# Anti-Drone System with Multiple Surveillance Technologies: Architecture, Implementation, and Challenges

Xiufang Shi, Chaoqun Yang, Weige Xie, Chao Liang, Zhiguo Shi, and Jiming Chen

The authors provide a comprehensive overview of the technologies utilized for drone surveillance and the existing anti-drone systems. They develop an anti-drone system at Zhejiang University, named ADS-ZJU, which combines multiple passive surveillance technologies to realize drone detection, localization, and radio frequency jamming.

## Abstract

In recent years, drones have undergone tremendous development. Due to the low price and ease of use, drones have been widely utilized in many application scenarios, which potentially pose great threats to public security and personal privacy. To mitigate these threats, it is necessary to deploy anti-drone systems in sensitive areas to detect, localize, and defend against the intruding drones. In this article, we provide a comprehensive overview of the technologies utilized for drone surveillance and the existing anti-drone systems. Then we develop an anti-drone system at Zhejiang University, named ADS-ZJU, which combines multiple passive surveillance technologies to realize drone detection, localization, and radio frequency jamming. Furthermore, we discuss the challenges and open research issues in such a system.

## Introduction

Drones, that is, small unmanned aerial vehicles (UAVs), are experiencing explosive growth nowadays, and they have been widely used in many areas (aerial photography, traffic monitoring, disaster monitoring, etc.). They have attracted much research interest with regard to path planning, secure communication, attack detection, and so on [1–4].

Nevertheless, the increasing use of drones poses great threats to public security and personal privacy. For example, an attacker might strap explosives or other dangerous materials to a drone to carry out an attack; criminals can use drones to smuggle illicit materials across borders; an operator can control a drone carrying a high-fidelity camera to fly over walls and spy on inhabitants' private information. The increasing frequency of incidents caused by drones makes it necessary to regulate drone air traffic. A few drone manufacturers (e.g., DJI) have embedded geofencing software into their drones to prevent them from flying over security-sensitive areas (government buildings, airports, etc.). However, it is unrealistic for geofencing to cover every place and every drone. Therefore, it is of great significance to deploy an anti-drone system in a geofencing-free but security-sensitive area. Such an anti-drone system is able to detect a drone at the time it flies into a sensitive area and estimate its location for drone defense (e.g., jamming, hunting, or control of the detected drone).

However, due to the drones' small size and low flying speed at low altitude, drone surveillance is a challenging task, and many technologies, such as radar surveillance, audio surveillance, video surveillance, and RF surveillance, have potential for drone detection and localization. Each technology has its strengths and weaknesses. A few anti-drone systems have been developed based on one or several of these technologies. The performance of these systems relies on the utilized technologies, while their application scenarios also vary with the utilized technologies. Moreover, not all the existing systems can simultaneously realize drone detection, localization, and defense.

In this article, we comprehensively review a few of the most widely used technologies in drone surveillance and some existing anti-drone systems. Then we build up an anti-drone system by fusing multiple surveillance technologies to conduct drone detection, localization, and RF jamming. Furthermore, challenges and open research issues are discussed.

## Surveillance Technologies and Anti-Drone Systems

### Surveillance Technologies

**Radar:** Radar is a useful tool for detection and tracking of large aircraft, but it faces severe challenges in detecting and tracking drones, since drones have a low radar cross-section and usually fly at low speed and low altitude.

Even so, radar surveillance is promising in detecting and tracking drones. It has been verified that by analyzing the micro-Doppler signatures obtained by multistatic radar, clutter/target discrimination can be improved, which enables drone detection and tracking with high accuracy [5]. Moreover, a series of experiments with a DJI Phantom 2 showed that the detection range of radar hardly exceeds 3000 m [6]. It should be noted that radar is one kind of active sensor that operates all day and night with high electromagnetic energy. Therefore, it might be inappropriate or even forbidden to deploy high-power radar in crowded urban areas.

**Audio:** During the flight of drones, the sounds

This work was supported in part by NSFC under grant No. 61772467 and No. U1401253, and the Fundamental Research Funds for the Central Universities (2017XZZX009-01).

Digital Object Identifier: 10.1109/MCOM.2018.1700430

*The authors are with Zhejiang University.*



0163-6804/18/$25.00 © 2018 IEEE

| Surveillance technology | Drone signature | Localization/tracking method | Detection range | Challenges |
|---|---|---|---|---|
| Radar | Micro Doppler | Doppler-based tracking<br>delay-based localization | ≤3000 m | Low radar cross section<br>Low speed and altitude |
| Audio | Time-frequency feature | DOA-based localization | 40–300 m | High ambient noise |
| Video | Appearance feature<br>Motion feature | Motion-based tracking | 100–1000 m | Occlusion<br>Indistingushable small objects |
| RF | Communication channel | RSS/DOA-based localization | ≤1000 m | Ambient RF noise<br>Multipath<br>Non-line of sight |

**Table 1.** Comparison of drone surveillance technologies.

Radar is a useful tool for detecting and tracking of large aircraft, whereas it faces severe challenges in detecting and tracking drones, since drones have a low radar cross section and usually fly with low speed at low altitude. Even so, radar surveillance is promising in detecting and tracking drones.

generated by the motors and fast rotating propellers can be utilized in detection, classification, and localization of drones by a system equipped with acoustic sensors. The acoustic signatures of drones can be obtained via analysis in both the time and frequency domains.

To get the location of the detected drone, the direction of arrival (DOA) of the acoustic signals can be estimated using array signal processing algorithms, such as Multiple Signal Classification (MUSIC) and beamforming. Audio surveillance systems have low implementation cost. However, audio surveillance is sensitive to ambient noise and suffers from a limited detection range, which depends on the drone type and testing environment. For instance, Christnacher *et al.* developed a network of tetrahedron acoustic arrays, whose largest detection ranges for different drones were 150 m for a customized drone, 150 m for an RC-Blade350 QX UAV, and more than 250 m (up to 300m) for a DJI Phantom 2 [7].

**Video:** Drone detection based on video images is essentially an object detection problem in the area of computer vision and pattern recognition. An object can be detected based on its appearance features [8] (colors, contour lines, geometric forms or edges, etc.) or/and its motion features across consecutive frames [9]. Appearance-based methods have great difficulty in distinguishing drones from other similar small objects (e.g., birds) in cluttered backgrounds without motion information. By comparing consecutive images, the position and moving direction of a moving object can be determined by motion-based methods, which are also utilized for object tracking. It was suggested to distinguish a drone from birds by looking at the flight patterns, since a bird will fly in a more random pattern than a drone will. However, this method might fail when the bird is gliding. For drone detection, it is promising to combine both motion features and appearance features, which would enable detection with higher accuracy. On the other hand, even though object detection and tracking based on video images have been well investigated, they still suffer from many issues (e.g., occlusions) that also exist in drone detection and tracking.

**RF:** The existing drones in the market or customized drones usually communicate with their controllers at some specific frequency bands, such as 2.400–2.483 GHz and 5.725–5.825 GHz for DJI Phantom 4. However, in a practical environment, the existence of many other RF signals (e.g., WiFi), which share the same frequency band with the drones, makes RF-based drone detection challenging. One simple way is to monitor a wide range of RF, such as 1 MHz–6.8 GHz in [10], and take any transmitter of unknown RF signals as a drone. This method will induce a high probability of false alarms, since an unknown RF transmitter is not necessarily a drone. Identifying the media access control (MAC) address of a drone is also a feasible method [11]. However, this method is only capable of detecting drones with open MAC addresses. As there is an ever increasing variety of drones, it is getting more difficult to build and update a comprehensive database of drones' MAC addresses. Moreover, to avoid being detected, a drone's MAC address can easily be spoofed. It is promising to extract the spectrum feature of the RF signals, which can be taken as the RF signature of a drone and is distinguishable even in urban environments [12]. With regard to drone localization based on RF signals, localization methods based on received signal strength (RSS) and DOA measurements are applicable; however, as is well known, it is necessary to take multipath and non-line-of-sight propagation into consideration.

Table 1 summarizes the above-listed surveillance technologies. It should be noted that the detection ranges are obtained from the literature and existing systems, and they might vary with the type of drones, the surveillance environments, the hardware parameters, and the corresponding algorithms.

## Anti-Drone Systems

In the literature, there are already several commercial/military anti-drone systems. Orelia Drone-Detector[1] is an audio-based detector, and is able to detect both fixed-wing and rotary-wing drones. Its detection range can reach 100 m when the background noise is less than 40 dB. Another system, DroneDetector,[2] which was developed by Dronelabs, utilizes audio and RF surveillance for drone detection, and its detection range is reported to be 1 km. Dedrone[3] has several products including DroneTracker, RF sensor, Drone Jammer, and more. DroneTracker combines microphones, optical cameras, and WiFi sensors, and it can detect a drone within 500 m. RF sensor can detect all drones connected through RF and WiFi within 1 km. Drone Jammer transmits RF

[1] http://www.drone-detector.com/en/, accessed on July 18, 2017.

[2] http://www.dronedetector.com/compare-detection-systems/, accessed on July 18, 2017.

[3] https://www.dedrone.com/en/dronetracker/drone-detection-hardware, accessed on July 18, 2017.

With regard to the realized functions, all of them can realize drone detection; some of them can realize both detection and localization; only two of them, i.e., Falcon Shield and AUDS, can simultaneously realize detection, localization and defence. Both Falcon Shield and AUDS have taken advantage of radar surveillance, which however is unsuitable to deploy in urban areas for all day and night monitoring.

| System | Surveillance technology | | | | Function | | |
|---|---|---|---|---|---|---|---|
| | Radar | Audio | Video | RF | Detection | aLocalization | Defense |
| Orelia Drone-Detector | No | Yes | No | No | Yes | No | No |
| DroneDetector | No | Yes | No | Yes | Yes | No | No |
| Dedrone | No | Yes | Yes | Yes | Yes | No | Yes |
| ARDRONIS | No | No | No | Yes | Yes | Yes | No |
| DroneShield | Yes | Yes | Yes | Yes | Yes | No | Yes |
| Falcon Shield | Yes | No | Yes | Yes | Yes | Yes | Yes |
| AUDS | Yes | No | Yes | No | Yes | Yes | Yes |
| **ADS-ZJU** | **No** | **Yes** | **Yes** | **Yes** | **Yes** | **Yes** | **Yes** |

**Table 2.** Comparison of anti-drone systems.

signals at multiple frequency bands via omnidirectional antennas to disrupt the drone communication. ARDRONIS,[4] which was developed by Rohde & Schwarz, is based on RF surveillance. For drones using frequency-hopping spread spectrum (FHSS) and direct sequence spread spectrum (DSSS) transmission systems, ARDRONIS builds an RF library for drone detection. The detection range of ARDRONIS can be up to 1–2 km, depending on RF transmission power, radio condition, and antenna gain. Apart from drone detection, ARDRONIS can realize localization of both the drone and its operator via direction finding. DroneShield[5] provides an integrated detection and defense solution. It utilizes radar, audio, video, and RF surveillance for drone detection with nominal detection ranges of 1.5 km for radar, 200 m for audio, 600 m for video, and 1 km for RF. Regarding drone defense, DroneShield also uses RF jamming to cease the video transmission from the drone back to its operator. The nominal maximum jamming distance is 2 km. Falcon Shield[6] utilizes three surveillance technologies (i.e., radar, video, and RF), and can realize drone detection, localization, and defense. However, the maximum effective range is unclear. AUDS[7] combines radar and video surveillance. With radar, AUDS can detect a drone with a distance up to 3.6 km. With RF inhibition, AUDS can defeat drone communication at multiple frequency bands, such as 433 MHz, 915 MHz, 2.4 GHz, 5.8 GHz, and GNSS bands.

Table 2 summarizes the utilized surveillance technologies and realized functions of each system. We can see that most of these systems take more than one surveillance technology, since multiple surveillance technologies can provide much more information for drone detection and localization. With regard to the realized functions, all of them can realize drone detection; some of them can realize both detection and localization; but only two of them, Falcon Shield and AUDS, can simultaneously realize detection, localization, and defense. Both Falcon Shield and AUDS have taken advantage of radar surveillance, which, however, is unsuitable to deploy in urban areas for all day and night monitoring.

Motivated by the above observations, our objective is to develop a system that is suitable to deploy in urban areas and can promptly detect, localize, and defend against intruding drones.

## Implementation of an Anti-Drone System: ADS-ZJU

In this section we develop an anti-drone system called ADS-ZJU, which combines three surveillance technologies: audio, video, and RF. Figure 1 shows the architecture of ADS-ZJU, which consists of four parts: a heterogenous sensing unit, a central processing unit, an automatic jamming unit, and a real-time display unit. In the following, we introduce each part in detail and take surveillance of DJI Phantom 4 as an example to show how each part works.

### Heterogenous Sensing Unit

In the heterogenous sensing unit, as shown in Figs. 2a–2c, three kinds of sensors are adopted to capture the information for drone detection and localization:

- The utilized acoustic sensor is a Type CHZ-213 1/2-inch free-field microphone with a Type YG-201 preamplifier. We build up L-shape acoustic arrays with four acoustic sensors uniformly installed along each side.
- The utilized optical camera is a HIKVISION DS-2DF7330IW Network PTZ camera, which supports 360° horizontal rotation and –2°–90° vertical rotation. It can achieve both automatic and manual focusing.
- The utilized RF sensor is USRP-2955, one kind of software defined radio, which has 4 independently tunable RX channels and can receive RF signals between 10 MHz and 6 GHz.

Acoustic signals, video images, and RF signals will be collected via these sensors and sent to the central processing unit. For the sake of experimental evaluation, ADS-ZJU is deployed on the rooftop of the Information Science & Electronic Engineering (ISEE) building at Zhejiang University. Figure 2e shows the system deployment and sensor locations.

### Central Processing Unit

The central processing unit is the key part of ADS-ZJU. It conducts drone feature extraction, drone detection, and drone localization.

**Drone Feature Extraction:** Drone feature extraction is essential for drone detection. By taking a DJI Phantom 4 as an example, we analyze the drone's features based on the received acoustic signals, video images, and RF signals.

[4] https://www.rohde-schwarz.com/us/products/monitoring-and-network-testing/ardronis/pg_overview_230808.html, accessed on July 18, 2017.

[5] https://www.droneshield.com/view-all-products/, accessed on July 18, 2017.

[6] http://www.us.selex-es.com/-/falconshield, accessed on July 18, 2017.

[7] http://www.blighter.com/products/auds-anti-uav-defence-system.html, accessed on July 18, 2017.

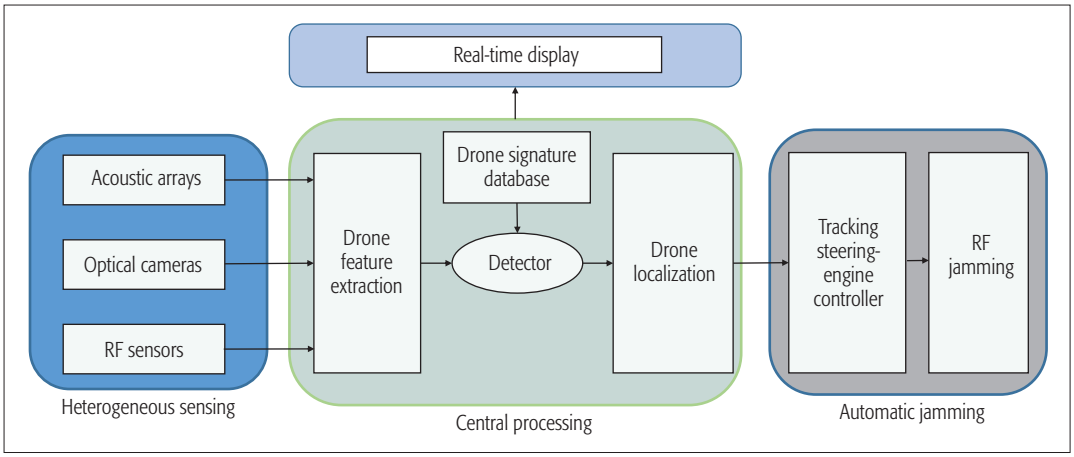


**Figure 1.** Architecture of ADS-ZJU.

Audio detection, video detection and RF detection are conducted in parallel. We consider that missed detection of the intruding drone will bring more security threats than false alarm. Therefore, we use logical "or" operation to fuse the results of the above three detectors and obtain the final decision.

***Acoustic Feature:*** The spectrum feature of the received acoustic signals is extracted via short-time Fourier transform (STFT). Figure 3a shows the STFT result of the acoustic signals generated by a flying DJI Phantom 4. In this figure, different colors represent the strengths of acoustic signals at different frequencies. The unit of the strength values is dB. We can see that the acoustic signals generated by DJI Phantom 4 are harmonic signals with fundamental frequency at about 180 Hz. Strengths of the harmonics are different from each other, but their distribution is quite stable. Therefore, we take the distribution of the harmonics' strengths as the drone's acoustic feature. The feature vector is computed as

$$\left[\frac{e_1}{\sum_{i=1}^{n} ei},\cdots,\frac{e_n}{\sum_{i=1}^{n} ei}\right],$$

where $e_1$, ..., $e_n$ are the strengths of the acoustic signals at the fundamental frequency and harmonics. For example, in Fig. 3a, for the acoustic signals sampled at 10 s, the fundamental frequency and harmonics are 180 Hz, 360 Hz, 540 Hz, 720 Hz, and so on. Then $e_1$, ..., $e_n$ are the signal strengths, i.e., color values, at (10,180), (10,360), (10,540), (10,720), and so on, respectively.

***Image Feature:*** We take histograms of oriented gradients (HOG), one of the most effective appearance feature descriptors in object detection [13], to describe the image feature of drones. Since a drone only occupies a small part of an image, the HOG feature of an image window is utilized in describing the feature of a drone. As shown in Fig. 3b, the red rectangle denotes an image window that is divided into a number of cells, and all the cells form a number of overlapping blocks. The basic procedure of HOG extraction is a standard one, which includes three steps:

1. The gradient of each pixel in the image window is computed by convolving it with the filter kernel [–1, 0, 1] in the horizontal direction and its transpose in the vertical direction.
2. Based on the computed oriented gradients, a histogram for each cell is created by a weighted voting from each pixel within this cell for an oriented-based histogram channel.
3. For the invariance to illumination and shadowing, the histograms of all the cells in each block are grouped together and further normalized into an HOG descriptor. The HOG descriptor for the image window is the concatenated vector of all the blocks' HOG descriptors. For more technical details, the readers can refer to [13].

***RF Feature:*** Preliminarily, we use a basic spectrum analyzer to analyze the feature of communication between DJI Phantom 4 and its controller. We find that when the drone communicates with its controller in the frequency band of 2.4–2.48 GHz, the frequency band is divided into 8 communication channels with bandwidth 10 MHz. In Fig. 3c, the blue line shows that the drone is communicating with its controller at channel 2.44–2.45 GHz, and the yellow line indicates that the communication channel between DJI Phantom 4 and its controller varies among these eight channels. Considering that the bandwidth of WiFi's communication channel is 20 MHz or 40 MHz, which is larger than that of the drone, the spectrum of the drone's RF signal is different from that of the WiFi signal. Therefore, the distribution of the received RF signals' strengths at different communication channels can be utilized to describe the RF feature of the drone. By setting each channel's bandwidth as 10 MHz, we let four of one RF sensor's receiving channels cover the frequency band of 2.4–2.44 GHz and four of the other RF sensor's receiving channels cover the frequency band of 2.44–2.48 GHz. Then the RSS values of 8 channels in the frequency band of 2.4–2.48 GHz can be obtained and denoted by $r_1$, ..., $r_8$. The normalized RSS distribution is taken as the RF feature vector, that is,

$$\left[\frac{r_1}{\sum_{i=1}^{8} ri},\cdots,\frac{r_8}{\sum_{i=1}^{8} ri}\right].$$

**Drone Detection:** The linear support vector machine (SVM) is utilized in drone detection. Before online detection, we first conduct offline training to obtain drone classifiers, which can separate the drone's feature vectors from other objects' feature vectors. We collect a large amount of acoustic signals, video images, and RF signals from both the drone and other objects in


**Figure 2.** Key hardware and deployment of ADS-ZJU: a) acoustic array; b) optical camera; c) RF sensor; d) RF jamming unit; e) system deployment and sensor locations.

the background environment, and extract the corresponding feature vectors. For audio, video, and RF detection, we train three SVM classifiers under supervised learning. Then in the online detection phase, the received acoustic signals, video images, and RF signals will be classified via the corresponding classifier. It should be noted that in video detection, we are dealing with a whole image frame. We use a sliding image window to scan this image frame, and ascertain whether there is an image window whose feature vector is matched with a drone. This process is time consuming. Therefore, to avoid such processing in every frame, we first detect if a moving object appears via the inter-frame difference method, that is, comparing each pixel's gray value between two consecutive frames, which is fast and simple. Then we utilize the trained SVM to identify if the moving object is a drone.

Audio detection, video detection, and RF detection are conducted in parallel. We consider that missed detection of the intruding drone will bring more security threats than false alarm. Therefore, we use logical "or" operation to fuse the results of the above three detectors and obtain the final decision.

**Drone Localization:** If a drone is detected, location-related information will be extracted from the received acoustic signals, video images, and RF signals for drone localization. From the acoustic signals, DOA measurements relative to the L-shaped acoustic arrays can be estimated via the MUSIC algorithm, which is one of the most widely used DOA estimation algorithms; technical details can be found in [14]. From the RF signals, both RSS and DOA measurements relative to the RF sensors can be obtained. From the video images, although it is difficult to precisely estimate the geometrical relationship between the detected drone and the camera, we can determine that the drone flies in a specific geographical area within the scope of camera view, which can be regarded as additional information for drone localization. The location of the detected drone can be estimated via existing localization algorithms [15] based on hybrid measurements including DOA and RSS under the constraints of the specific geographical area coming from video images.

## Automatic Jamming Unit

In ADS-ZJU, we take advantage of RF jamming to defend against drones that fly into a sensitive area. As shown in Fig. 2d, the automatic jamming unit mainly consists of four parts:

1. Two steering engines: One can achieve 360° horizontal rotation, and the other one can achieve 180° vertical rotation.
2. A steering engine controller.
3. A planar directional antenna, whose antenna gain is 14 dBi.
4. An RF signal generator that can generate RF signals at frequency 2.4–2.5 GHz.

When the automatic jamming unit receives the estimated location of the detected drone, it will

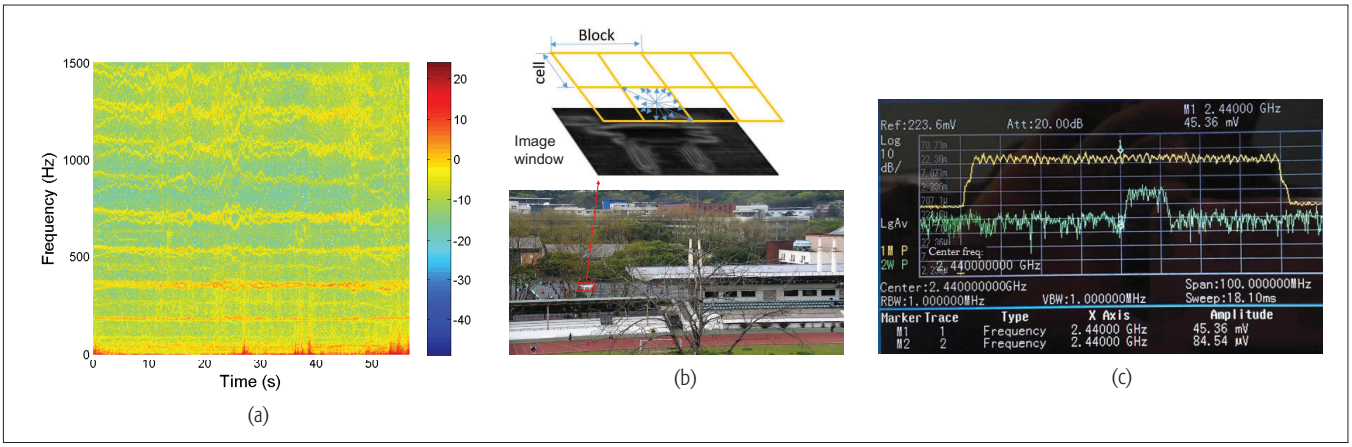


**Figure 3.** Drone (DJI Phantom 4) features extracted from different signals: a) acoustic feature; b) image feature; c) RF feature.

compute a three-dimensional azimuth angle of the drone relative to the panel antenna. Based on this azimuth angle, the steering engines will be controlled by a PID controller and drive the panel antenna in the direction of the detected drone. Then the panel antenna will transmit RF signals and interfere with the communication between the drone and its controller, which will take the drone out of the ground controller's control. It is worth noting that the automatic jamming unit only transmits RF signals when it is necessary to defend against the intruding drones, since arbitrarily transmitting RF signals is dangerous and forbidden in our campus.

### Real-Time Display Unit

The real-time display unit is a liquid crystal display (LCD), which consists of four 46-in subscreens. We can select 1–4 scenes to display the drone surveillance results. As shown in a demo,[8] we can see multiple results from this displayer, including DOA estimates of the acoustic signals, the real-time trajectory of the detected drone, the detection results obtained by video surveillance, the automatic jamming unit that moves toward the detected drone, and so on.

### Performance Evaluation

To test the performance of ADS-ZJU, we have conducted field experiments in our campus with a DJI Phantom 4. We first let the drone fly at different distances and conduct 10,000 detections at each distance to see the corresponding detection probabilities, which are computed as

$$P_D = \frac{N_D}{N_P},$$

where $N_P$ denotes the number of conducted detections at each distance, and $N_D$ denotes the number of accurate detections where the flying drone is successfully detected. Then we conduct 10,000 detections when there is no drone in the environment and see the false alarm probabilities, which are computed as

$$P_{FA} = \frac{N_{FA}}{N_N},$$

where $N_N$ denotes the number of conducted detections when there is no drone in the environment and $N_{FA}$ denotes the number of false alarms. In our experiments, both $N_P$ and $N_N$ equal 10,000.

| Surveillance technology | Detection probability (%) | | | | False alarm probability (%) |
|---|---|---|---|---|---|
| | 20 m | 50 m | 80 m | 100 m | |
| Audio | 87.4 | 76.9 | 50.7 | 21.1 | 2.2 |
| Video | 97.8 | 98.1 | 93.9 | 95.4 | 1.1 |
| RF | 100 | 88.2 | 78.7 | 73.3 | 2.8 |
| Fusion | 98.8 | 99.3 | 94 | 97.3 | 5 |

**Table 3.** Detection performance of ADS-ZJU.

Table 3 shows the experimental results on the detection performance of ADS-ZJU. This table shows that ADS-ZJU can quickly detect the intruding DJI Phantom 4 within 100 m in a campus environment. The detection probability of audio surveillance decreases quickly with the increase of drone-sensor distance due to the impact of background noise; the detection probability of video surveillance stays above 95 percent within 100 m since no occlusion occurs during the experiments; the detection probability of RF surveillance decreases with the increase of drone-sensor distance at a slower rate than that of audio surveillance. By fusing three surveillance technologies, the detection probability becomes higher, while the false alarm probability is also higher.

Apart from DJI Phantom 4, we also tested a DJI Phantom 3 and a Mavic Pro. Both of them illustrate similar results to that of the DJI Phantom 4. The detection result of a DJI Phantom 3 and a Mavic Pro using video surveillance is shown in a demo.[9]

## Challenges and Open Research Issues

Although we have realized basic functions for drone surveillance in our anti-drone system, new challenges have been raised, and there are still some open research issues to be addressed:

**Heterogenous Information Fusion:** The result of drone detection should be more than a simple combination of the results separately obtained by audio, video, and RF surveillance, which will induce great information loss. It is of great significance to develop reliable techniques for the fusion of audio, video, and RF information from the aspect of feature fusion and decision fusion.

**Energy-Efficient Sensor Coordination:** Multiple surveillance technologies sometimes bring

[8] https://www.youtube.com/watch?v=S-AIjuVM-WLk&feature=youtu.be, accessed on Sep. 9, 2017].

[9] https://youtu.be/fPf7WhcKevU, accessed on Sep. 9, 2017].

The result of drone detection should be more than a simple combination of the results separatively obtained by audio, video and RF surveillance, which will induce great information loss. It is of great significance to develop reliable techniques for the fusion of audio, video and RF information, from the aspect of feature fusion and decision fusion.

redundant information. It is unnecessary to let all the heterogenous sensors work all the time and everywhere, which will induce high energy consumption, and high communication and computational load. Dynamical sensor coordination in an anti-drone system has potential for energy savings.

**Signature Database Build-Up:** Nowadays, an ever increasing variety of drones are developed by commercial companies and hobbyists. The features of drones might be different from each other. The aforementioned drone signatures are not enough for detecting more kinds of drones. More signatures and feature extraction methods are required to build up an increasing database of drone signatures.

**Multiple Drones Detection and Localization:** Most of the existing anti-drone systems tackle one drone. When multiple drones appear in the area of interest, one key problem is data association, that is, how to associate the data from heterogeneous sensors with the corresponding drones. Both clutter and similar drones in the environment will bring challenges to data association, and then affect drone detection and localization.

**Power Control of RF Jamming:** The automatic jamming unit transmits RF signals to interfere with the communication between the detected drone and its controller, but this may also interfere with the ambient wireless communications. It remains to be addressed how to control the transmission power of the RF jamming signals so that the detected drone can be effectively defended without interfering with the ambient wireless communications.

## Conclusion

In this article, we give a comprehensive review of four of the most widely used surveillance technologies in drone detection and localization, and also summarize existing anti-drone systems. Then we develop an anti-drone system, called ADS-ZJU, which combines three passive surveillance technologies. Experimental results show that our system can detect and localize the intruding drone in a campus environment. RF jamming to the detected drone is also available if necessary. Furthermore, we discuss the challenges and open research issues in such a system.

## References


[1] H. Sedjelmaci, S. M. Senouci, and N. Ansari, "Intrusion Detection and Ejection Framework against Lethal Attacks in UAV-Aided Networks: A Bayesian Game-Theoretic Methodology," *IEEE Trans. Intell. Transport. Sys.*, vol. 18, no. 5, May 2017, pp. 1143–53.

[2] J. Su *et al.* "A Stealthy GPS Spoofing Strategy for Manipulating the Trajectory of an Unmanned Aerial Vehicle." *IFAC-PapersOnLine*, vol. 49, no. 22, 2016, pp. 291–96.

[3] A. Sanjab, W. Saad, and T. Bas?ar, "Prospect Theory for Enhanced Cyber-Physical Security of Drone Delivery Systems: A Network Interdiction Game," arXiv preprint arXiv:1702.04240, accesssed July 18, 2017.

[4] C. Zhao, J. He, and J. Chen, "Resilient Consensus with Mobile Detectors against Malicious Attacks," *IEEE Trans. Signal Info. Process. Net.*, 2017; http://ieeexplore.ieee.org/abstract/document/8013830/, accessed Sept. 7, 2017. DOI. 10.1109/TSIPN.2017.2742859

[5] F. Hoffmann *et al.*, "Micro-Doppler Based Detection and Tracking of UAVs with Multistatic Radar," *Proc. IEEE RadarConf*, Philadelphia, PA, May 2016, pp. 1–6.

[6] 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.

[7] F. Christnacher *et al.*, "Optical and Acoustical UAV Detection," *Proc. SPIE Security+ Defense*, vol. 9988, 2016, pp. 99880B-1–99880B-13.

[8] Z. Zhang *et al.*, "An Intruder Detection Algorithm for Vision Based Sense and Avoid System," *Proc. IEEE ICUAS*, Arlington, VA, June 2016, pp. 550–56.

[9] S. R. Ganti and Y. Kim, "Implementation of Detection and Tracking Mechanism for Small UAS," *Proc. IEEE ICUAS*, Arlington, VA, June 2016, pp. 1254–60.

[10] DDC, "Domestic Drone Countermeasures"; http://www.ddcountermeasures.com/products.html, accessed Apr. 17, 2017.

[11] M. Peacock and M. N. Johnstone, "Towards Detection and Control of Civilian Unmanned Aerial Vehicles," *Proc. 14th Australian Info. Warfare and Security Conf.*, Edith Cowan Univ., Perth, Western Australia, Dec. 2013, pp. 9–15.

[12] P. Nguyen *et al.*, "Investigating Cost-Effective RF-Based Detection of Drones," *Proc. 2nd ACM Wksp. Micro Aerial Vehicle Networks, Systems, and Applications for Civilian Use*, Singapore, June 2016, pp. 17–22.

[13] N. Dalal and B. Triggs, "Histograms of Oriented Gradients for Human Detection," *Proc. IEEE CVPR*, San Diego, CA, June 2005, pp. 886–93.

[14] H. Tang, "DOA Estimation Based on MUSIC Algorithm," 2014; https://pdfs.semanticscholar.org/5ff7/806b44e60d41c21429e1ad2755d72bba41d7.pdf, accessed Sept. 7, 2017.

[15] S. Wang, B. R. Jackson, and R. Inkol, "Hybrid RSS/AOA Emitter Location Estimation Based on Least Squares and Maximum Likelihood Criteria," *Proc. 26th IEEE QBSC*, Prague, Czech Republic, May 2012, pp. 24–29.


## Biographies


Xiufang Shi [M] (xfshi.zju@gmail.com) received her B.Sc. degree in automation from East China University of Science and Technology in 2011 and her Ph.D. degree in control science and engineering from Zhejiang University, Hangzhou, China, in 2016. Currently, she is a postdoctoral researcher in the College of Control Science and Engineering, Zhejiang University. Her major research interests include wireless localization, target tracking, wireless sensor networks, and statistical signal processing.

Chaoqun Yang (chaoqunyang@zju.edu.cn) received his B.Sc. degree in ocean technology from Xiamen University, China, in 2015. He is currently pursuing a Ph.D. degree with the Department of Information Science and Electronic Engineering, Zhejiang University. His current research interests include multi-target tracking, data fusion, and anti-UAV technology.

Weige Xie (nbfhxwg@gmail.com) received his B.Sc. degree in automation from North China Electric Power University in 2015 and is a Ph.D. candidate in control science and engineering at Zhejiang University. His major research interests include computer vision and machine learning.

Chao Liang (chaoliang@zju.edu.cn) received his B.Sc. degree in automation from Xi'an Jiaotong University in 2015. Currently, he is a Master's degree candidate, doing research at the College of Control Science and Engineering, Zhejiang University. His major research interests include unmanned aerial vehicle systems and anti UAV.

Zhiguo Shi [SM] (shizg@zju.edu.cn, corresponding author) received his B.S. and Ph.D. degrees in electronic engineering from Zhejiang University in 2001 and 2006, respectively. Since 2006, he has been a faculty member with the Department of Information and Electronic Engineering, Zhejiang University, where he is currently a full professor. From 2011 to 2013, he visited the Broadband Communications Research Group, University of Waterloo, Ontario, Canada. His current research interests include networked signal and data processing.

Jiming Chen [SM] (jmchen@iipc.zju.edu.cn) received his B.Sc. and Ph.D degrees, both in control science and engineering, from Zhejiang University in 2000 and 2005, respectively. Currently, he is a full professor with the College of Control Science and Engineering, and vice director of the State Key laboratory of Industrial Control Technology andthe Institute of Industrial Process Control at Zhejiang University. His research interests include cyber security, sensor networks, smart grid, and networked control.