have good visibility conditions, generally choose flat, open highlands, can also choose the top of the building:

(2) Electromagnetic environment: try to avoid electromagnetic environment interference areas such as microwave stations, radio transmission towers, and high-voltage line towers crossing zones, as well as ground object areas that are easy to produce multipath effects:

(3) Natural environment: avoid the tuyere as far as possible to reduce the wind load of the equipment antenna: For areas with many thunderstorms, avoid areas prone to water accumulation and lightning strikes:

(4) Electrical environment: try to avoid areas that are prone to communication interference such as electrified railways:

(5) Basic guarantee: near a stable, safe and reliable power supply, support access to public or private communication networks:

(6) Other factors: there is a construction land and a good security environment, and the deployment site has a certain load bearing and firmness, which is convenient for personnel maintenance and long-term operation of the equipment site.

3.3 Device Host Deployment

You can select fixed installation or mobile vehicle deployment based on the specific application scenario.

1.the ground installation is fixed, the four supporting feet of the equipment are installed at the bottom of the equipment, and the model is installed in an open area without shelter. In the specific deployment, the construction plan can be

formulated according to the site survey.
2. Mode 2: Mobile vehicle deployment mode
The installation scheme varies according to the chassis platform on which the system is installed. In the actual deployment, the modification plan of the vehicle modification plant shall prevail.

3.4 Installing the Host Antenna

(1) Screw the FRP antenna to the radio processing unit one by one in a clockwise direction according to the corresponding interface marked on the antenna and the radio processing unit. The detection and attack antennas of the same frequency band can be common, and the detection and attack antennas of different frequency bands can not be common.
(2) Connect one end of the waterproof special network cable to the radio processing unit, and the other interfaces are used for spare or subsequent equipment upgrade spread spectrum. Note: Different devices may be slightly different. When connecting the antenna, you must connect the antenna and the radio processing unit according to the interface identifier. Otherwise, the radio processing unit will be damaged after the system is turned on.

3.5 Charging Terminal Deployment

Charge terminal is generally deployed in the customer security center or duty room, through the equipped waterproof special network cable and the device host can be connected, display can also be through HDMI cable to charge platform and other types of display terminal.

3.6 Connecting the Power Network

(1) Network access. The radio processing unit can be connected to the charge terminal through the TCP/IP interface by optical fiber or standard network cable, and the data server can be connected to the Internet by wireless connection.
(2) Power access. Radio processing unit, 220V AC, can be connected by fixed power supply or UPS. Reserve 220V fixed power supplies or deploy UPS power supplies at the deployment site. Note: The UAV detection and defense system uses wired network access by default. If wireless network access is required, contact the local network operator for wireless network access services.

4. System login description

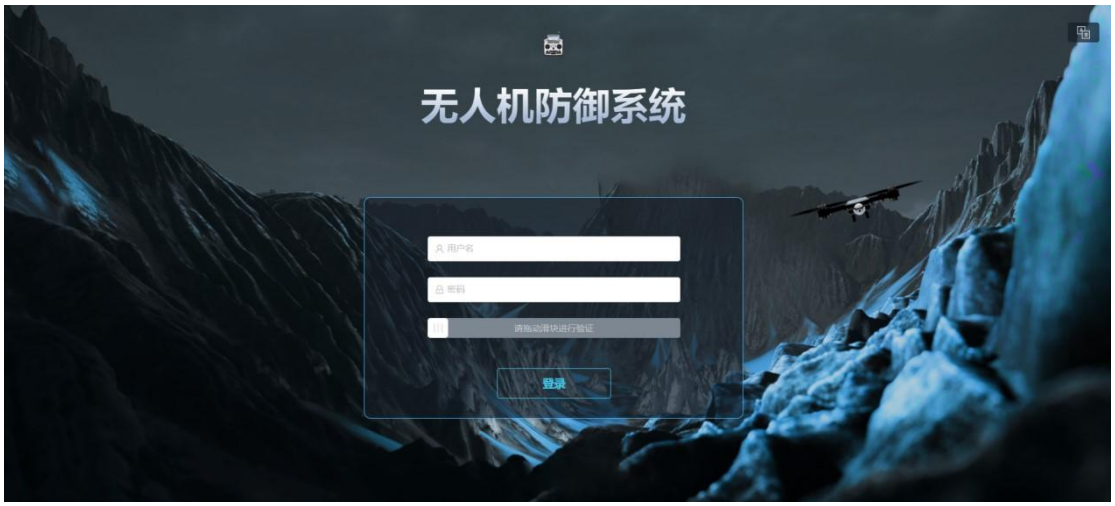
4. 1. Direct cable connection:

(1) The computer and the fixed equipment RJ45 network port are connected through network cables

(2) Open the network Settings on the computer, and configure the network segment of the network port connected to the device as 192.178.10.xxx. Note that the IP address of the fixed device is not set to repeat

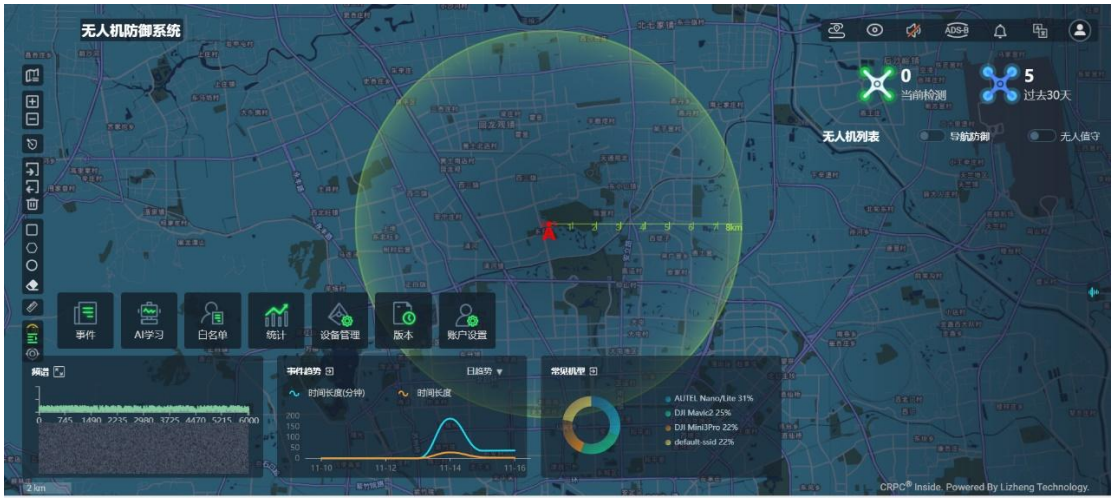
(3) Open the browser on the computer and visit the website: 192.178.10.130

(4) System interface



(5) The default user name and password for embedded Web are as follows: User name: admin password: abc123

(6) Login interface After entering account (demo) and password (secret) on the login interface, you can enter the main interface of system work (for supporting account and password, please ask the supplier).



4.2. Main interface of the software

According to the distribution orientation, the main interface of the software has three main function partitions, namely, the left function menu area, the lower function menu area, and the right information display control area.

Figure 7 Software main interface menu

1) Left function menu area

The main functions of the function button area include map display control, prevention and control zone setting, etc. Users can select and click the corresponding function button to operate according to their needs.

2) Function menu area on the lower side

The main functions of the function button area on the lower side include historical event query, whitelist query, UAV information statistics, device management, version and account setting, etc. Users can select and click the corresponding function button to operate according to their needs.

Figure 8 Software function menu

3) Right information display control area

The main functions of the information display control area include hiding/displaying the menu bar of the main interface, volume adjustment, notification switch, Chinese and English switching, system login/exit and other operations. Users can select and click the corresponding function buttons to operate.

In addition, this area is mainly responsible for the real-time detection information display and control functions of drones, which can display the number of current detection and historical detection drones, as well as the detailed information of currently detected drones.

4) Drone detection

Once the drone is detected, the system will automatically alarm and display the general position and direction indication information of the drone on the main interface. The right side of the system displays the number, model, frequency, electronic fingerprint (ID), intrusion direction and other information of the detected drones in real time.

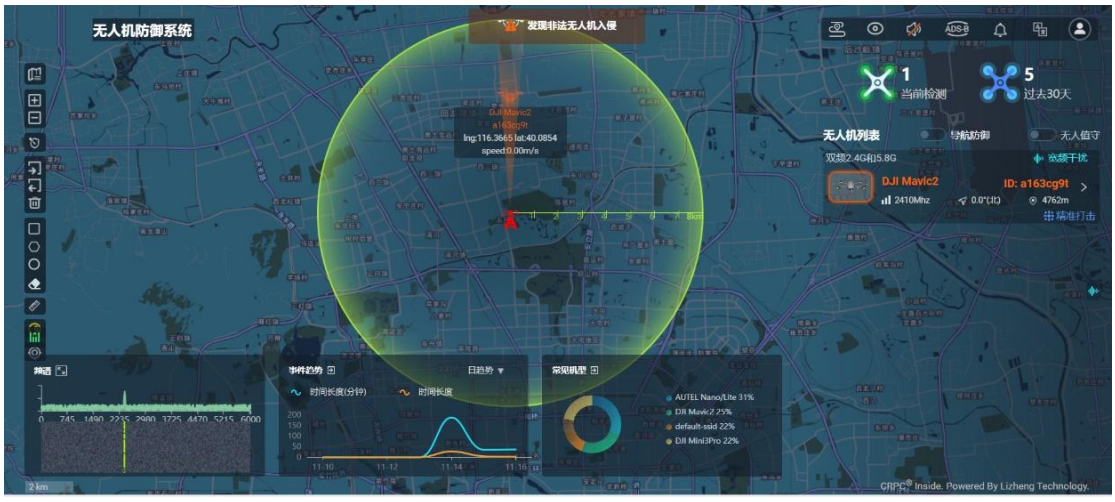


FIG. 9 Display interface of UAV detection

5) Initiate the jamming

Users can manually select the designated interference frequency band according to the actual situation, and implement "broadband interference" or "precision, strike" on the UAV.

Figure10 Jamming control interface

6) Cancel the strike

Click the "Cancel strike" button on the software interface, and the device will cancel the drone strike.

Figure11 Cancel control interface

7) No one is on duty

After the unattended mode is turned on, once the system detects the UAV, it will automatically identify and filter the "whitelist" list UAV, start the "precision strike" or "broadband interference" on the "blacklist" UAV, and automatically cancel the strike after the alarm is no longer raised. The strike process can be manually canceled, and the navigation decoy can be manually opened or canceled.

Figure12 Automatic strike interface

8) Set the whitelist

After the system detects the drone, open the drone list expansion menu and click Add/Remove whitelist.

Figure13 Whitelisting

Figure14 Removing the whitelist

9) Attribute information annotation

After the system detects the UAV, open the UAV list and expand the menu, click "Properties" to open the property setting page, and set the information or name of the specified UAV according to customer needs.

The modified UAV name or information will be displayed on the main interface of the system.

Figure15 Input of UAV attribute information

10) View historical events

Move the mouse to the "Function menu bar" on the lower left side of the software and click "Event" to enter the list of UAV historical events, and view the discovery time, duration, model, UAV identification code, working frequency band and other information. The list can also be expanded by "time" or merged by "model", as shown in the following figure. This function allows you to expand or merge Event Trend on the main screen with one click.

Figure17 Historical event view

11) View the whitelist

Move the mouse to the "Function" menu bar on the lower left side of the software and click "Whitelist" to enter the whitelist interface and manage the whitelist
drone.

Figure16　Whitelist viewing page

12) View the statistics report

Move the mouse to the "Function menu bar" on the lower left side of the software and click "Statistics" to enter the statistics interface. You can view the statistics report of UAV incidents, including the number of detected drones, common models, intrusion time, and development trend of UAV incidents, etc. At the same time, this function supports one-click expansion/merging of "Common samples" on the main interface.

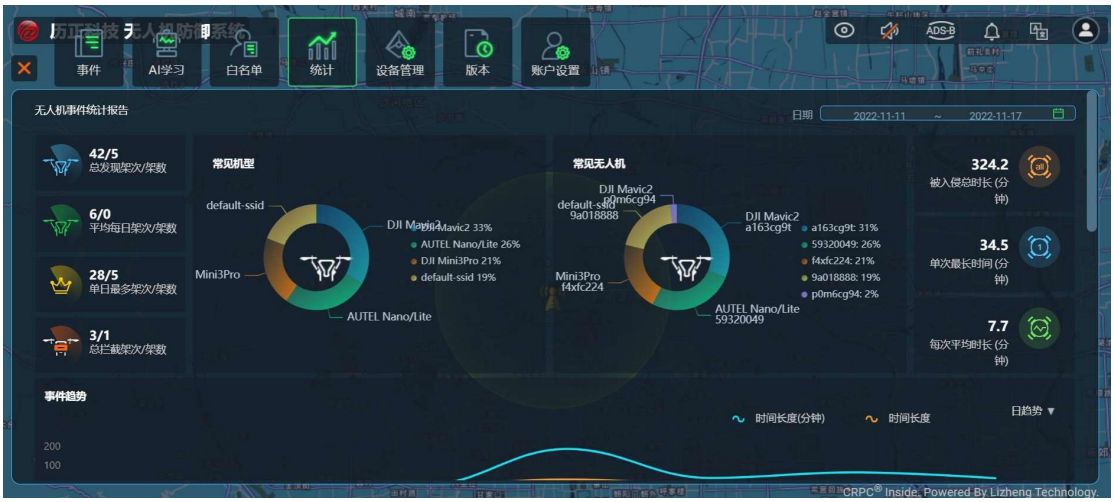


Figure18 Statistical report view

13) Check the device status

Click the Device Management button to view and monitor the basic device running status information of the controller, computing engine, and sensor.

Figure19　Viewing device status

1. Check the controller status. You can view the controller running status, online time, and configuration file.

2. Check the computing engine. You can view the running status, online time, temperature, version, and packet sending status of the computing engine.

3. Status of the sensor. You can view the operating status, online time, software version, and configuration files of the two sensors.

4. Jammer status. You can view the operating status, online time, fault status, GPS status, software version and other information of the two jammers, as well as the configuration file.

* Note: In case of equipment failure, click "Equipment failure" and follow the prompts to operate or consult after-sales personnel.

14) Account Settings

Click the "Account Settings" button, the user can change the password here, change to add a user.

Figure 21 Account information Settings

Note: The system control software interface diagram is for reference only, the actual object shall prevail.

5. Basic troubleshooting

a) Verify that the computer is turned on and that the terminal equipment and all components are supplied with power;

b) Ensure that all cables are securely connected to the appropriate ports;

c) Ensure that feeders, power supplies, and network cables are not damaged or worn;

d) Ensure that the pin connecting the plug is not bent or damaged;

e) Restart the computer and check whether the problem still exists;

f) Unplug the power plug of the terminal device, wait 30 seconds, and try to plug it back in;

g) After the server and detection terminal devices are started, check whether the "Device Management" process (controller, computing engine, sensor) on the server interface works properly;

h) Check whether the network connection between the device and the service terminal is normal;

i) If the fault still cannot be removed, please contact our technical personnel, do not disassemble the chassis.

5. Use precautions

a) Make sure that the attack and detection antennas of the detection terminal equipment are connected properly before power on. Do not power on before installing the detection and detection antennas;

b) If the server stops running due to power failure, please turn on the power switch again, start the server, start the service, the server can resume normal operation;

c) In order to ensure the normal operation of the device, it is recommended not to install other software unrelated to the operating system on the display terminal, such as software system problems caused by arbitrary installation of software by customers are not covered by the warranty;

d) Do not delete internal system files, do not arbitrarily change the date and time of the system, do not arbitrarily shut down or restart the server;

e) This product is a highly technical equipment, if the system in use in the process of failure, should inform our after-sales service department in time, must not be disassembled at will, so as to avoid damage to the internal structure or improper operation and damage to your rights and interests;

f) Please use this product within the scope permitted by national laws and regulations. Any adverse consequences caused by violation of laws and

regulations shall be borne by the customer.

6. Packaging, transportation and storage

a) The packing box shall meet the requirements of moisture-proof and shock-proof. The packing box shall have packing list, inspection certificate and product manual, etc.;

b) During the transportation process, avoid throwing, sun and rain, and avoid the mixed transportation of corrosive substances;

c) The product should be stored in a cool, ventilated and dry warehouse, prohibited from sharing with oil substances, away from heat sources. When stacking, keep the equipment 20cm away from the ground and 20cm away from the wall.

7. Legal Statement

1. The contents of this document may not be published, copied or used for any purpose, in whole or in part, without permission. We reserve the right to modify any information in this manual at any time/without prior notice and without liability.

2. In order to avoid the possible impact of improper use of satellite navigation frequencies on the flight safety of aircraft, solemnly remind: Please be sure to configure and use the product in strict accordance with the relevant national and local laws and regulations. Any adverse consequences and legal liabilities resulting from violation or illegal use of the product shall be borne by the customer.

Drone detection defense system