Drones Security and Privacy: Detection Strategies

CPS and IoT Security

Alessandro Brighente

Master Degree in Cybersecurity

UNIVERSITÀ DEGLI STUDI DI PADOVA

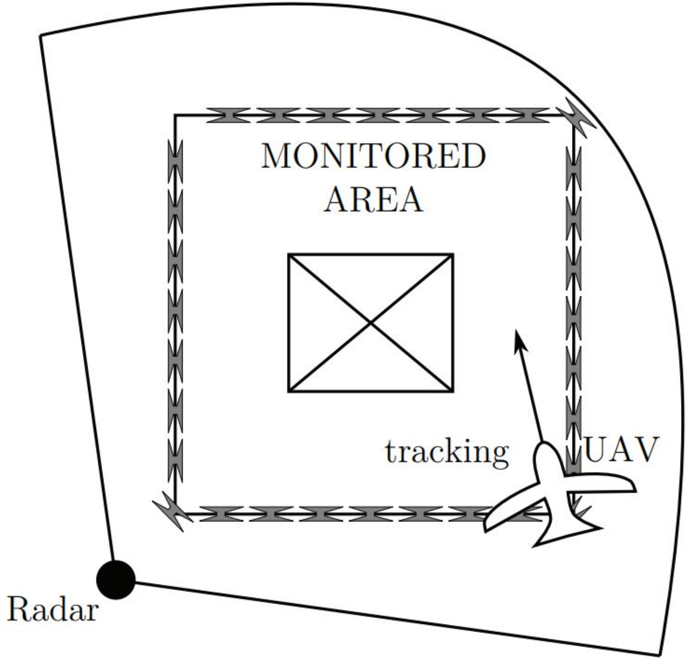
SPRITZ SECURITY & PRIVACY RESEARCH GROUP

Drone Detection

- Detection and tracking represent the first action points in defending against drones
- Detection: recognize that there is a drone nearby
- Tracking: determine the exact location of the drone over time
- Methodologies currently available for detection and tracking include:
  - Radar
  - RF scanner
  - Video and thermal cameras
  - LiDAR
  - Acoustic detection

Radar-Based Detection

- We use very high frequencies (35GHz) to detect the presence of drones
- We assume two modes:
    - Area mode: uses a wide beam for detection, tracking and imaging

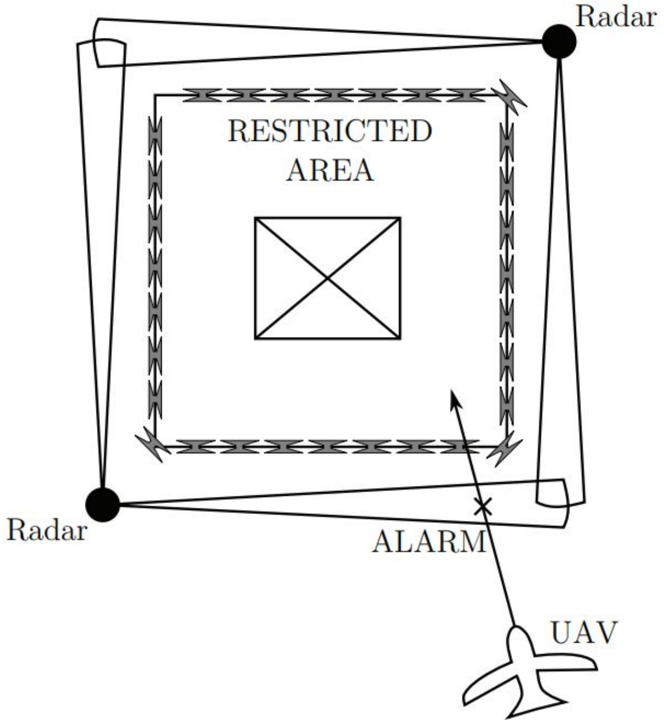


Radar-Based Detection

SPRITZ
Security & Privacy
Research Group

Università
degli Studi
di Padova

- We use very high frequencies (35GHz) to detect the presence of drones
- We assume two modes:
  - Barrier mode: use a narrow beam radar to surveil smaller areas

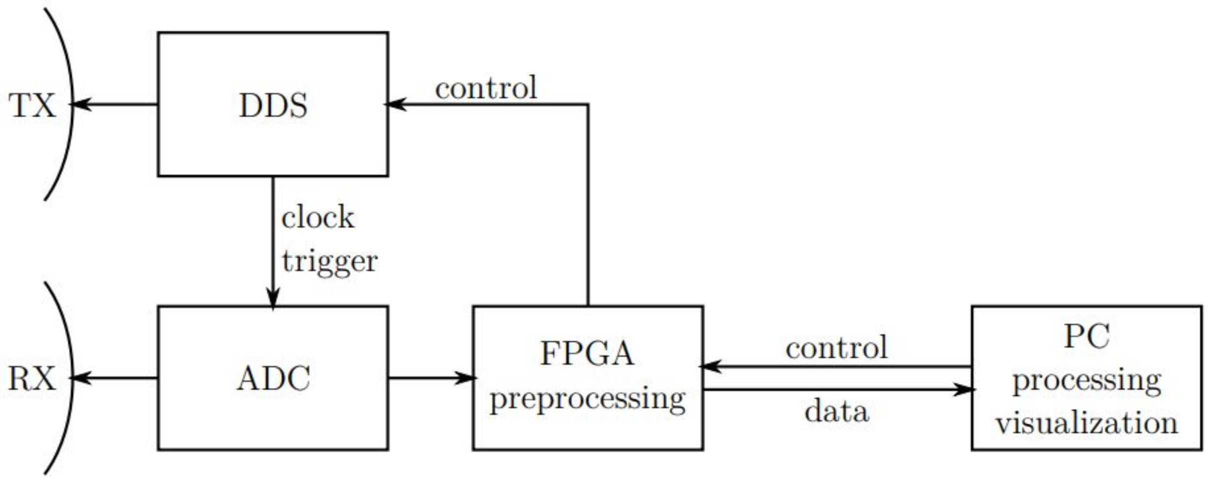


Radar Working Principles

- A radar system has a transmitter that emits radio waves (radar signals) in predetermined directions
- Signals that impinge on an object are usually reflected or scattered in many directions
- Radar signals benefit by high reflectability especially by materials with considerable electrical conductivity
- The reflected signals get to the radar receiver which, based on signal processing techniques, detects/tracks objects

System Diagram

- In the receiving part, processing starts by grouping signals into a block with a chosen integration time
- Then apply signal windowing at 2D-DFT

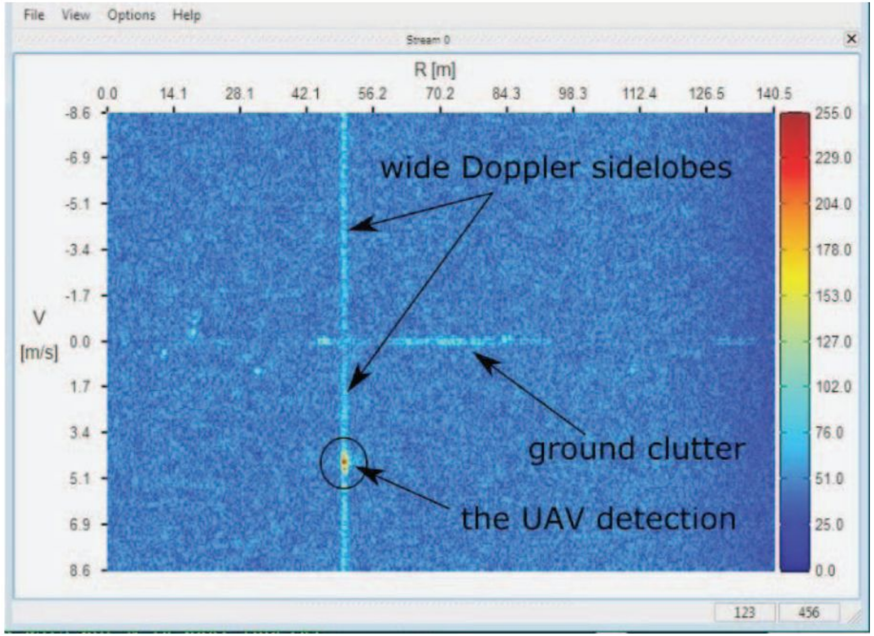


Obtained Range Doppler

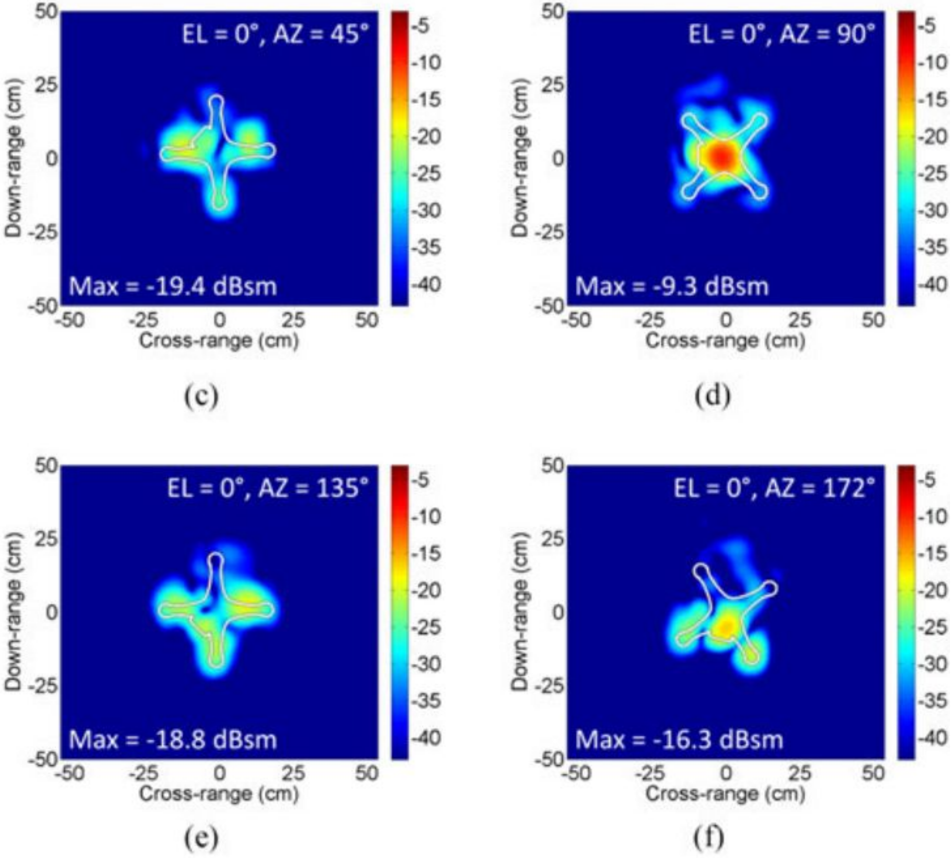
SPRITZ Security & Privacy Research Group

Università degli Studi di Padova

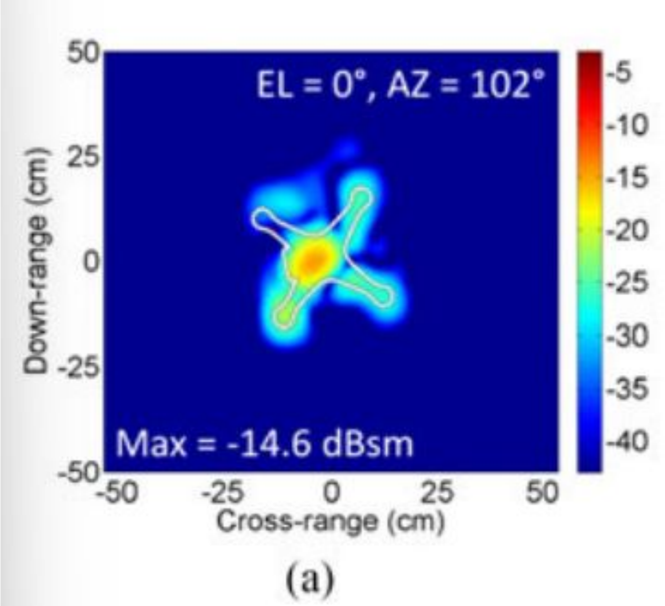
- Wide doppler sidelobes occur due to the very high frequency
- The wide doppler spread comes from the rotating drone parts
- These often vary for different units, so they can be used for target recognition and classification



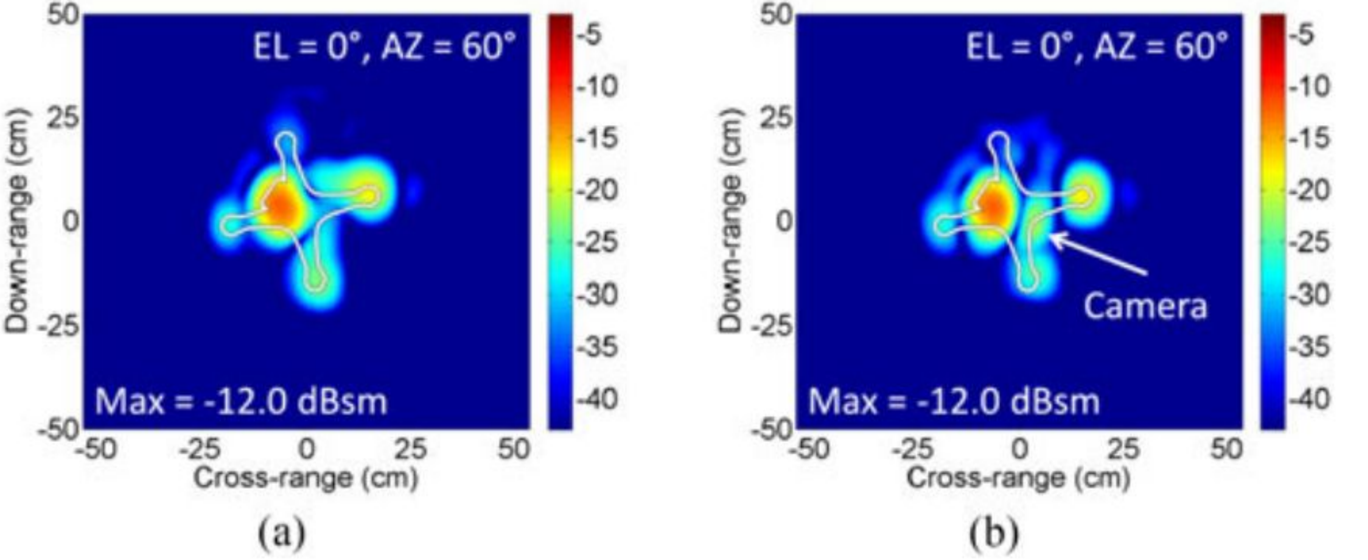
Rotating Azimuth Angle



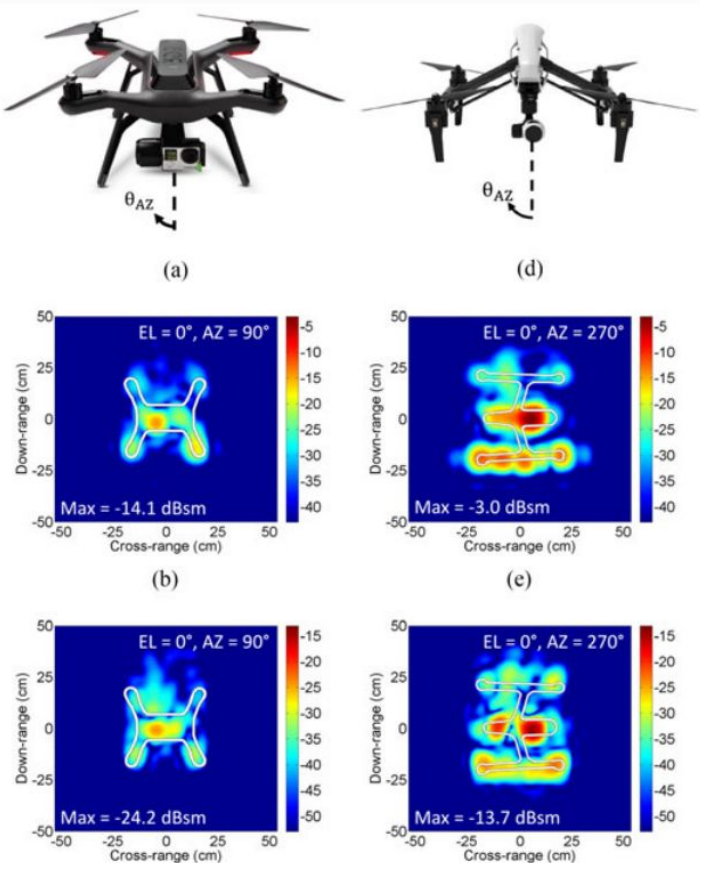
Effect of Rotating Blades



Effect of Camera



Differences



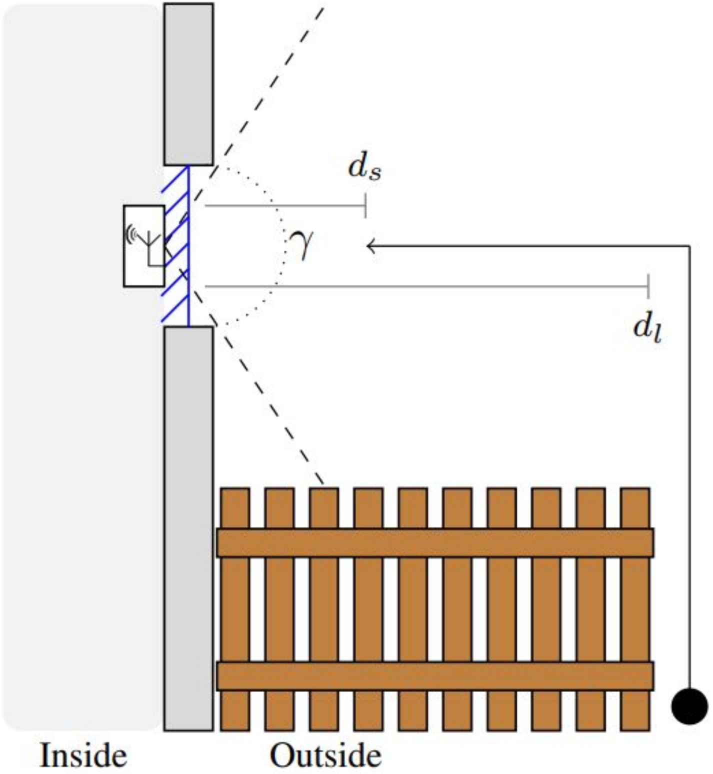
Considerations

- Commercial radars have wide operation ranges (10-50 km) and are not influenced by weather conditions
- However, they rase false positives in the presence of birds
- They are very expensive
- Not intended to be deployed in urban environment, and require a dedicated area/facility for deployment

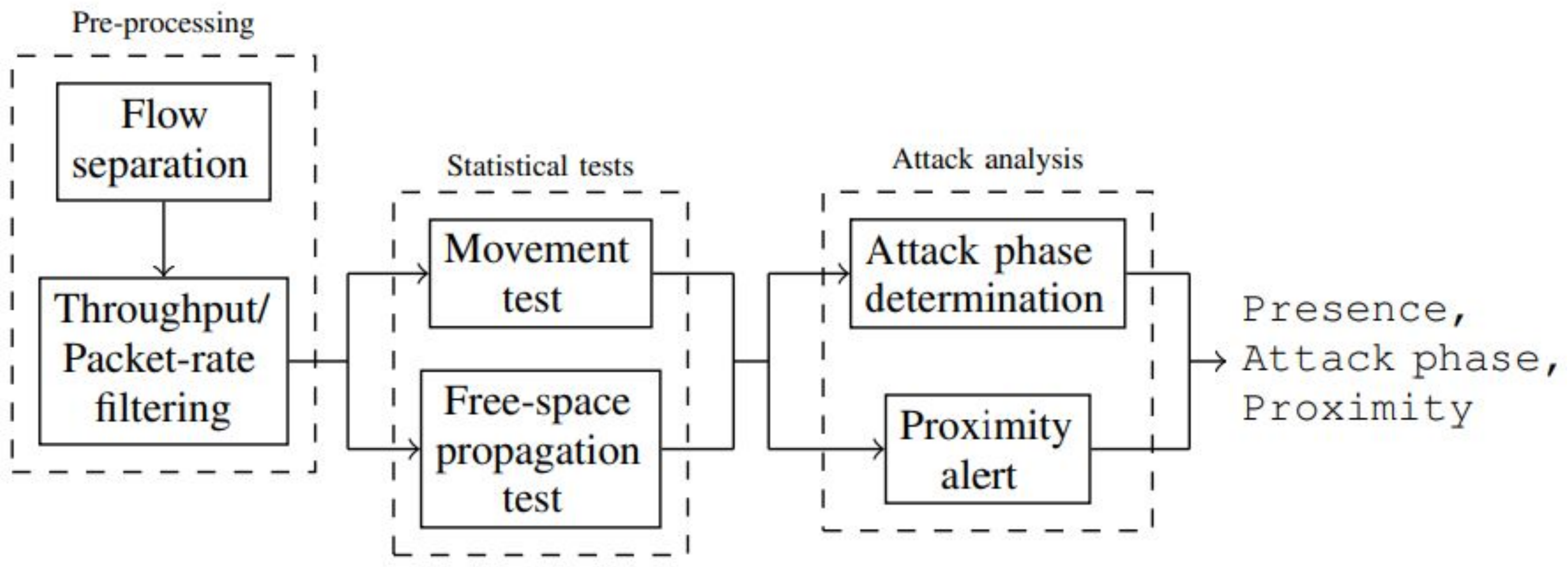
RF Scanners

- Radio Frequency-based detection leverages the fact that drones are usually controlled via radio frequency transmissions
- Most commonly employed bands are around 2.4 and 5 GHz
- The idea is to perform network traffic analysis to detect the presence of drone control channels
- Time domain analysis:collect packets in a pcap file to analyze the packets flow
- Frequency domain analysis:identification of FPV can be based on the fact that the power around FPV frequencies outperforms that of others

Statistical Metrics for Movement and Proximity



Statistical Metrics for Movement and Proximity



Pre-Processing

- The first thing to do, is to separate different data flows
- Assumption: the drone is unmodified and communicates via IEEE 802.11 Wi-Fi standard
- We assume the drone is recording videos to invade privacy
- The FPV channel requires high bandwidth to convey live video streaming, therefore we can exclude all flows that do not show this characteristic

Statistical Test

- The drone must establish a line of sight channel with the window to conduct a privacy invasion attack
- We assume that the LoS channel is established also with the controller and therefore that the Received Signal Strength (RSS) does not vary much in time (effect only on cross-traffic interference and noise)
- Over a long time period, the movements of the drone affect the RSS
- We use both a short time window and long time window and expect the aforementioned changes

Statistical Test

- The free-space path loss for the i-th measurement is given by

$$x_i = 20\log_{10}\left(d_s + \frac{i}{r}\cdot v_{\max}\right) + 20\log_{10}(f) - 27.55$$

- Where r is the packet rate, d is the distance drone-window
- We consider a length w time window, and receive N = rw packets
- The unbiased sample standard deviation is

$$s(N) = \sqrt{\frac{1}{N-1}\sum_{j=1}^{N} x_j - \boxed{\bar{x}}}$$

sample mean

Statistical Test

- Assuming we know the noise variance of our receiver, we can compute the maximum window size such that the standard deviation is below the noise threshold

$$w_s = \max\left\{w | s(w \cdot r) < \sigma\right\}$$

- The noise threshold hance bound the random variable Free Space Path Loss (FSPL) within window w
- When using measurements however we are computing the std of the sum of two variables

Statistical Test

- We consider the sum of FSPL and noise, with variance

$$Var(FSPL + X_N) = Var(FSPL) + Var(X_N) \\ + 2Cov(FSPL, X_N)$$

- We know that $Var(FSPL) < \sigma^2$ and that $Var(X_N) = \sigma^2$ and that the two r.v.s are uncorrelated → Cov = 0
- Therefore $Var(FSPL + X_N) < \sigma^2 + \sigma^2 + 2 \cdot 0 = 2\sigma^2$
- Based on this, we know that the short-term free space propagation test fails when the standard deviation of measured samples during w_s is greater than $\sqrt{2}\sigma$

Statistical Test

- We now want to detect whether the drone is moving
- We expect a velocity v for the drone, such that the FSPL is

$$x_i = 20\log_{10}\left(d_l - \frac{i-1}{r}\cdot v\right) + 20\log_{10}(f) - 27.55$$

- We now look for the minimum window size to detect movement

$$w_l = \min\{w | s(w \cdot r) > \sigma\}$$

- By doing the same computations as before, we can show that the movement test is successful if the samples collected in w_l have variance higher than $\sqrt{2}\dot{\sigma}$

Attack Analysis

SPRITZ Security & Privacy Research Group

Università degli Studi di Padova

- We apply a test to all flows that are recognized to be drones
- We monitor the long-term RSS trend and apply a proximity test to drones that appear to be approaching
- We detect the attack by taking the mean of the first and second half of w_l

$$\Delta x = \bar{x}_{[1,\lfloor \frac{N}{2} \rfloor]} - \bar{x}_{[\lceil \frac{N}{2} \rceil, N]}$$

- If the difference is greater than zero, the drone is approach
- Otherwise the drone is escaping
- If zero, the drone is still, but this not necessarily implies that is snooping at the window → need proximity test

Proximity Test

SPRITZ
Security & Privacy
Research Group

Università
degli Studi
di Padova

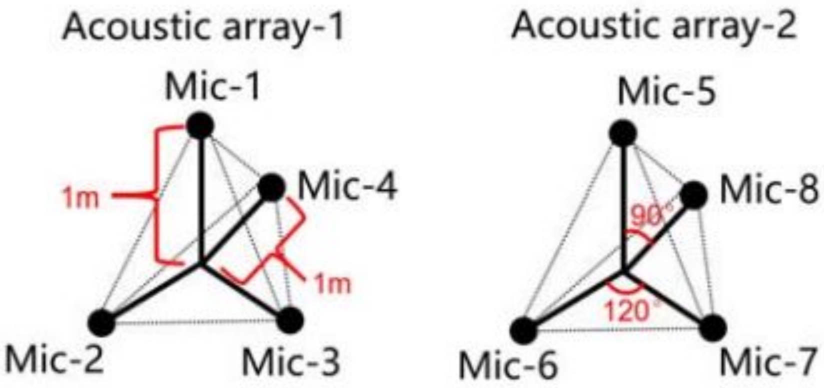
- As we did before, we use RSS to detect the proximity of the drone
- In particular, the drone has arrived at a surveillance distance d_s if Δx is larger than or equal to σ_p

$$x_i = 20\log_{10}\left(d_s + \frac{i}{r}\cdot v\right) + 20\log_{10}(f) - 27.55$$

$$N = w_l \cdot v,\ \Delta x \geq \sigma_p$$

Acoustic Detection and Tracking

- Drones emit noise that is characteristic for their propellers
- This peculiarity can be used to detect and track drones
- Need to deploy an acoustic array, composed by multiple microphones
- We consider two arrays, each composed by four microphones



- Methodologies:
  - Direction of arrival estimation: high complexity (both algorithms and number of microphones) and noise sensitivity
  - Received signal strength: high noise sensitivity
  - Time Difference of Arrival (TDOA): usually computed via the generalized cross-correlation function having low complexity, high accuracy, and good robustness

TDOA Estimation

- Denote m and n as microphone n and microphone m respectively
- We denote as $x_m(t)$ the acoustic signal received by m at time t
- We denote as $G_{x_m x_n}(f)$ the Fourier transform of the cross correlation function
- We use the Cross Power Spectral Density function

$$R_{x_m x_n}(\tau, k) = \int_{-\infty}^{\infty} G_{x_m x_n}(f) \boxed{\varphi_{mn}(f)} e^{-j2\pi f \tau} df$$

freq. domain pre-filter

- The peak value denotes the TDOA result

Drone Localization

SPRITZ Security & Privacy Research Group

Università degli Studi di Padova

- Denote as S the location of the microphone sensors and S_0 as the location of the drone
- For each pair of microphone we can write $d_{mn} = \|S_m - S_0\| - \|S_n - S_0\|$ which is the path difference between drone and mic
- Noise is inherently included in our TDOA measurements $\tau_{mn} = \tilde{\tau}_{mn} + \varepsilon_{mn}$
- Noticing that $d_{mn} = c\tau_{mn}$, we can write a system of equations and find a solution by minimizing the following quadratic form

$$Q = (T - F)^T S_{\text{cov}}^{-1} (T - F)$$

Drone Detection with Single Camera

- Analyzing video images provides means for detecting flying and moving objects
- However it is not always easy to distinguish small objects in complicated and feature-rich images

Detection without Motion Stabilization

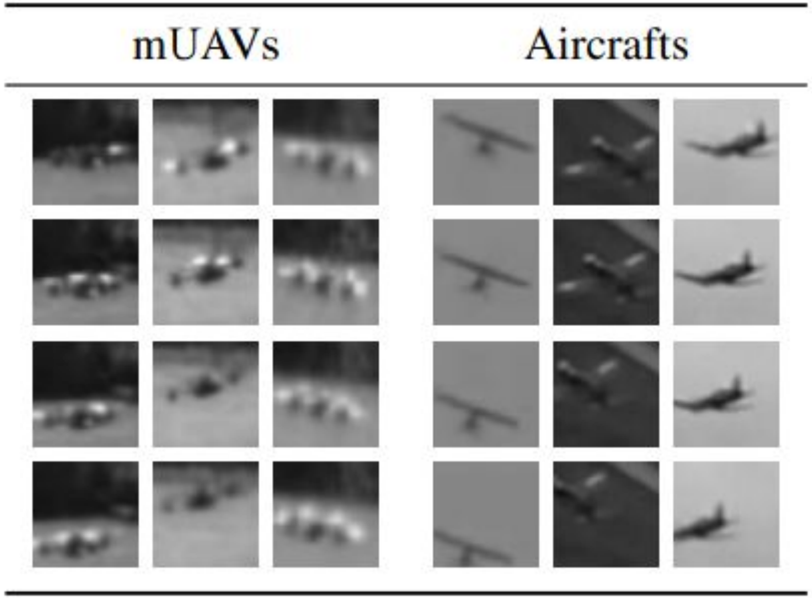
- We define spatio temporal cubses (st-cubes), where spatial dimensions are sx and sy, while the temporal is st
- We use a training set composed of st-cubes and binary labels indicating whether or not the image contains a target object
- We then train an AdaBoost classifier

$$F : \mathbb{R}^{s_x \times s_y \times s_t} \rightarrow [0,1], \qquad F(b) = \sum_{j=1}^{T} \alpha_j f_j(b)$$

- Where alphas are the weights and T is the number of weak classifiers learnt
- However, the orientation of gradients is a problem here

Object-Centric Motion Stabilization

- To eliminate the problem, we need to guarantee that the target object, if present in an st-cube, remains at the center of all spatial slices
- This means that we can allows the spatial slices to move horizontally and vertically in individual images



Training the Regressor

SPRITZ Security & Privacy Research Group

Università degli Studi di Padova

- We train two boosted trees regressors: one for horizontal motion and one for vertical motion
- It does not use similarity between consecutive frames and can predict how far the object is from the center based on just a single patch
- We use regression trees as weak learners
- At every iteration, the boosting approach finds the weak learner that minimizes function

Regression tree

$$h_j(\cdot) = \underset{h(\cdot)}{argmin} \left(\sum_{i=1}^{N} w_i^j \left(\boxed{h(x_i)} - \boxed{r_i} \right)^2 \right)$$

Expected response

Motion Compensation

SPRITZ
Security & Privacy
Research Group

Università
degli Studi
di Padova

- We use the two regressors in an iterative way to compensate for the motion of the aircrafts in the st-cube
- The resulting st-cube keeps the aircraft close to the center throughout the whole sequence of patches

$$(sh_h, sh_v) = (\phi_h(m_p), \phi_v(m_p)) \longrightarrow \text{prediction}$$

$$(i_n, j_n) = (i_{n-1} - sh_v, j_{n-1} - sh_h) \longrightarrow \text{compensation}$$

$$m_k = m_{i_n, j_n, p} \longrightarrow \text{patch}$$

Assessment

- Before taking down a drone we need to determine whether it is or not hostile
- This is particularly critical in areas where drones are allowed to fly
- A method to assess the drone intentions is based on classification
- We refer to classification as the process of identifying the manufacturer and model of the drone
- The assumption is that we know which types of drones are allowed in a given area and which other are not

Available Information

SPRITZ
Security & Privacy
Research Group

Università
degli Studi
di Padova

- We can inspect packets to infer information on the model and make of drones and hence decide if they should or not be allowed to fly
- The vendor MAC address is identifiable along with individual fingerprints determined via nmap
- FTP and Telnet are (sometimes) enabled without security, so it possible to connect and upload files while the UAV is operating

Drones’ Fingerprints

- We want to capture drone body movements by using RF signals
- We have a transmit antenna at the drone’s side and a receiving antenna at a fixed location
- The transmit antenna emits a single tone 2.4 GHz when the drone is flying
- The idea is to capture variations in RSSI and phase of the signal to infer drone body movements
- Drone classification based on the frequency of vibration

Existing Anti-Drone Systems

- In real life situations, we cannot simply rely on a single technology to detect drones
- We usually combine radar, cameras, LiDAR,.., to develop a robust system
- Different technologies provide different capabilities in terms of range, coverage, possibility for classification, tracking

Existing Anti-Drone Systems

		Radio		Optical			Acoustic	Features				
Company Name	Product Name	Radar	RF Scanner	Camera	LiDAR	Infrared	Microphone	Effective Range (KM)	Classification	Coverage (°)	Tracking	Mobility
3DEO	Rogue Drone Detection Mitigation [107]				✓			2			✓	
Aaronia	Drone Detection System [71]	✓	✓	✓		✓		50	✓	90/360	✓	✓
Anti-Drone.eu	GROK [72]	✓						4	✓		✓	
	Droneshield [130]						✓	0.5				
Aveillant	Gamekeeper 16U - Holographic Radar [73]	✓						5		90	✓	
Black Sage - BST	UAVX [74]	✓		✓		✓		0.5		90	✓	✓
C speed LLC	LightWave Radar [75]	✓									✓	
CACI	SkyTracker [86]		✓						✓			
CerbAir	Hydra [87]		✓					2	✓	90/360	✓	✓
Chess Dynamics Ltd	AUDS [76]	✓		✓		✓		10		180	✓	✓
DeDrone.com	DroneTracker [88]		✓	✓					✓			✓
DeTect	DroneWatcher [89]		✓					1.6-3.2	✓			✓
	HARRIER DSR [77]	✓		✓			✓	3.2	✓		✓	
Digital Global Systems	SigBASE [90]		✓									✓
DroneShield	FarAlert/WideAlet Sensors [105]					✓	✓	1		30		✓
Gryphon Sensors	Skylight [78]	✓	✓	✓		✓		3-10		360	✓	✓
HGH Infrared Systems	UAV Detection & Tracking [100]			✓		✓				360		
Kelvin Hughes Limited	SharpEve SxV Radar [79]	✓		✓		✓		1.5		360	✓	✓
MAGNA	Drone Detection [101]			✓		✓	✓	0.5-1				
Microflown AVISA	Skysentry AMMS [91]		✓				✓	0.4-1		360	✓	
Mistral Solutions	Drone Detection and Classification System [92]		✓	✓		✓		1	✓			
ORELIA	Drone-Detector [113]						✓	0.1		360		

Example

- Link