

Fixed unmanned aerial vehicles for checking and combating



PrefacePreface

The UAV detection and defence system is a low altitude security system that adopts the Cognitive Radio Protocol Cracking (CRPC) technology to solve the problem of domestic and foreign civil UAV detection, identification, orientation and defence.

It is a low-altitude security system that solves the problem of detecting, identifying, orienting and defending domestic and foreign civil drones. The system can detect, identify, omnidirectionally jam or accurately strike the UAVs in the protected area, which is widely used.

The system can detect and identify UAVs in protected areas, interfere with them in all directions or strike them accurately, and is widely used in the low-altitude security defence of public security, airports, prisons, important facilities, large venues and venues for major events.

Cognitive radio protocol reverse analysis technology is the fourth-generation UAV defence method, which monitors the radio environment in the target defence zone through antenna arrays, and conducts 24-hour round-the-clock monitoring of the radio environment in the target

defence zone.

The technology monitors the radio environment in the target defence zone through antenna arrays, collects radio signals in the defence zone 24 hours a day, and transmits the collected signals to the signal processing unit for precise demodulation and reverse parsing of the drone signals.

The collected signals are transmitted to the signal processing unit for precise demodulation and inverse analysis of the UAV signals, after which the analysed UAV signals are transmitted to the data server through the network, which identifies the enemy and us and guides the jamming module to identify the enemy and us.

The data server identifies the enemy and guides the jamming module to strike and defend against the UAV.

I. Introduction

The UAV detection and defence system is a low-altitude security system that adopts Cognitive Radio Protocol Cracking (CRPC) to solve the detection, identification, orientation and defence of domestic and foreign civil UAVs. The system can detect and identify drones in protected areas, carry out omni-directional jamming or precision strikes, and is widely used in low-altitude security defence for public security, airports, prisons, important facilities, large venues and major event venues.

Cognitive radio protocol reverse parsing technology is the fourth generation of drone defence method, which monitors the radio environment in the target defence zone through antenna arrays, collects radio signals in the defence zone 24 hours a day, and transmits the collected signals to the signal processing unit, which accurately demodulates and reverse parses the drone signals, and then transmits the analysed drone signals to the data server through the network, and the data server analyzes the received signals and analyses them. After that, the analysed UAV signal is transmitted to the data server through the network, and the data server identifies the enemy and us on the received UAV signal and guides the jamming module to the UAV. Fixed UAV detection and countermeasure equipment is a fixed-rack form of UAV detection equipment equipped with a comprehensive UAV control system. Through in-depth analysis and data mining of drone signals, the device can monitor the serial number, model, location (latitude, longitude, azimuth), speed, altitude, altitude, take-off point, return point, trajectory, remote control position (latitude, longitude, azimuth) and other multi-dimensional information of the drone within the monitoring range.

The equipment is suitable for low-altitude security in political core areas, border guards, restricted military areas, military management areas, power and petrochemical parks and airports, etc. It can work offline on a stand-alone basis, and can be flexibly and rapidly deployed and responded to in a mobile manner to meet the needs of all kinds of scenarios; and it can form a tight low-altitude protection network. It can also be used for strike defence.

Performance Indicators

No.	Indicator	Parameters	Notes
1	Detectable Frequency Range	2.46, 5.86	
2	Scanning Time	≤0.25s for 120M bandwidth scanning	
3	Detection Distance	1~3km	Affected by environment and aircraft type
4	Detectable Aircraft Types	500+ (Common models: DJI Avata 2, mini4pro, Autel EVO II pro v3, EVO filter, etc. 220+; Custom/FPV drones 110+; WiFi drones like UDI, Wuxiang, Sima, etc.)	Expandable
5	Locatable Aircraft Types	Partial DJI models	
6	Rapid Detection Performance	≥3km detection/location distance for brand/model drones in unobstructed airspace	
7	Trajectory Detection	≥3km detection/location distance for brand/model drones in unobstructed airspace	
8	Minimum Detection Altitude	0m	
9	Detection Azimuth Angle	<15°	
10	Recognition Time	≤1s (Time to identify drone brand, model, and ID)	
11	Recognition Capacity	≥20 drones per single recognition cycle	
12	Connection Method	Ethernet/WiFi hotspot	
13	Operating Temperature	-40°C ~70°C	
14	Power Supply	AC 200V	
15	Whitelist/Blacklist	Supported	
16	HD GIS System	Displays perimeter environment, device info, etc.	
17	Log & Playback	Drone logs with angle, alarm time, frequency info; record retrievable	
18	Statistical Reports	Visualized drone intrusion reports with audio/light alarms	
19	Positioning	GPS positioning; location marked on map	
20	Auto-Calibration	System auto-calibration	
21	Weight	Single module ≤15kg; Single reflector ≤22kg	
22	Operating Time	7 月 24 日	
23	Software Compatibility	Supports DJI series and upgradable for other brands	
24	Operating Mode	Spectrum + Data Band Protocol Analysis; Radio-silent monitoring, real-time automatic detection, no electromagnetic radiation, compatible with EM-sensitive areas.	
25	Features	Precise drone localization	
26		Precise recognition of drone serial numbers	
27	Positioning Innovation Time	≤3-10s	

28	Operating System	Android/Windows system	"Windous" corrected to "Windows"
29	Protection Level	IP68	
30	Display	Tablet or laptop-sized screen	
31	Detection Sensitivity	Better than -96dBm (25kHz)	
32	Frequency Accuracy	$\leq 1\text{kHz}$	
33	Laser Time	$\leq 3\text{min}$	
34	Detection Success Rate	99%	
35	Anti-Spoofing Range	$\geq 2\text{km}$	
36	Response Time	$\leq 1\text{s}$	
37	Performance Testing	≥ 3 units	
38	Interference Mode	Distance and area-based	
39	Anti-Spoofing Success Rate	$\geq 99\%$	
40	Reflector Operating Band	Output terminal; Average output power (Total reflector power: 350W)	
41	Anti-countermeasure operating frequency bands	400-450MHz	30w
42		1550-1650MHz	50w
43		2300-2500MHz	50w*4
44		5150-5300MHz	50w
45		5150-5300MHz	
46	Makings	Aluminium alloy + high performance FRP	
47	Antenna Type	Multi-dimensional composite signal wave modulation	
48	Self-defence	Unattended operation	
49	System Integration	Provides expansion interfaces for integration with jamming devices	

Schema



Equipment Components

No.	Equipment Name	Quantity	Description	Form Factor	Notes
1	Fixed checking and typing all-in-one equipment	1	Main equipment unit	Fixed installation	
		1	Power and network connection	Cable	
		1 set	Antenna array for the main unit	Modular array	
		1	Power supply cable	Standard cable	

III. Installation deployment

3.1 Check the equipment list

Before equipment assembly and erection, according to the equipment packing list check all the spare parts, standard parts of the specifications, the number, read the Read and understand the equipment user manual and other supporting information, and familiarise yourself with the main points of equipment installation.

3.2 Survey and selection of site

The equipment is usually deployed outdoors, and adequate site investigation should be carried out before equipment installation and deployment. The following factors should be noted in site survey.

Factors:

(1) Visual environment: it should have better visual conditions, and generally choose flat and open highland, or the top of the building.

The top of the building can also be selected;

(2) Electromagnetic environment: Try to avoid microwave stations, radio transmission towers, high-voltage towers through the electromagnetic environment, and other

(2) Electromagnetic environment: Try to avoid electromagnetic environment interference zones such as microwave stations, radio transmission towers, high-voltage line tower crossing zones, as well as features that are prone to multipath effects;

(3) Natural environment: try to avoid the wind in order to reduce the wind load of the equipment antenna; for the area of thunderstorms, avoid waterlogged areas and locations prone to lightning strikes.

(4) Electrical environment: Try to avoid the wind to reduce the wind load of the equipment antenna;

(4) Electrical environment: try to avoid electrified railway and other areas that are prone to communication interference;

(5) Basic security: stable, safe and reliable power supply in the vicinity to support access to public or private communication networks;

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

3.3 Equipment Host Deployment

The equipment can be deployed according to the specific use scenario, choose fixed installation or mobile vehicle deployment.

1. Ground installation and fixation, install the four supporting feet of the equipment on the bottom of the equipment and choose the model to be installed in the open area without any obstruction. Specific

Specific deployment, can be combined with the existing survey to develop construction programmes.

2. Mode 2: Mobile vehicle deployment mode

According to the system carries a different chassis platform, the use of different installation programmes. The actual deployment should be based on the modification programme of the

vehicle modification factory.

programme shall prevail.

3.4 Host Antenna Installation

(1) Screw the FRP antenna onto the radio processing unit in clockwise direction one by one according to the corresponding interface identified on the antenna and the radio processing unit.

(1) Screw the FRP antenna onto the radio processing unit in clockwise direction one by one according to the corresponding interface identified on the antenna and radio processing unit. The antennas for detecting and striking in the same frequency band can be used in common, while the antennas for detecting and striking in different frequency bands cannot be used in common. can be common.

(2) Connect one end of the waterproof cable to the radio processing unit, and the other interfaces are for spare or subsequent upgrading of the equipment.

(2) Connect one end of the waterproof special cable to the radio processing unit, and the other interfaces are for spare or subsequent upgrading of the equipment.

Note: Different equipment may be slightly different, when connecting the antenna, you must connect the antenna and the radio processing unit according to the interface identification.

Otherwise, the radio processing unit will be damaged when the system is switched on.

3.5 Deployment of Charge Terminal

The accusation terminal is usually deployed in the customer's security centre or duty room, and can be connected to the main unit through the waterproof special network cable.

It can be connected with the host of the equipment through the waterproof special network cable, and the display can also be projected to other kinds of display terminals such as the accusation platform through the HDMI cable.

3.6 Power network access

(1) Network access. Optical fibre or standard network cable can be used through the TCP/IP interface to connect the radio processing unit with the accusation terminal.

The radio processing unit can be connected to the accusation terminal through the TCP/IP interface by means of optical fibre or standard network cable, or the data server can be connected to the Internet by means of wireless connection.

(2) Power supply access. The radio processing unit, 220V AC power, can be accessed by fixed power supply or UPS.

It is enough to reserve 220V fixed power supply or deploy UPS power supply in the deployment place.

Note: UAV detection and defence system is wired network access by default, if you need to configure wireless network access, you need to contact the local network operator in advance. If you need to configure wireless network access, you need to contact the local network operator in advance for wireless network access service.

IV. System login instructions

4.1. Direct connection mode of network cable:

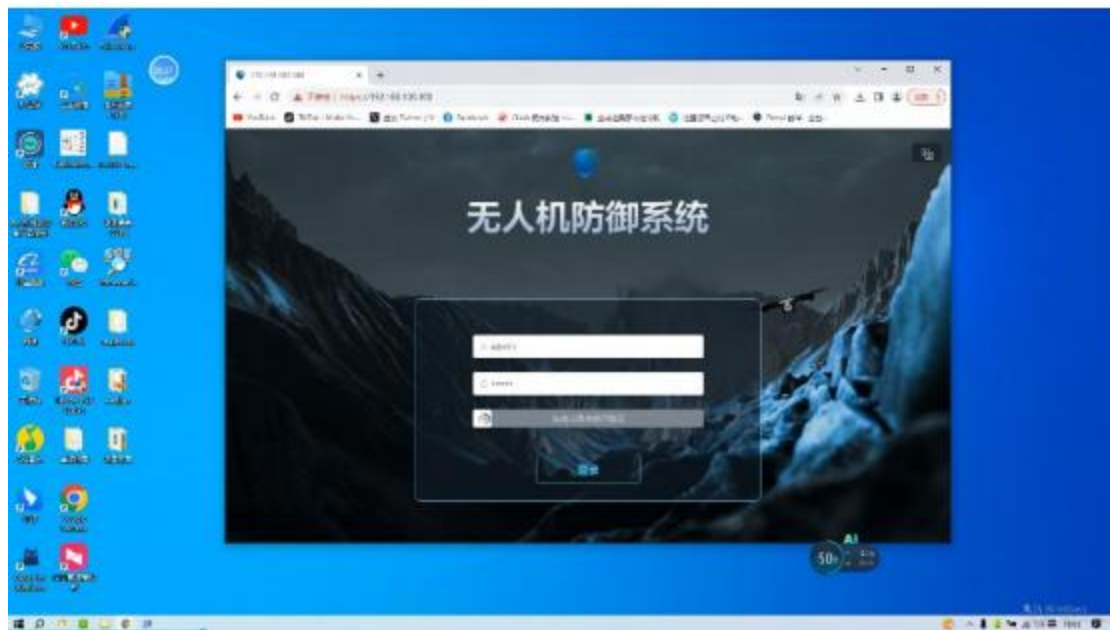
(1) Computer and fixed device RJ45 network port connected through the network cable.

(2) The computer opens the network settings, will connect to the device's network port network segment configuration for 192.168.100.xxx Note that

Do not set and fixed device IP address duplication

(3) Computer open the browser, visit the URL: 192.168.100.100 can be

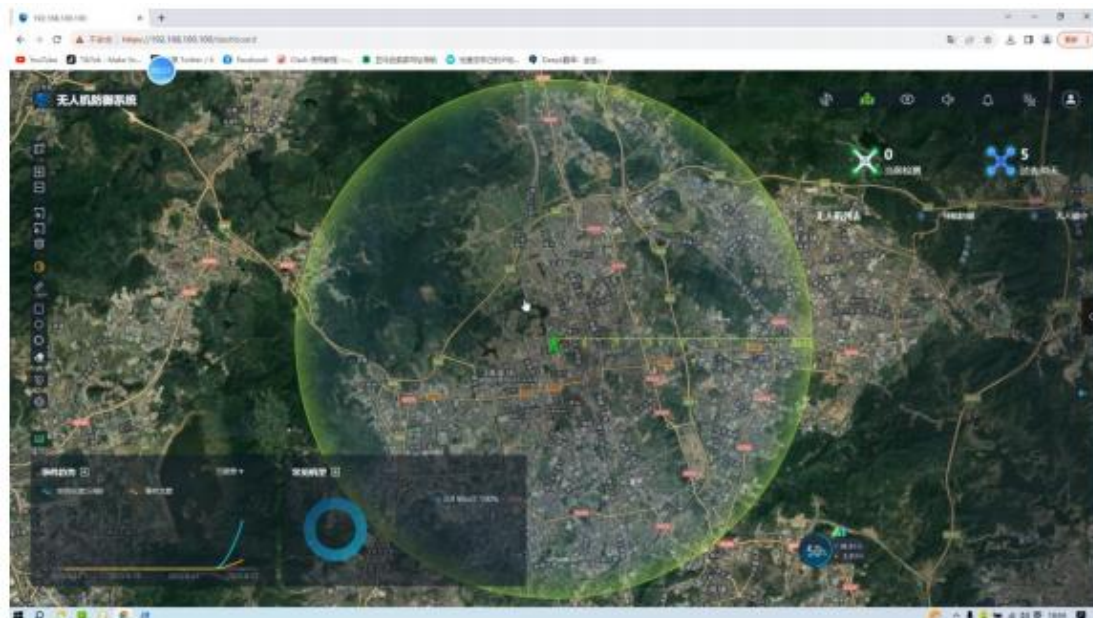
(4) System interface



(5) Login interface

After entering the account number (demo) and password (secret) in the login interface, you can enter the main interface of the system (matching account number and password can be obtained from the supplier).

(Please ask the supplier for the account number and password).



4.2 Software main interface

The main interface of the software has three main functional divisions according to the distribution orientation, i.e. the left side functional menu area, the lower side functional menu area, and the right side information display control area.

(1) Left side function menu area

The main functions of the function button area include map display control, defence and control

partition setting, etc. Users can choose to click the corresponding function buttons for operation according to their needs.



(2) Lower Function Menu Area

The main functions of the lower side function button area include historical event query, whitelist query, UAV information statistics, equipment management, version and account settings, etc. Users can choose to click on the corresponding function buttons for operation according to their needs.



3) Right side information display control area

The main functions of the information display control area include the hiding/displaying of the menu bar of the main interface, volume adjustment, notification switch, Chinese/English switching, system login/exit, etc. Users can choose to click on the corresponding function buttons to operate according to their needs.



In addition, this area mainly undertakes the function of displaying and controlling real-time drone detection information, which can display information on the number of currently detected and historically detected drones, as well as detailed information on the currently detected drones.

4) Drone Detection

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



5) Start Strike

Users can manually select the specified jamming frequency band according to the actual situation to carry out 'broadband jamming' or 'precision strike' on the UAV.



6) Strike cancellation

By clicking the ‘Cancel Strike’ button on the software interface, the device will cancel the drone strike.



7) Unattended Mode

When unattended mode is turned on, once the system detects a drone, it will automatically identify and filter the ‘white list’ list of drones, and turn on ‘precision strike’ or ‘broadband jamming’ for ‘black list’ drones, until the strike is automatically cancelled after no more alarms are raised. ‘Wideband jamming’, until the alarm is no longer activated, then the strike will be cancelled automatically, and the strike process can be cancelled manually.



8) Setting Whitelist

After the system detects a drone, open the drone list to expand the menu and click Add/Move Out Whitelist.



(9) Attribute information labelling

After the system detects the drone, open the drone list to expand the menu, click 'Attribute' to open the attribute setting page, you can set the information or name of the specified drone according to the customer's needs.



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



10) View Historical Events

Move the mouse to the 'Function Menu Bar' on the bottom left side of the software and click 'Events' to enter the list of historical UAV events, view the time of discovery, duration, model and UAV ID, working frequency band and other information, the list also supports to expand or merge by 'Time' or 'Model', as shown in the figure below. The list can be expanded by 'time' or merged by 'model', as shown in the following figure. This function supports expanding/merging by 'Event Trend' in the main interface.



11) View Whitelist

Move your mouse to the ‘Function’ menu bar on the bottom left side of the software, and click ‘Whitelist’ to enter the whitelist interface to manage whitelisted drones.



12) View statistical reports

Move the mouse to the ‘Function Menu Bar’ on the bottom left side of the software, click ‘Statistics’ to enter the statistics interface, you can view the statistical report of drone events, including the number of drone sightings, common models, invasion time, drone event development trend and other information. Meanwhile, this function supports expanding/consolidating the ‘Common Samples’ in the main interface with one click.



13) View Device Status

By clicking the ‘Device Management’ button, you can instantly view and monitor the basic information about the operating status of controllers, computing engines, and sensors.



- **Controller Status View.** Allows you to view controller operational status, online time, and configuration files.
- **Compute Engine View.** You can view the compute engine running status, online time, temperature, and version, as well as the send/receive packet status.
- **Sensor Status.** You can view the running status, online time, software version and other information of the two sensors, as well as the configuration files.
- **Jammer Status.** You can view the operational status, online time, fault status, GPS status, etc. of the two jammers, as well as the configuration file. You can view the operating status of the two jammers, online time, fault status, GPS status, software version and other information, as well as the configuration file.

Note: If there is a device failure, click on ‘Device Failure’ and follow the prompts or consult an after-sales representative.

14) Account Settings

Click ‘Account Settings’ button, users can change the password and add users.



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

V. Basic Troubleshooting

- a) Verify that the computer is on and that the test terminal and all components are powered;
- b) Ensure that all cables are securely connected to the appropriate ports;
- b) Ensure that all cables are securely connected to their respective ports. c) Ensure that feeder, power, and network cable cables are not damaged or frayed;
- d) Ensure that the pins of the connecting plugs are not bent or damaged;
- e) Restart the computer and check if the problem persists;
- f) Unplug the terminal device and wait 30 seconds, then try plugging it back in;
- g) After the server and the testing terminal device are switched on, make sure that the 'Device Management' process (controller, controller, terminal device, etc.) in the server interface is working properly.
- g) After the server and the testing terminal equipment are switched on, confirm whether the 'device management' processes (controller, computing engine, sensor) in the server interface are working normally;
- h) Whether the network connection between the testing device and the service terminal is normal;
- i) If the problem still cannot be solved, please contact our technicians and do not dismantle the chassis privately.

VI. Precautions for use

a) Confirm that the strike and detection antennas of the detection terminal equipment are connected normally before powering on, and it is strictly prohibited to power on the equipment before installing the detection and strike antennas.

It is strictly prohibited to power on the device before the detection and strike antennas are installed;

b) If the server stops running due to power failure, please turn on the power switch again, switch on the server and start the service.

The service can be restored to normal operation;

c) In order to ensure the normal operation of the equipment, it is recommended that please do not install other software not related to the operating system on this display terminal, such as the software system caused by the customer's arbitrary installation of software.

c) To ensure the normal operation of the equipment, it is recommended that you do not install other software on this display terminal that is not related to the operating system;

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

e) This product is a highly technical equipment, if the system fails in the process of use, you should notify our after-sales service department in time.

e) This product is a highly technical equipment, if the system malfunctions during use, you should notify our after-sales service department in a timely manner, do not disassemble it at will, so as not to damage the internal structure or improper operation and damage your rights and interests;

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

f) Please use this product within the scope permitted by national laws and regulations.

VII. Packaging, transport and storage

- a) The packing box meets the requirements of moisture-proof and shock-proof, and the packing box should have packing list, inspection certificate and product specification.
- b) In the process of transport, it should be
 - b) In the process of transport, avoid dropping, sunshine and rain, and avoid mixing of corrosive substances;
- c) The products should be stored in a cool, ventilated and dry warehouse, prohibited from being put together with oil substances and kept away from heat sources. Stacking should be
 - Keep the equipment 20cm from the ground and 20cm from the wall.

VIII. Legal Notice

1. The entire contents of this document may not be published, reproduced, 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.

We reserve the right to amend 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 safety of aircraft flights, we would like to remind you that you must strictly follow the national and local laws and regulations on the use of satellite navigation frequencies.

You must configure and use this product in strict accordance with relevant national and local laws and regulations. If any adverse effect is caused by the illegal use of this product, please contact us.

Any adverse consequences and legal liabilities caused by the illegal or non-legal use of the product shall be borne by the customer himself/herself.

Drone Detection and Defence System