Wi-Fly?: Detecting Privacy Invasion Attacks by Consumer Drones

Simon Birnbach, **Richard Baker**,

Ivan Martinovic

UNIVERSITY OF OXFORD

DEPARTMENT OF COMPUTER SCIENCE

2017 NDSS

EPSRC Engineering and Physical Sciences Research Council

Let’s Talk About Drones

Why Should We Care?

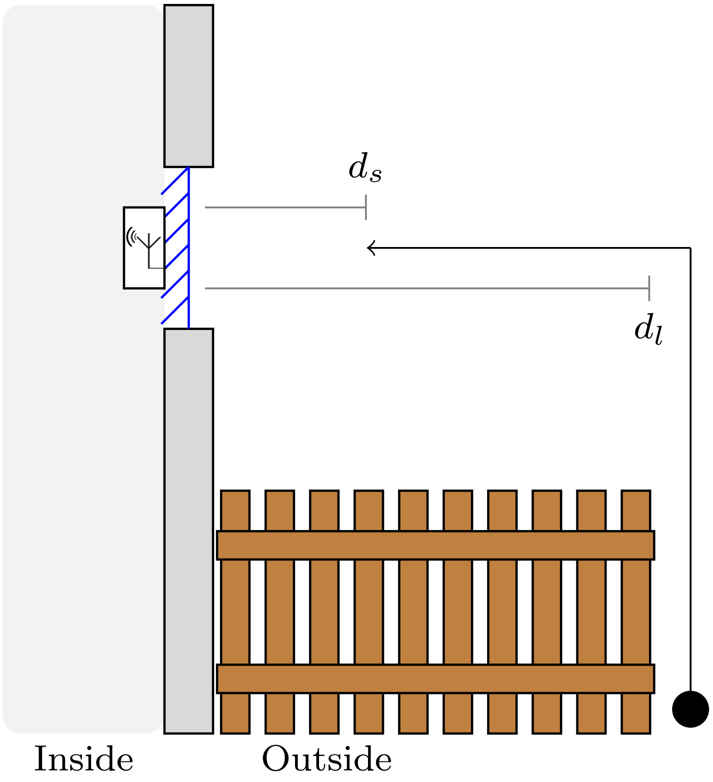
- Ignore physical access restrictions
- High-quality camera equipment
- Spy tools in the hands of everybody
- Privacy invasions by drones get more common

How to Detect?

- Various approaches
  - Optical sensors
  - Acoustic cameras
  - High-frequency radar
- Expensive hardware needed
- Goal: Design cheap detection system
  - Radio Frequency

Adversary Model

- Unmodified consumer drone
  - Controlled over WiFi
  - Streams live video
- Objective:
  Capture video through window
  - Line-of-Sight (LOS) to window needed
- No direct access to premises

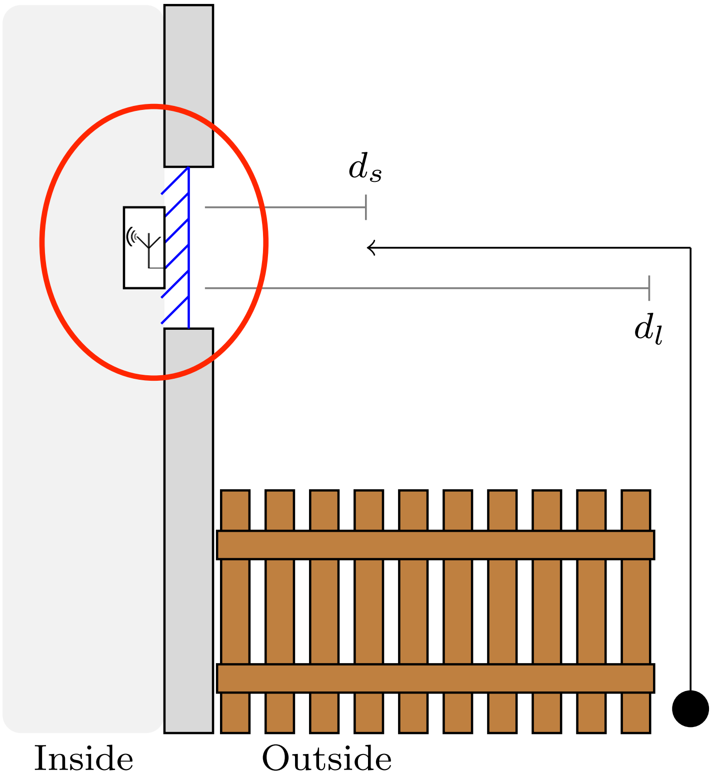


d_l: Launch distance
d_s: Surveillance distance

General Idea

- Off-the-shelf WiFi receiver
- Placement in window
  - Guarantees LOS
- Access restrictions
  - Drone starts further away
  - Forces attacker to fly higher

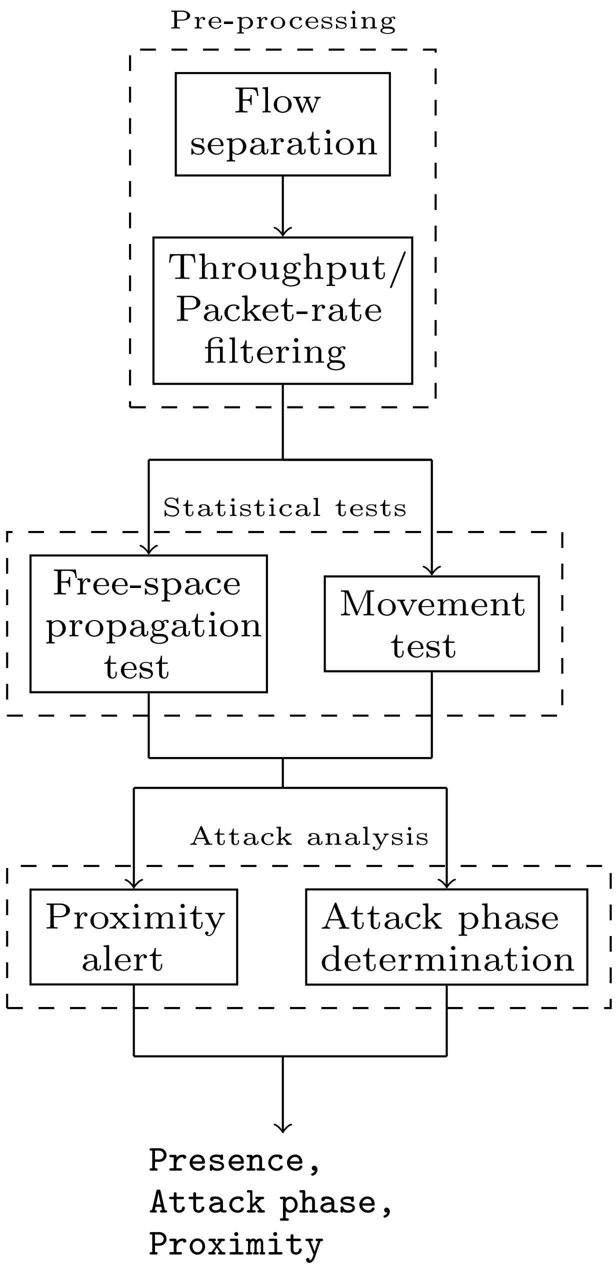
- Challenges
  - Received signal strength (RSS) → noisy data
  - Unknown flight behavior
  - Early detection



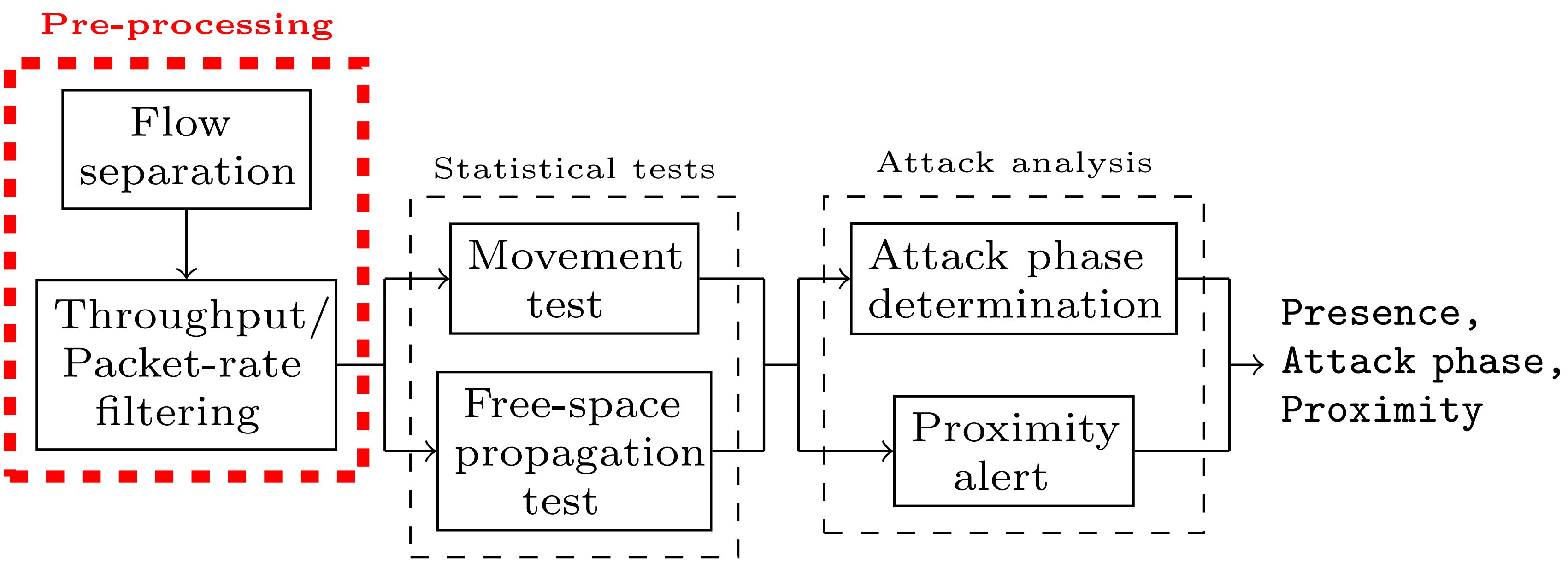
d_l: Launch distance
d_s: Surveillance distance

System Overview

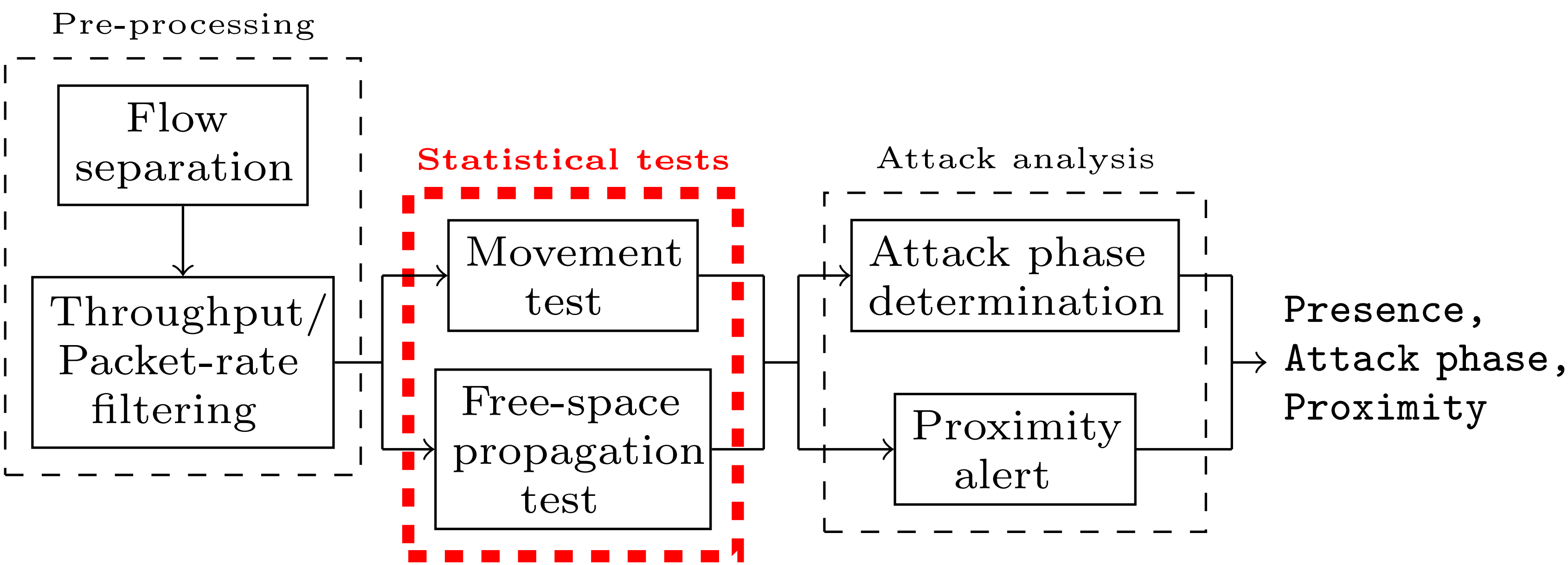
- Pre-processing
- Statistical tests
  - Presence
    → Drone nearby
- Attack analysis
  - Attack phases
    → Approach
    → Surveillance
    → Escape
  - Proximity
    → Closeness to window



Pre-Processing



Statistical Tests



Statistical Tests

Attacker has to:

- …overcome physical access restrictions
  → Drone is flying high above ground
- …establish LOS to the window
  → changes of multipath effects
  → we expect far less multipath effects due to strong LOS component (compared with ground-based transmitters)
- …move towards the window
  → RSS increases as drone approaches

- Detection method based on statistical tests:
  - Testing for flying: Closer to free-space propagation than non-flying transmitters
  - Testing for approaching & movement: significant RSS changes as distance to receiver varies

Statistical Tests

- Free-space propagation (FSP)
  - RSS depends on distance and receiver noise
  - Only noise varies in short time frame w_s (<0.1s)
- Movement
  - More distance variation than noise in longer interval w_l (>1s)
- Compute standard deviation of RSS measurements
- Noise threshold t
  - Derived from background noise

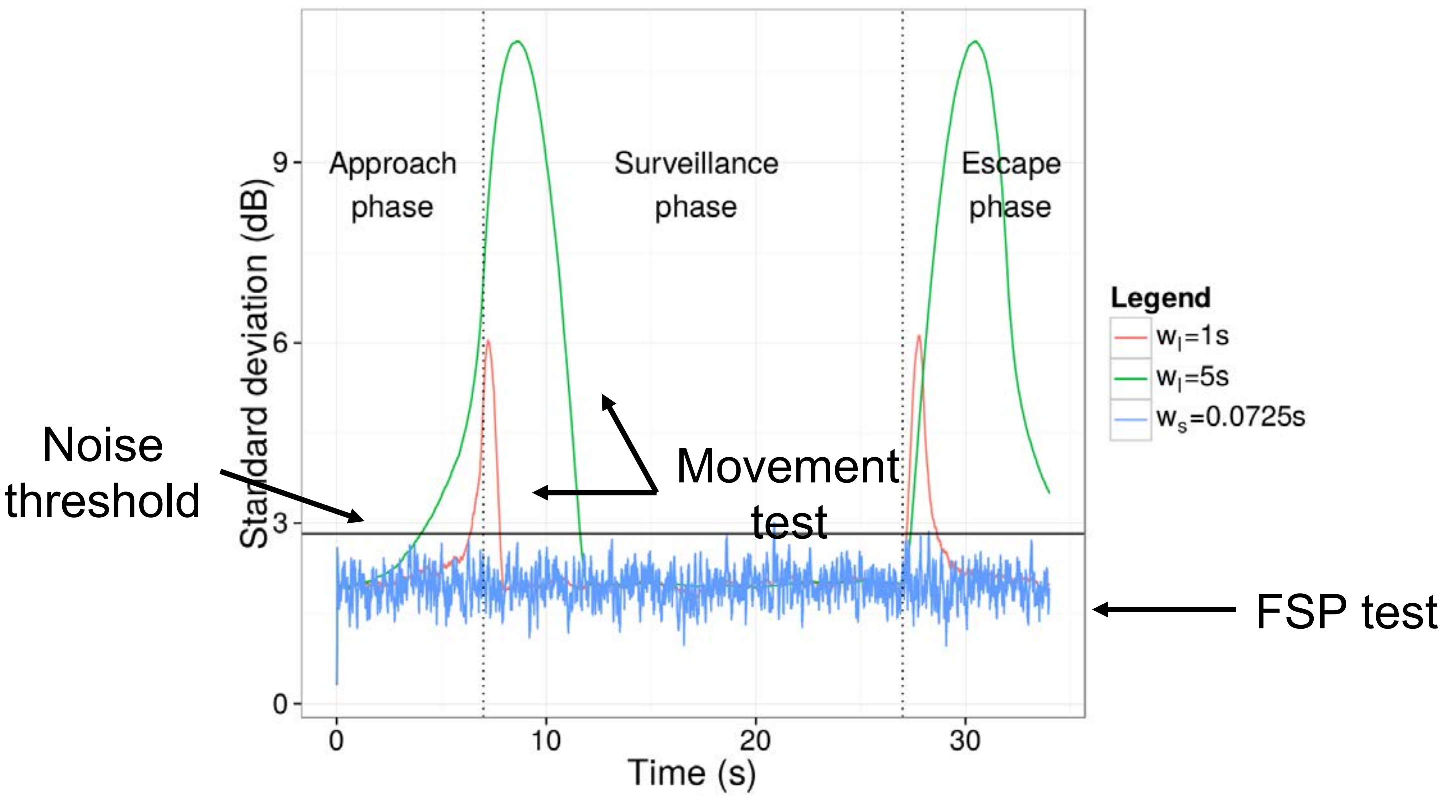
A drone is detected if:

$$s(w_s) < t \;\&\; t < s(w_l)$$

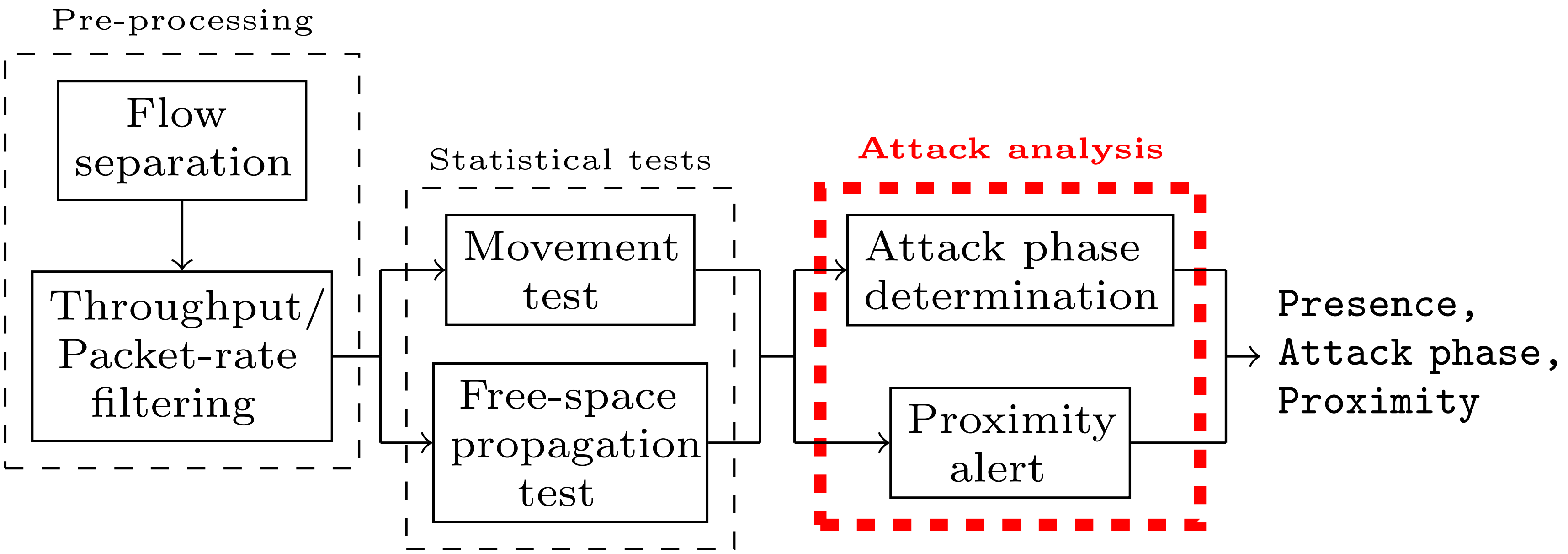
Statistical Tests

A drone is detected if:

$s(w_s) < t$ & $t < s(w_l)$

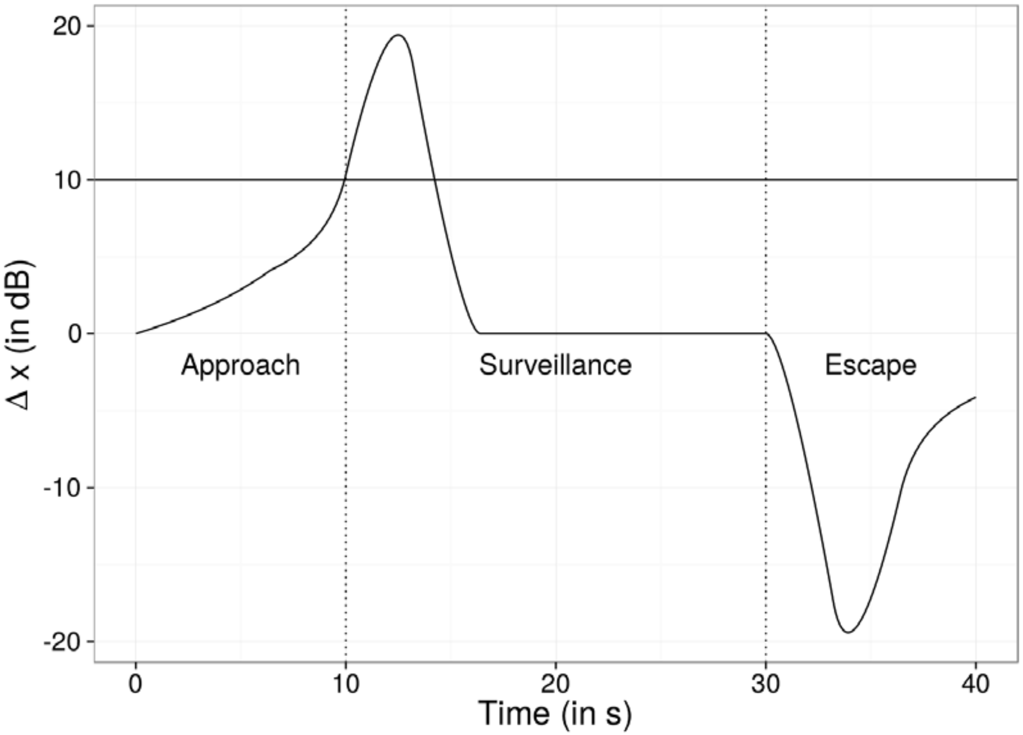


Attack Analysis

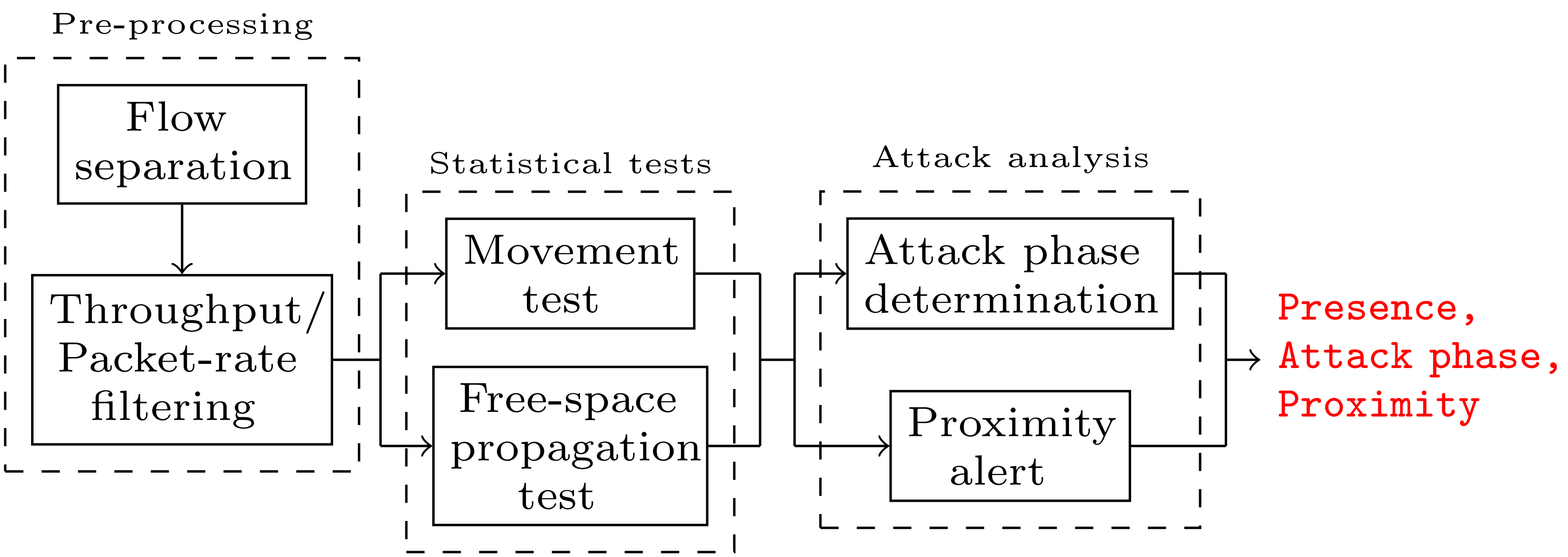


Attack Analysis

- Approach detection
  - Increase in RSS difference shows drone is approaching
- Proximity alert
  - User gets warned if RSS difference exceeds threshold

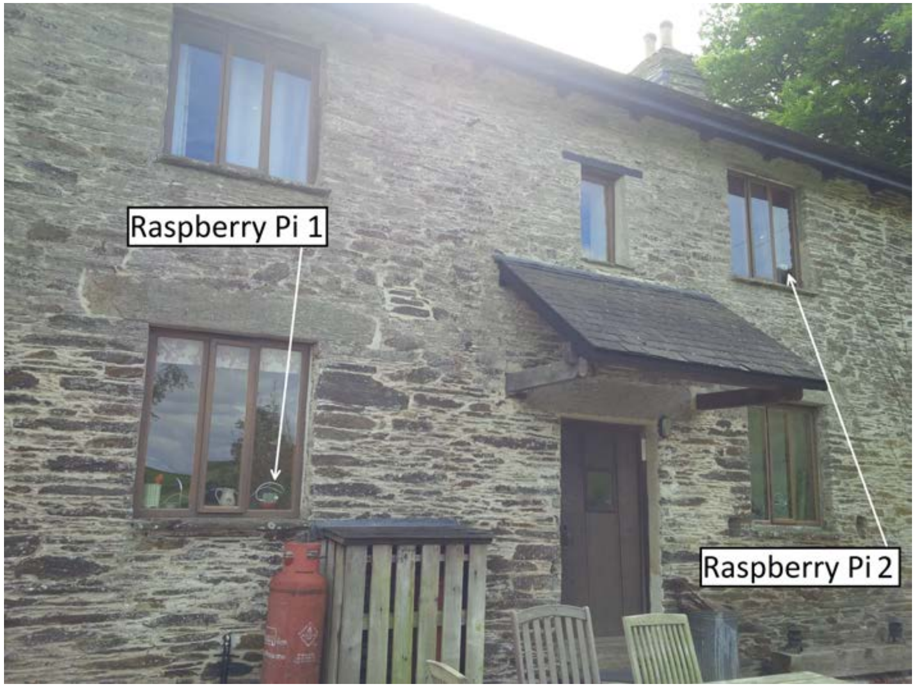


System Output

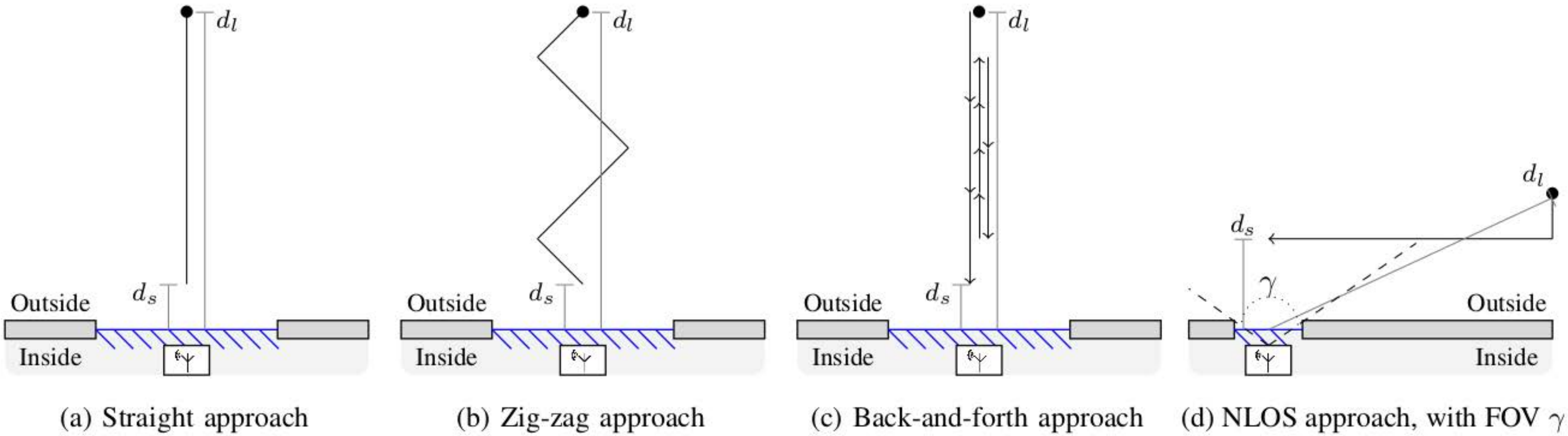


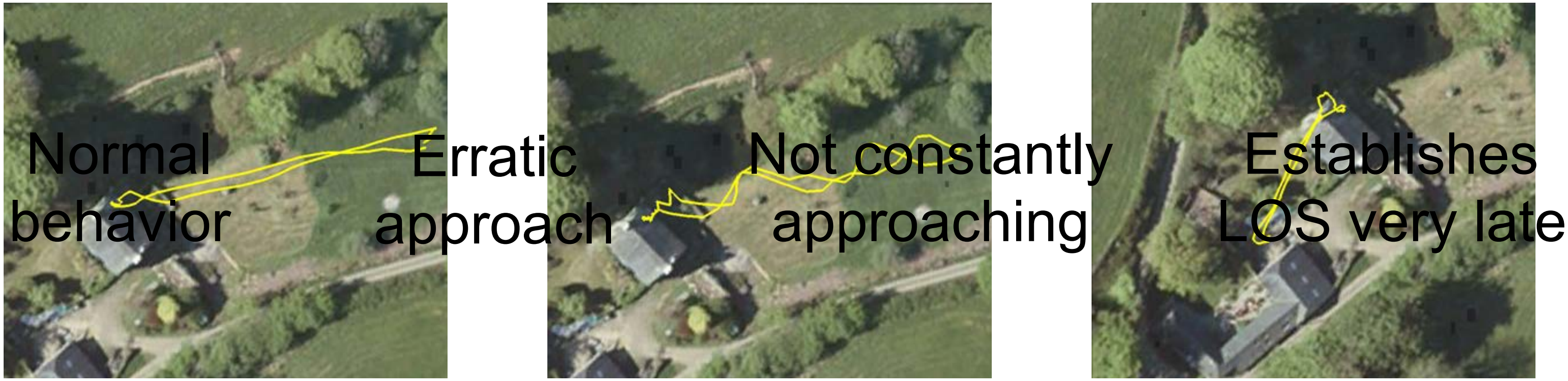
Experiment Setup

- Executed in secluded farmhouse
- Drones: DJI Phantom 3 Standard, Parrot Bebop
- Receiver: Raspberry Pi with WiPi stick mounted in window

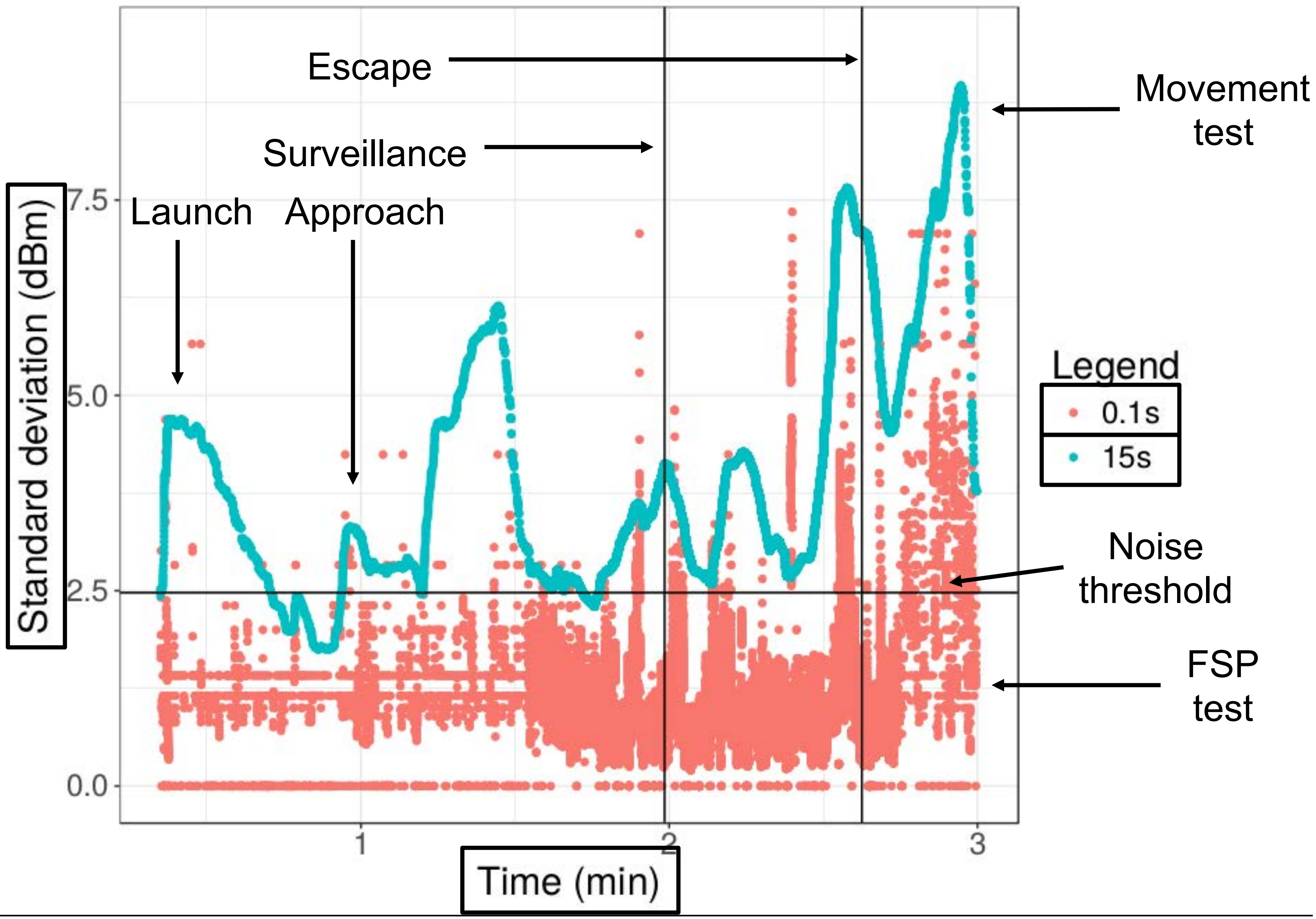


System Challenges

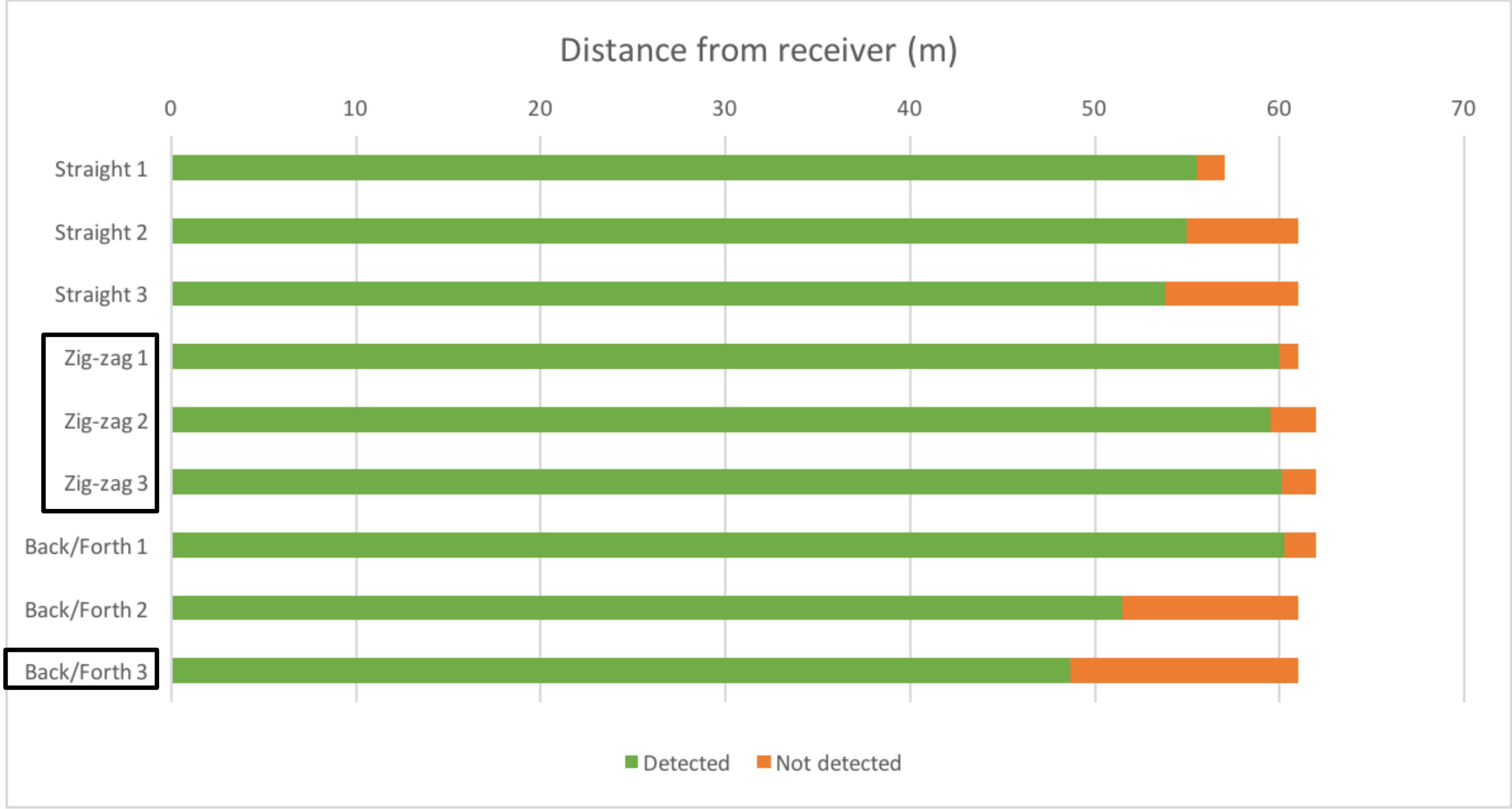




Straight Approach



Detection Distances



Conclusion

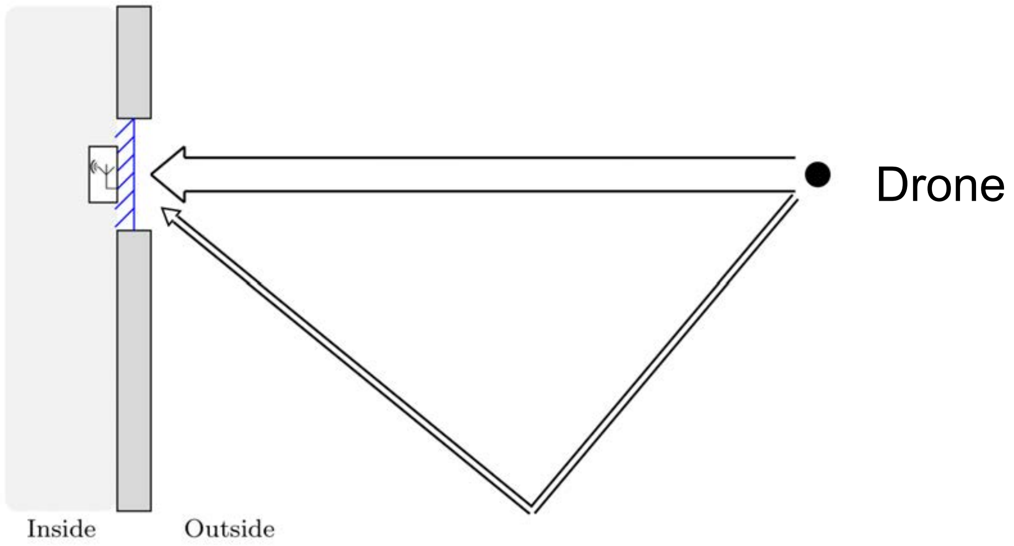
- Developed method to detect drone privacy invasions
- Implemented on cheap hardware
- Real-world experiment with variety of approach patterns shows feasibility
- Good performance, minimal detection distance 48m

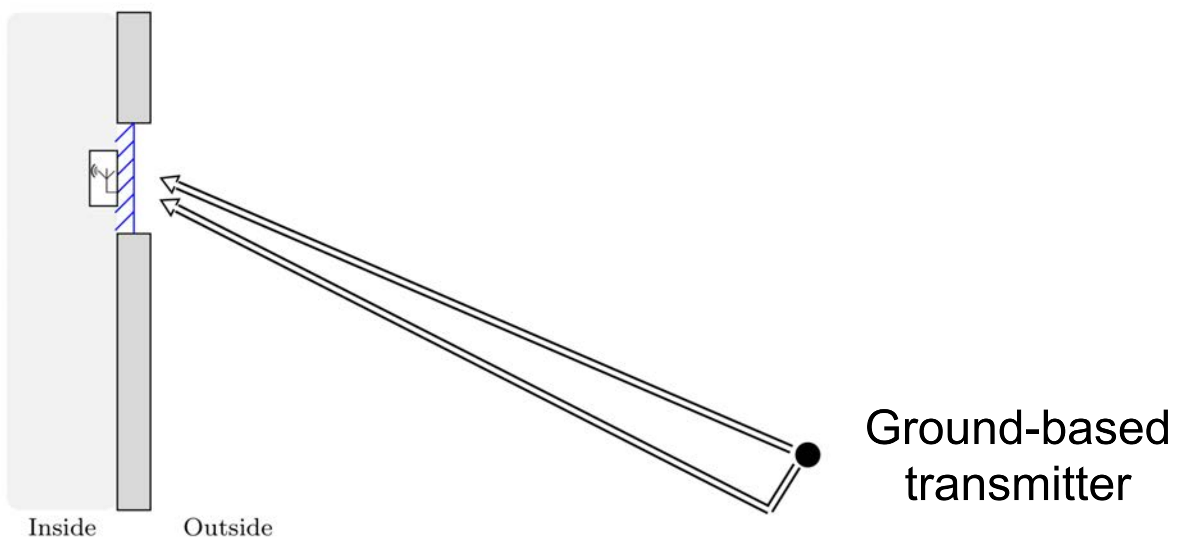
Thank you for your attention!
Questions?

simon.birnbach@cs.ox.ac.uk

Backup slides

Multipath effects



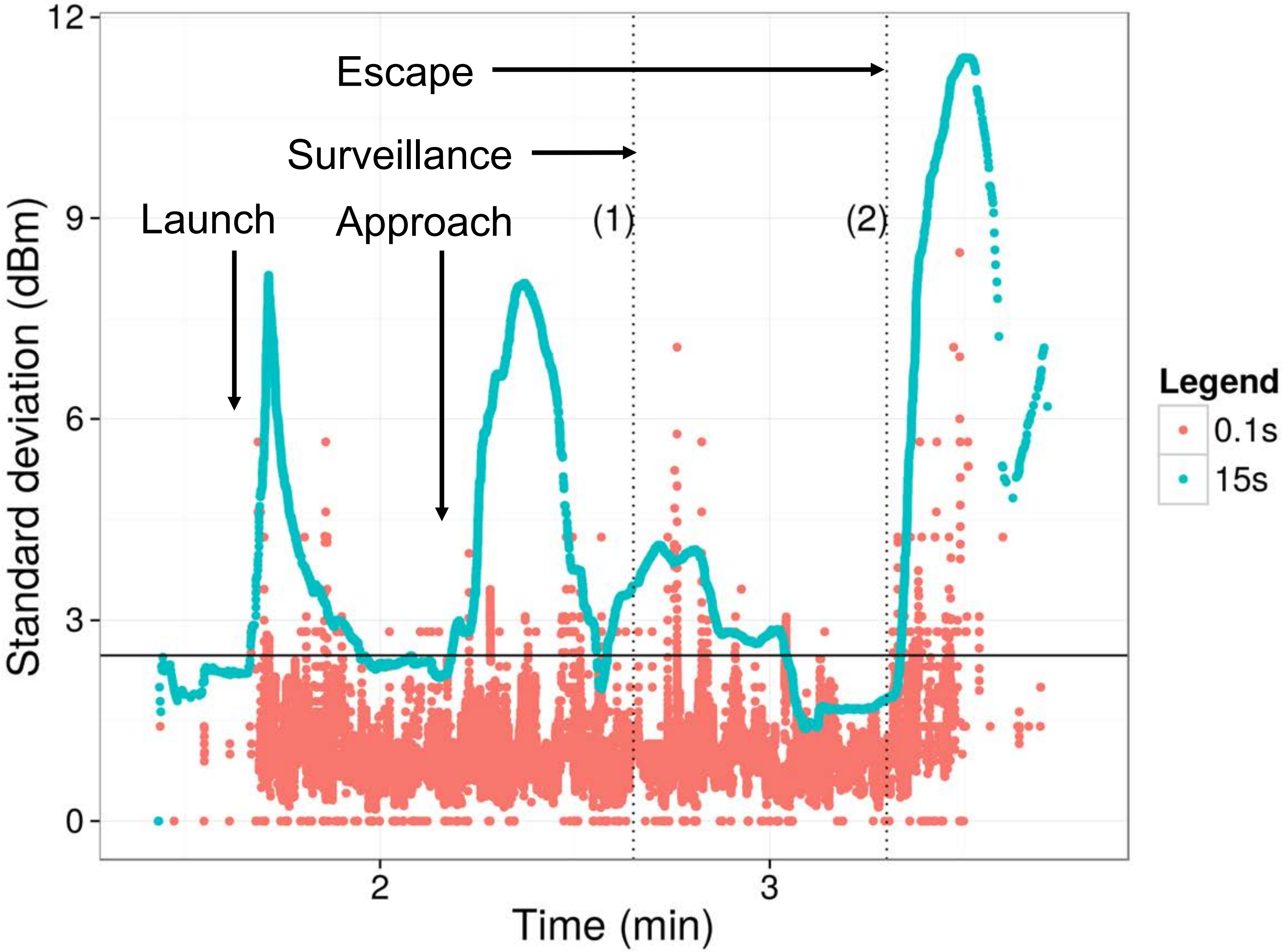


System Parameters

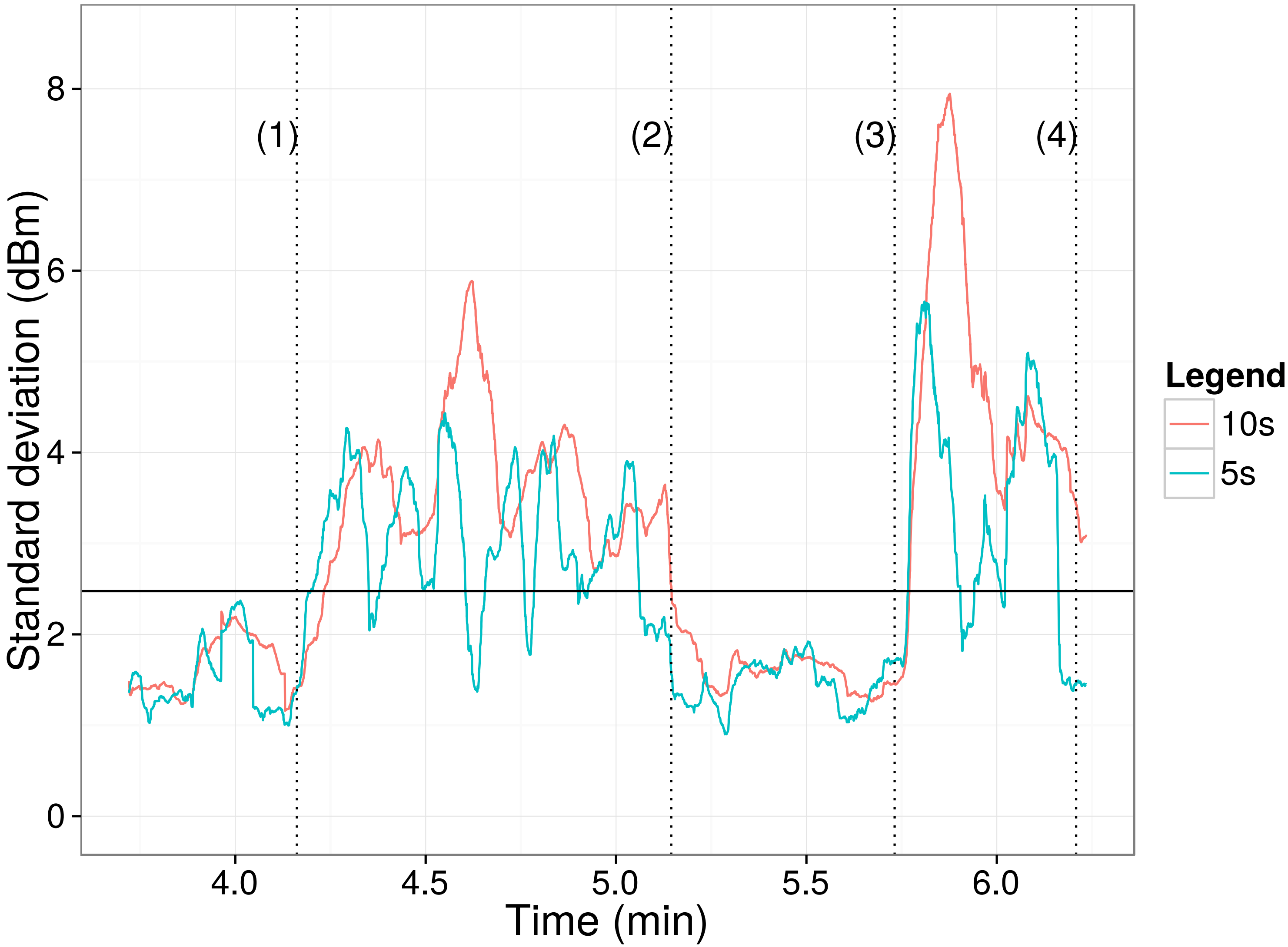
- Surveillance distance
- Launch distance
- Maximal drone speed
  - Determines FSP test window size
- Set of drone movement speeds
  - Determines movement test window sizes
- Noise threshold
  - Derived from background noise
- Proximity threshold
  - Derived from surveillance distance

Parameter	Example values
d_s	1m
d_l	50m
w_s	0.1s
w_l	5s, 10s, 15s, 30s
t	$\sqrt{2} \cdot 1.75$dB
σ_p	10dB

NLOS Approach

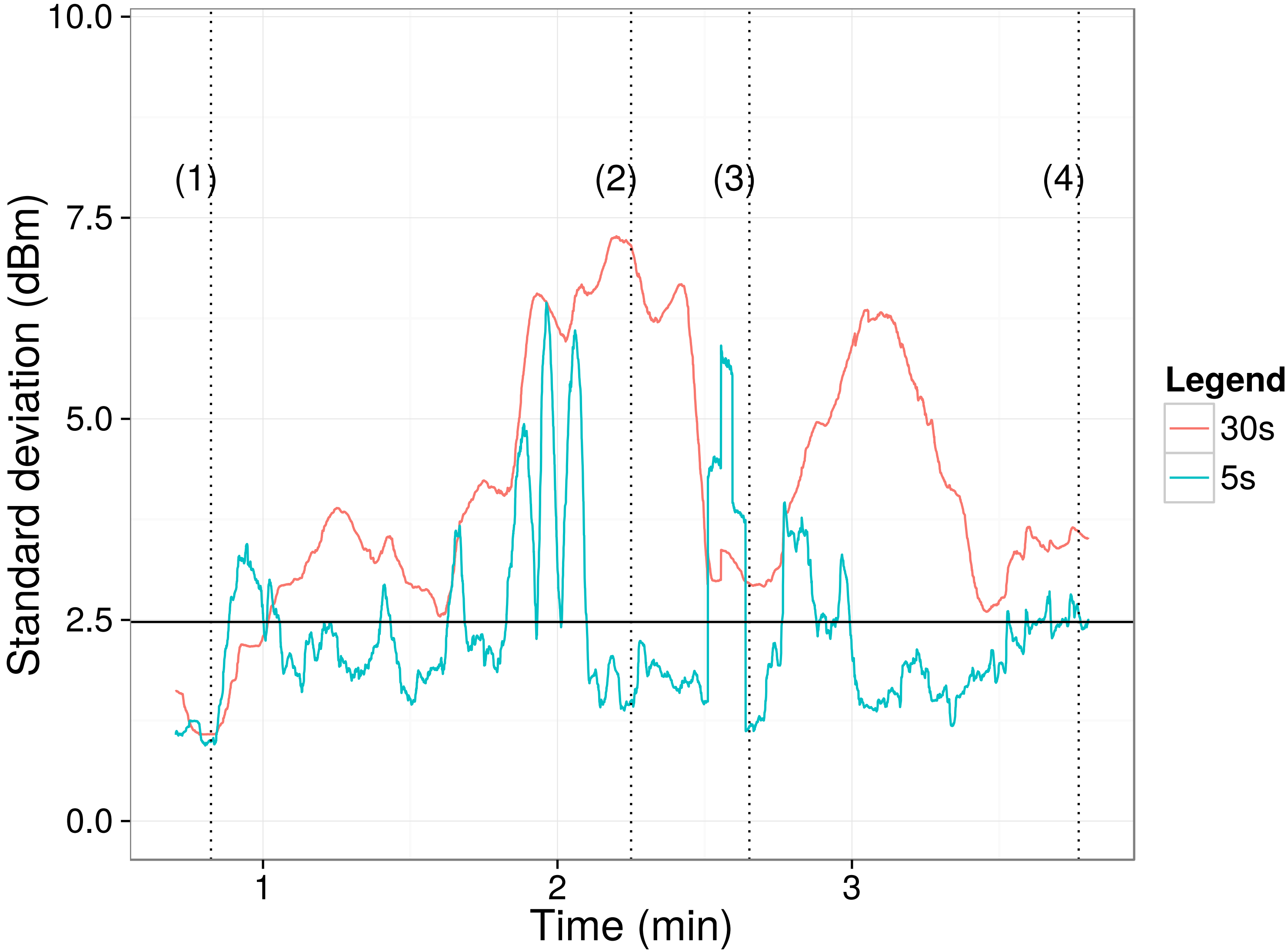


Zig-zag

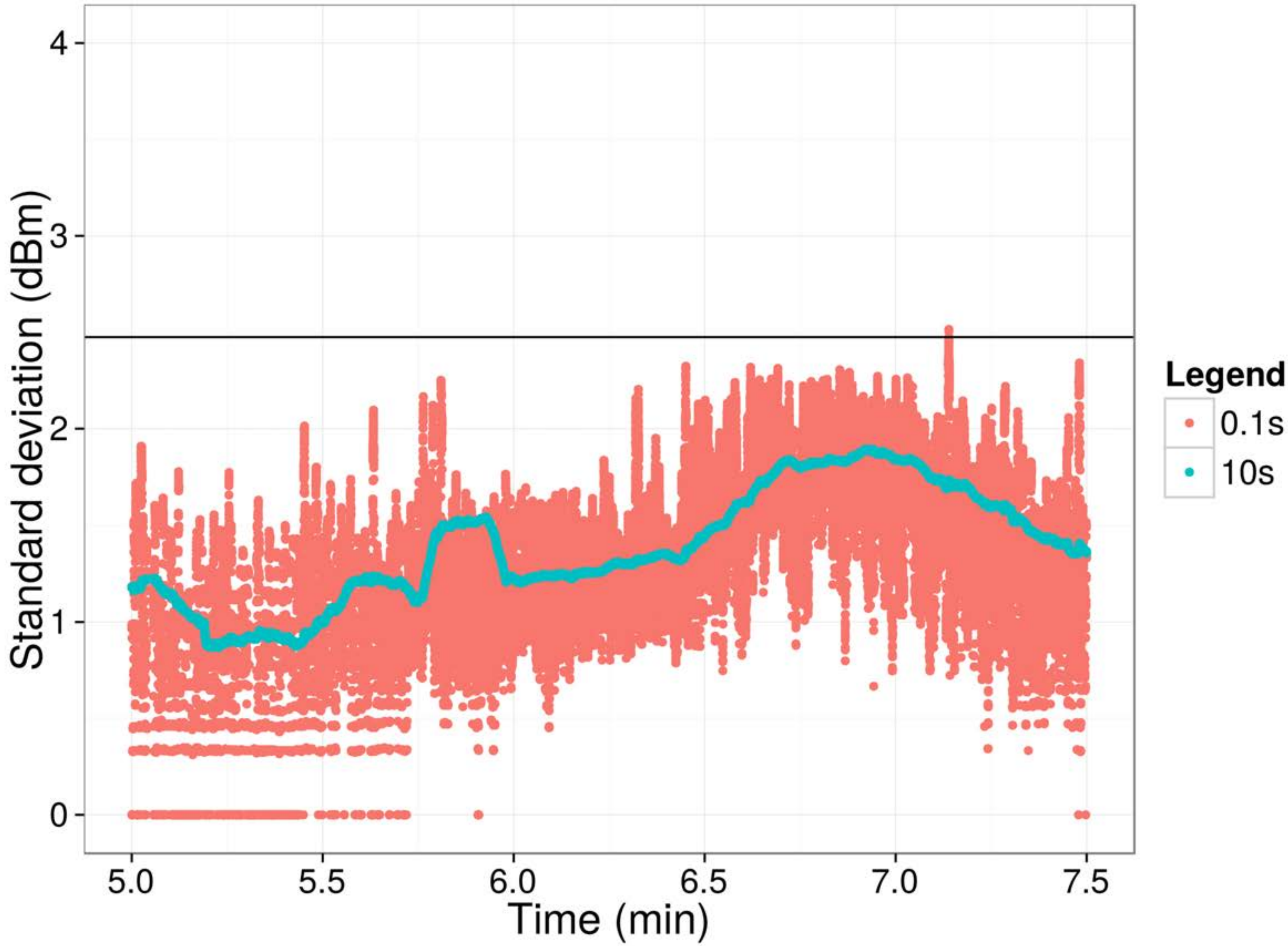


Standard deviation (dBm)
8
6
4
2
0
(1)
(2)
(3)
(4)
4.0
4.5
5.0
5.5
6.0
Time (min)
Legend
10s
5s

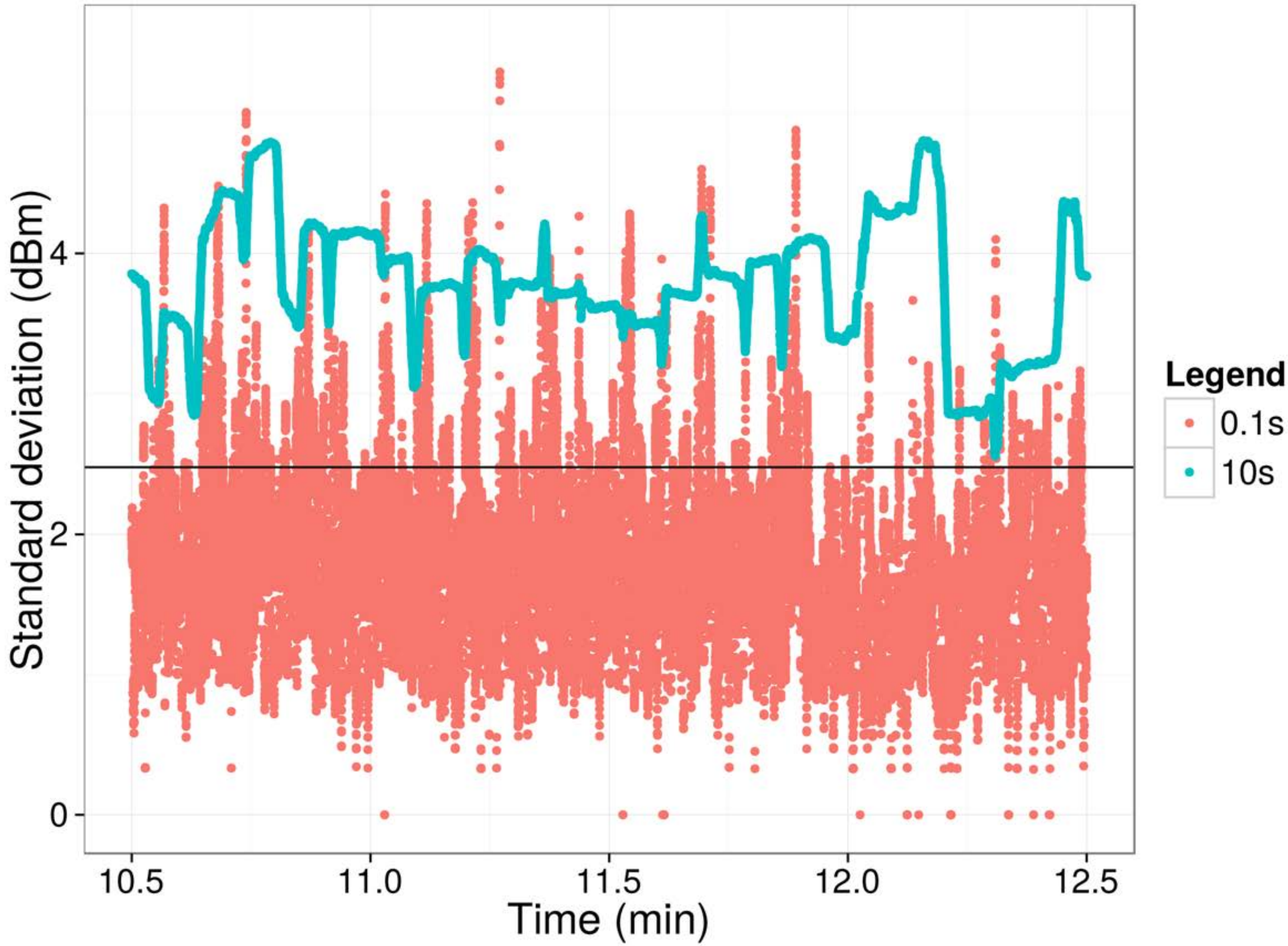
Back-and-Forth



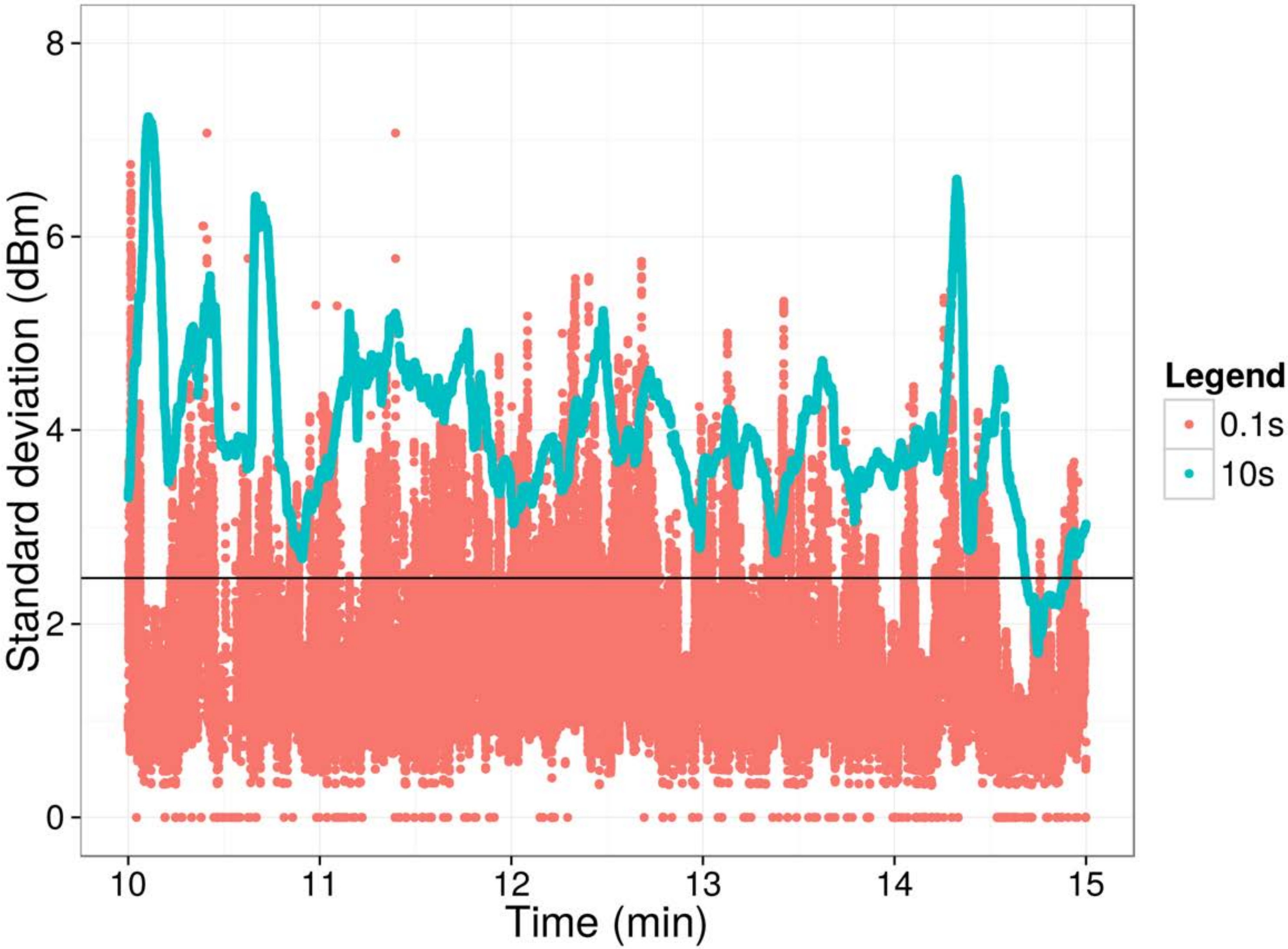
Stationary in static environment



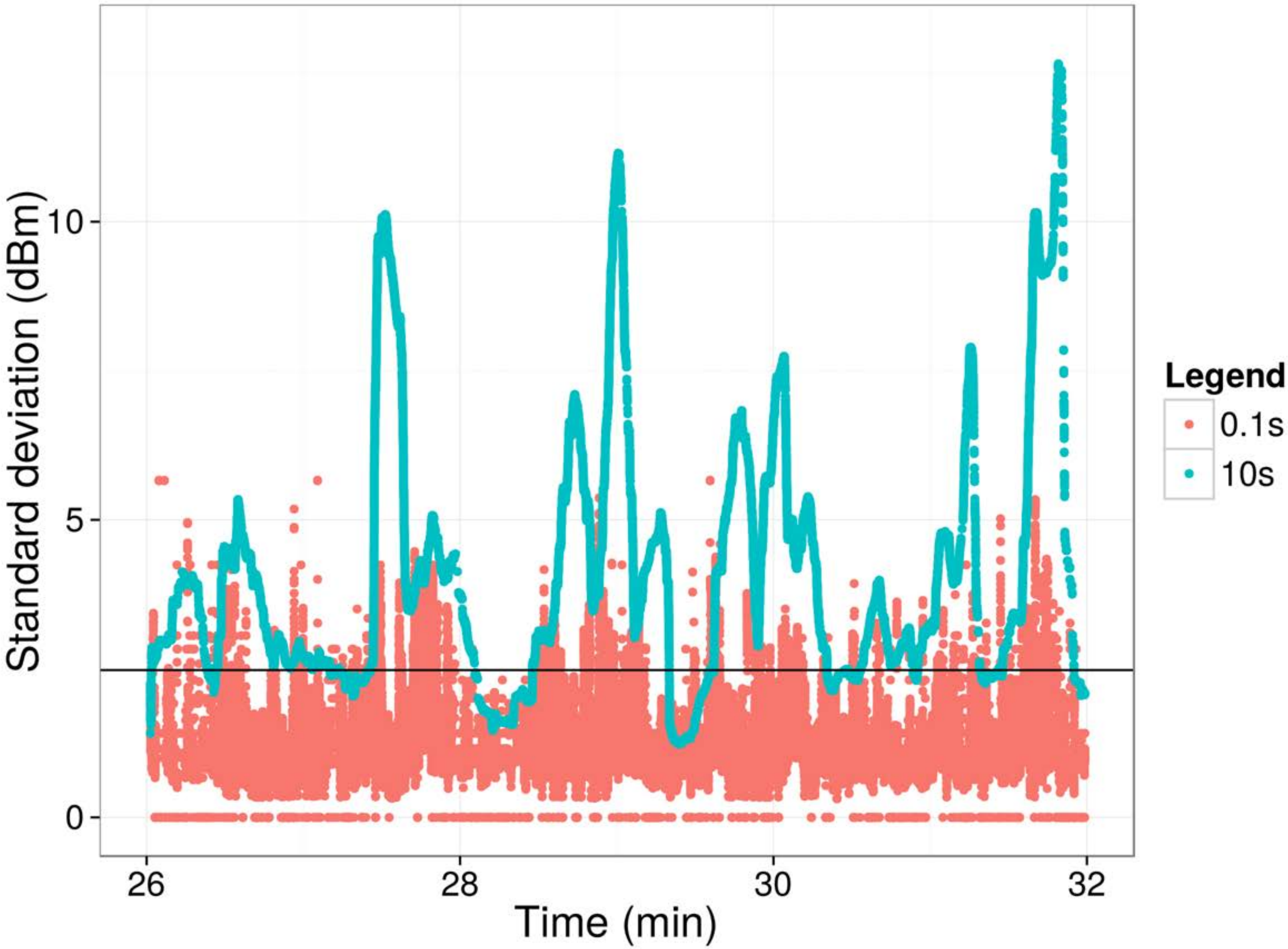
Stationary in dynamic environment



Moving indoors



Moving outdoors



Ground approach