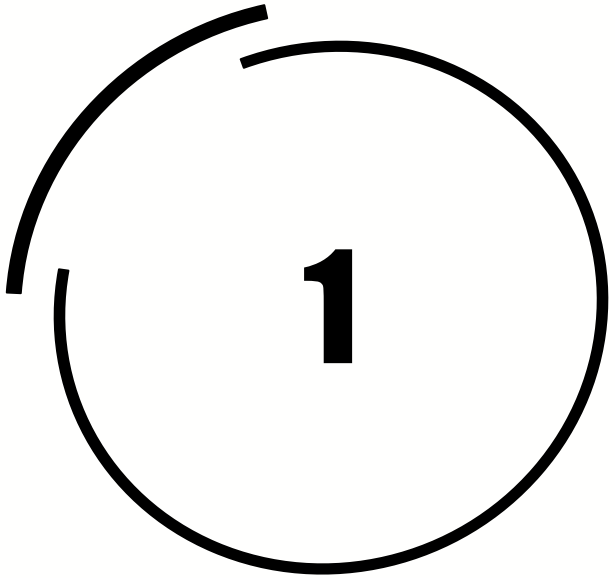
University of Glasgow

ACSAC 2022

# Drone Authentication via Acoustic Fingerprint

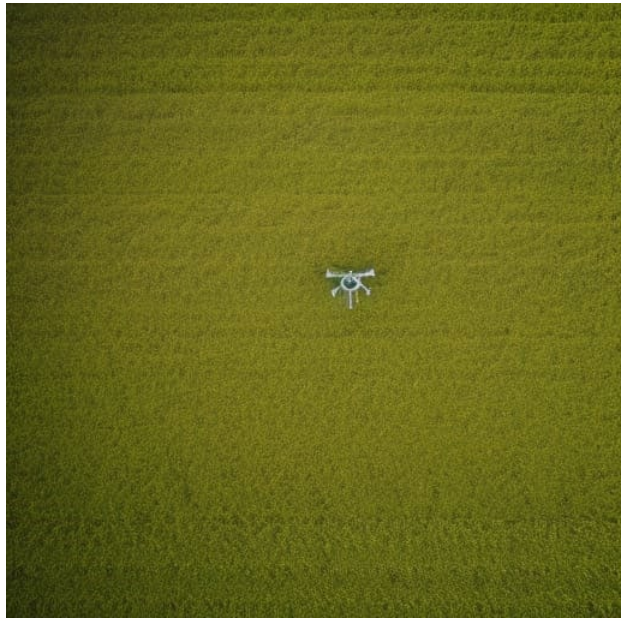
**Yufeng Diao**, Yichi Zhang, Guodong Zhao, Mohamed Khamis
University of Glasgow


Reported by: **Yufeng Diao**




# Introduction

# Drones in everywhere

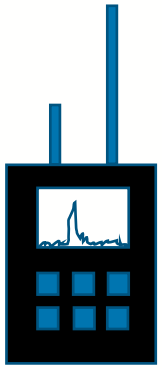


Agriculture

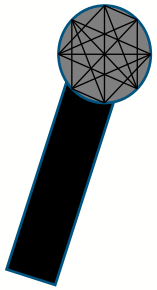
Film production

Rescue operation

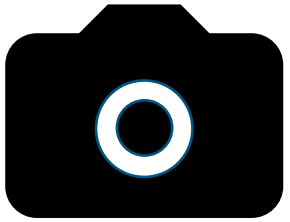
# Current Solution of Drone Detection and Classification



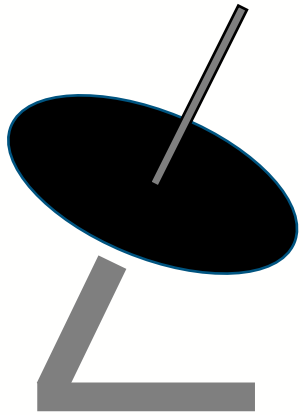
Radio frequency analyzers



Acoustic sensors



Optical sensors



Radar

Limitation: cannot authenticate drones

# Drone Authentication Methods

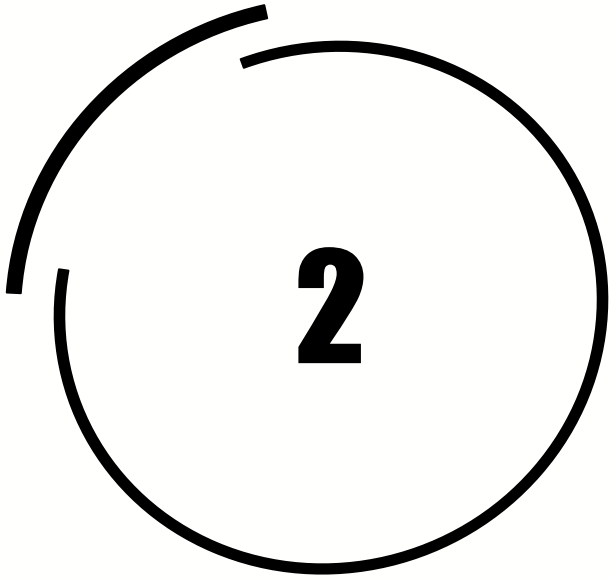
- Software-level digital certificate
  - General used
  - But vulnerable to cyber attack

- Physical characteristic
  - Naturally embedded inside a drone
  - Could be used as additional authentication with a digital certificate

University of Glasgow

# Our Contribution

- Flying drone authentication
- Explore the setting of the Mel-frequency cepstral coefficient (MFCC)
- Performance of eight machine learning methods
- Acoustic fingerprint = body × propellers
- Closed set + Open set authentication problems




# Dataset Collection

# Recording Room

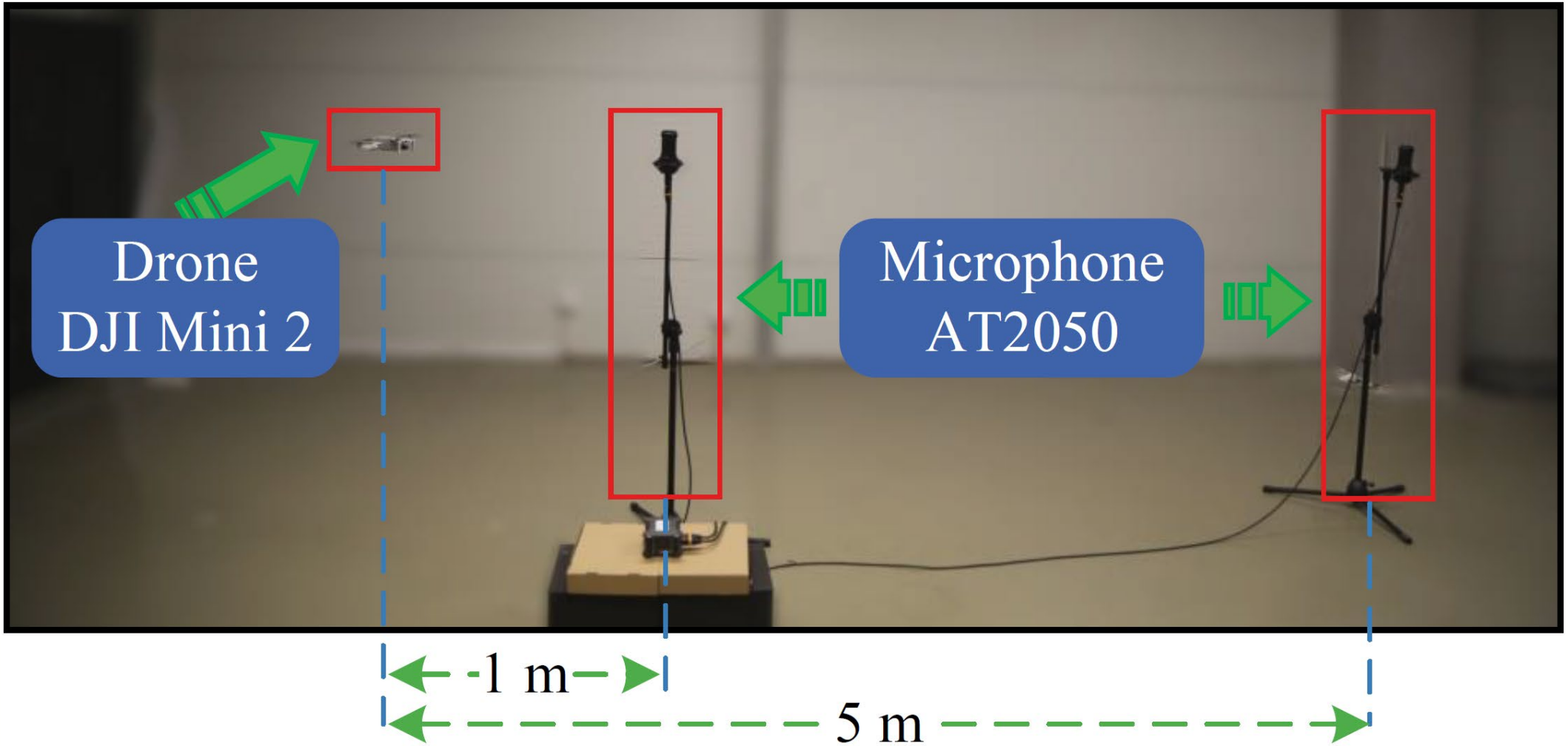
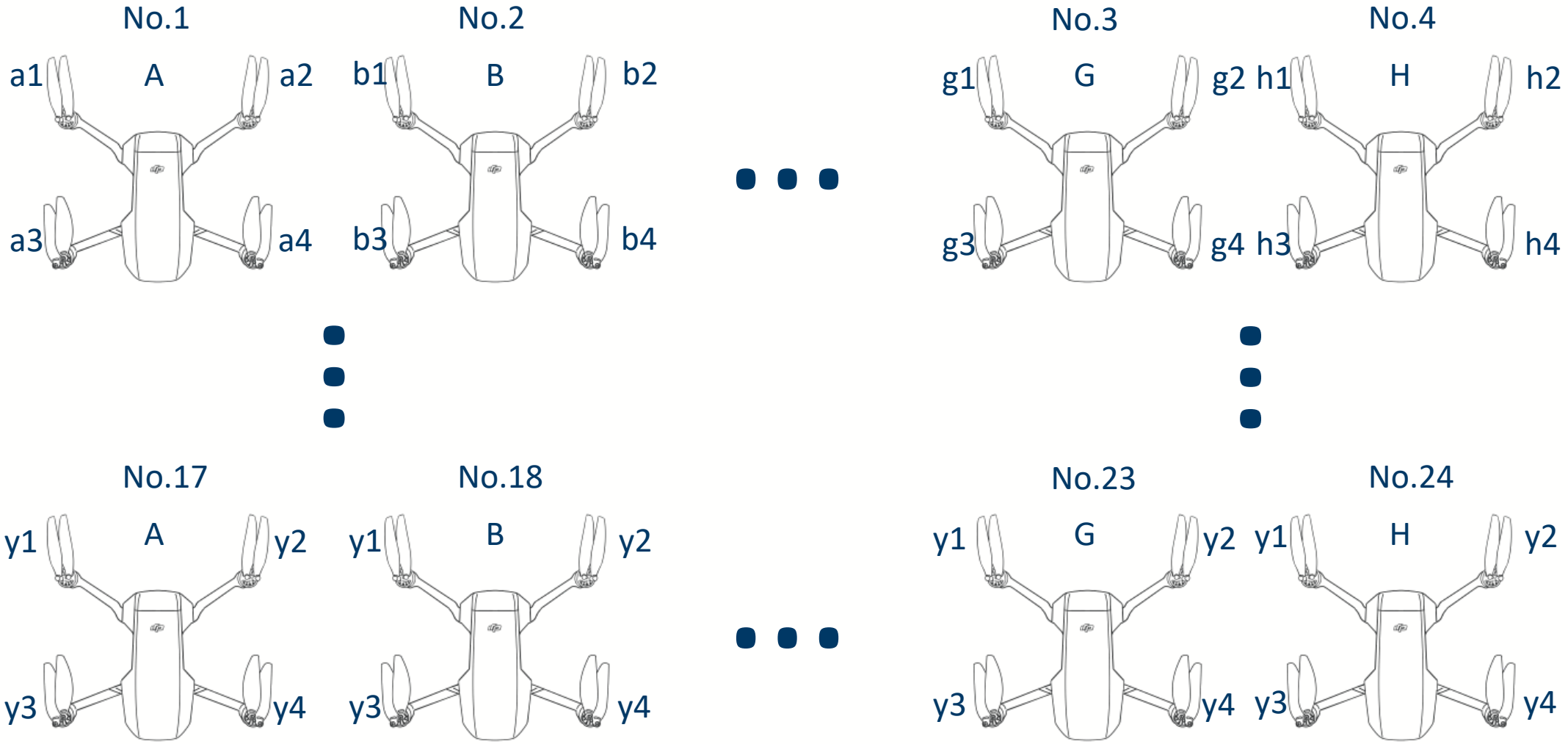



Figure: Recording room setup

# Drone No.




Combination of drone body and propellers

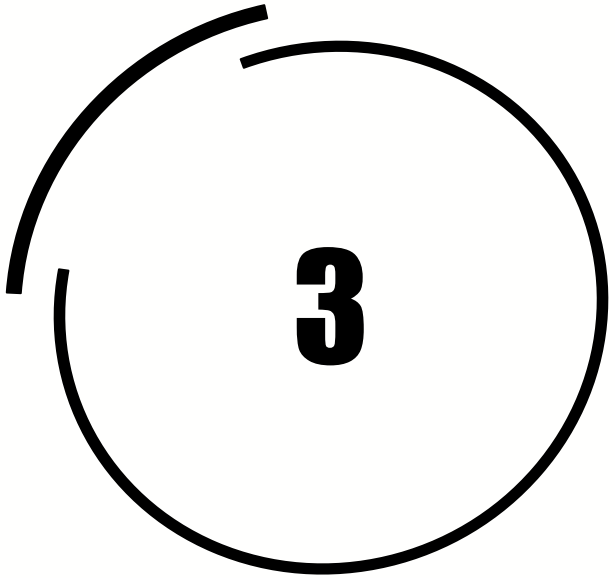
University of Glasgow

# Dataset

- DS1: No.1 – No.8
- DS2: No.1 – No.24
- DS1N: AWGN + DS1
  - 0 dB SNR
- DS2N: AWGN + DS2
  - 93 levels of SNR
  - SNR range from -8.00 dB to 15.00 dB
- 60 minutes of real indoor noise

| Drone No. | Combination | 1m (s) | 5m (s) | Total (s) |
|---|---|---|---|---|
| 1 | "A" & a1-a4 | 609.94 | 609.94 | 1219.88 |
| 2 | "B" & b1-b4 | 605.00 | 605.00 | 1210.00 |
| 3 | "C" & c1-c4 | 612.01 | 612.01 | 1224.02 |
| 4 | "D" & d1-d4 | 606.00 | 606.00 | 1212.01 |
| 5 | "E" & e1-e4 | 605.93 | 605.93 | 1211.87 |
| 6 | "F" & f1-f4 | 605.93 | 605.93 | 1211.87 |
| 7 | "G" & g1-g4 | 606.00 | 606.00 | 1212.01 |
| 8 | "H" & h1-h4 | 607.07 | 607.07 | 1214.14 |
| 9 | "A" & x1-x4 | 609.94 | 609.94 | 1219.88 |
| 10 | "B" & x1-x4 | 604.93 | 604.93 | 1209.87 |
| 11 | "C" & x1-x4 | 615.08 | 615.08 | 1230.16 |
| 12 | "D" & x1-x4 | 608.07 | 608.07 | 1216.14 |
| 13 | "E" & x1-x4 | 603.93 | 603.93 | 1207.87 |
| 14 | "F" & x1-x4 | 607.00 | 607.00 | 1214.01 |
| 15 | "G" & x1-x4 | 610.07 | 610.07 | 1220.15 |
| 16 | "H" & x1-x4 | 608.00 | 608.00 | 1216.01 |
| 17 | "A" & y1-y4 | 626.02 | 626.02 | 1252.05 |
| 18 | "B" & y1-y4 | 605.93 | 605.93 | 1211.87 |
| 19 | "C" & y1-y4 | 607.07 | 607.07 | 1214.14 |
| 20 | "D" & y1-y4 | 627.96 | 627.96 | 1255.92 |
| 21 | "E" & y1-y4 | 604.93 | 604.93 | 1209.87 |
| 22 | "F" & y1-y4 | 605.00 | 605.00 | 1210.00 |
| 23 | "G" & y1-y4 | 605.00 | 605.00 | 1210.00 |
| 24 | "H" & y1-y4 | 635.96 | 635.96 | 1271.93 |
| Total | - | 14642.89 | 14642.89 | 29285.79 |

Table: Collected Drone Audio




# MFCC Exploration

# Range of Useful Frequency

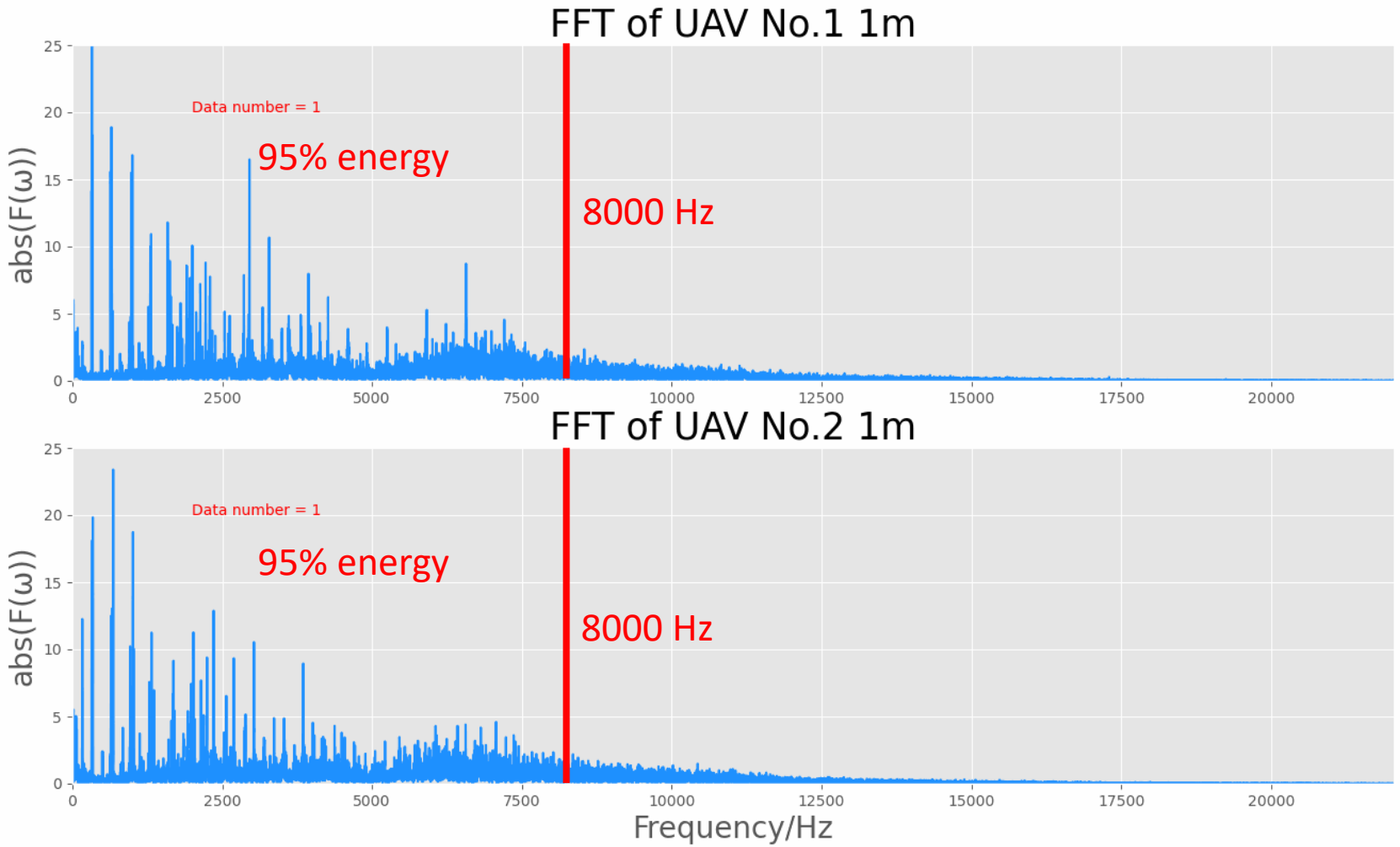



Figure: Spectrum of Drone No.1 and No.2

University of Glasgow

# Feature Extraction

- Mel-frequency cepstral coefficient (MFCC)
- Delta MFCC (DMFCC)
  - Difference between two MFCC
- Delta-Delta MFCC (DDMFCC)
  - Difference between two DMFCC
- Reduce the instantaneous noise via feature normalization
  - $v'_{\text{Feature}} = \frac{v_{\text{Feature}}}{||v_{\text{Feature}}||}$

# Eight Widely Used Machine Learning Method

- Linear Discriminant Analysis (LDA)
- Quadratic Discriminant Analysis (QDA)
- Linear kernel Support Vector Machine (LSVM)
- Radial Basis Function kernel Support Vector Machine (RBF-SVM)
- K-Nearest Neighbor (KNN)
- Decision Tree (DT)
- Random Forest (RF)
- Gaussian Naïve Bayes (GNB)

University of Glasgow

# Influence of Frame Length on Accuracy

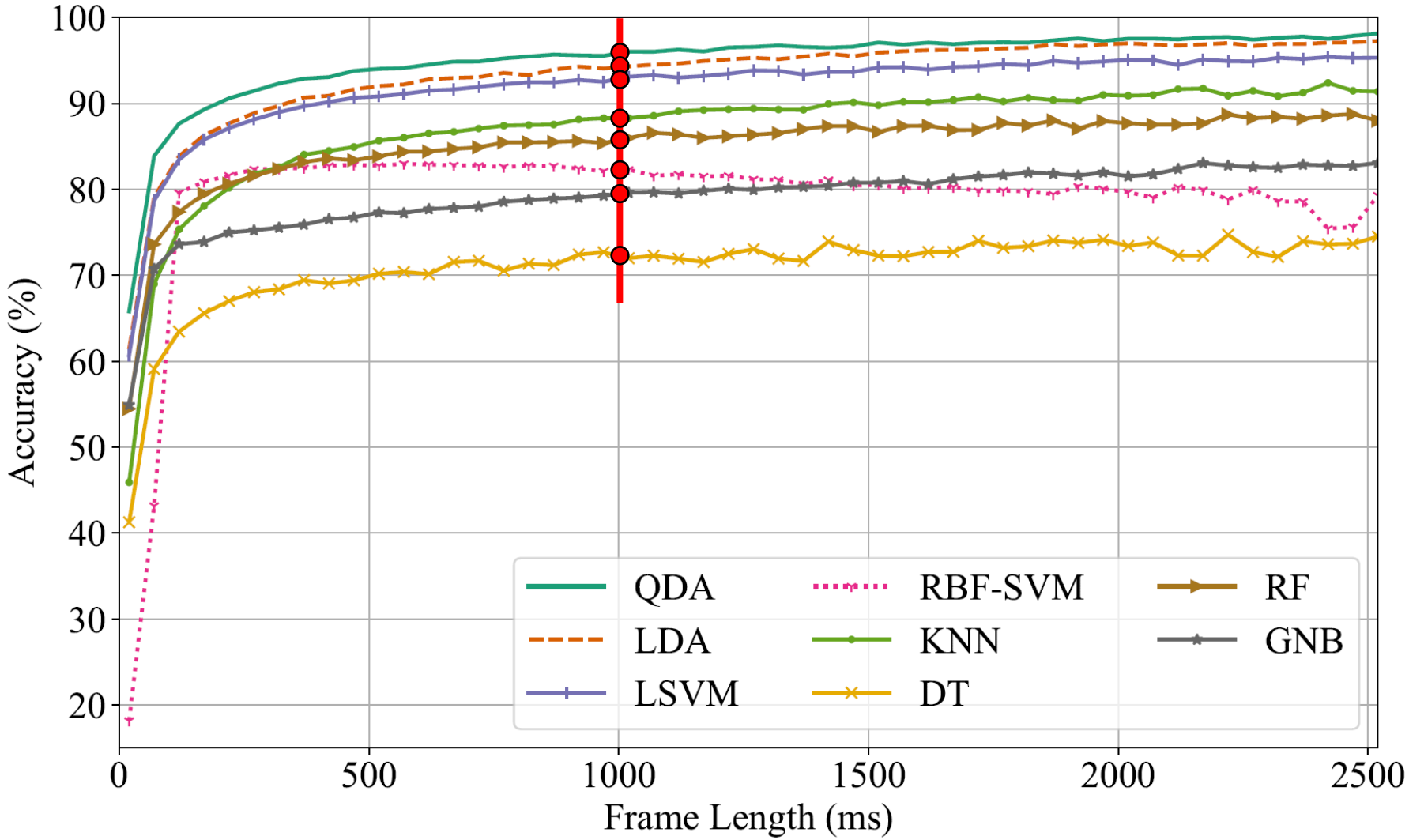
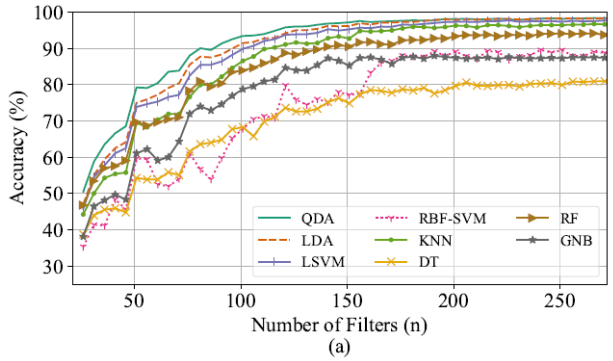
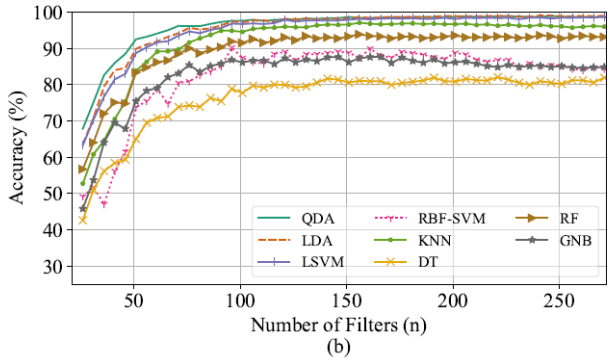
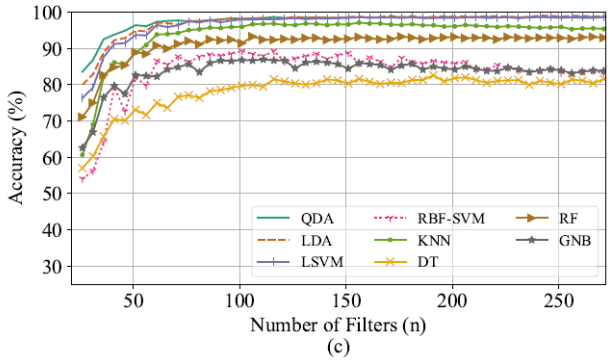
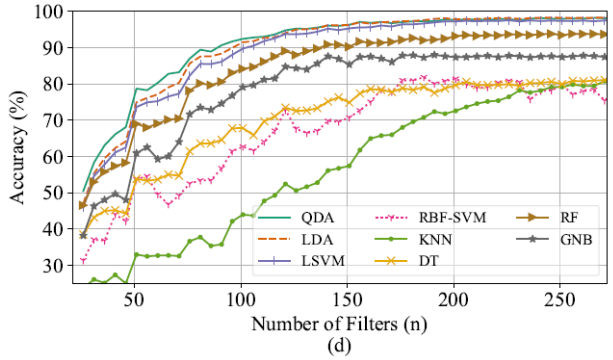
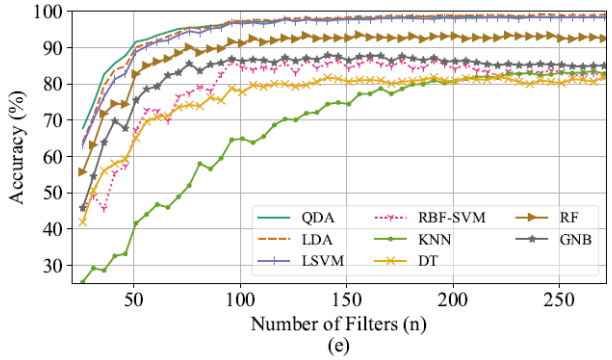
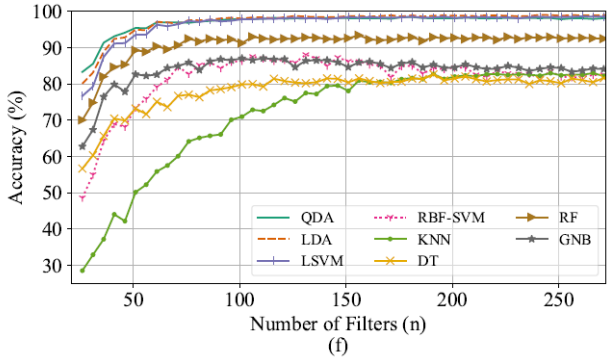
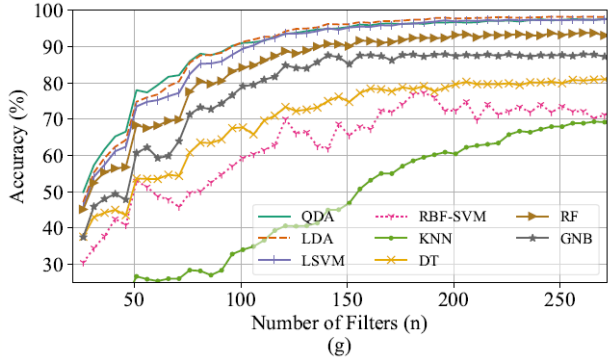
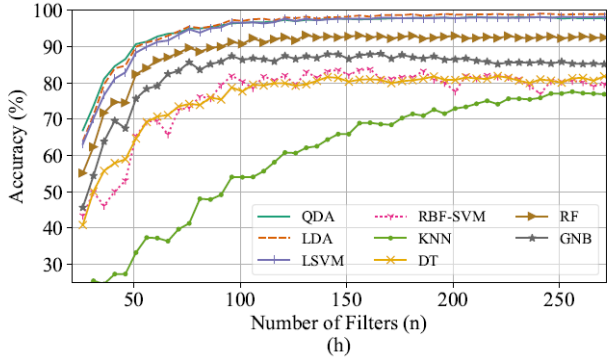
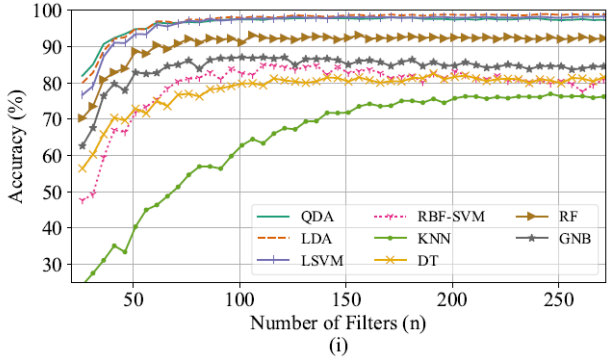



Figure: the influence of frame length on accuracy

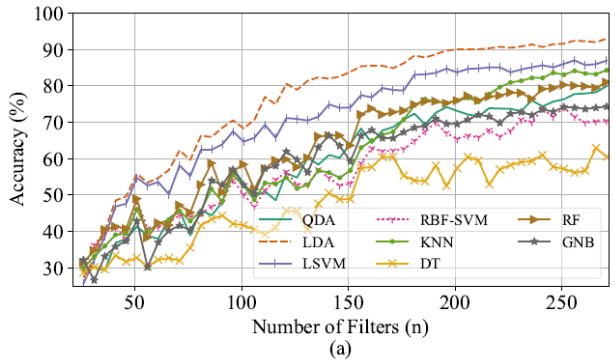
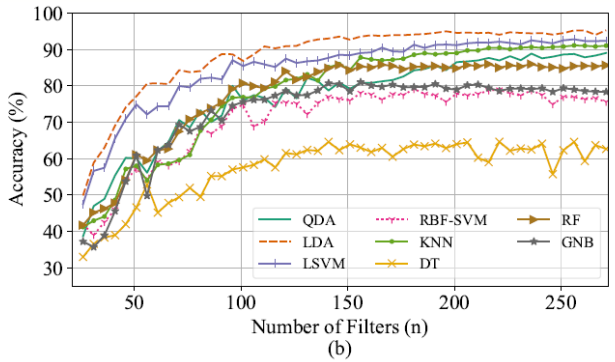
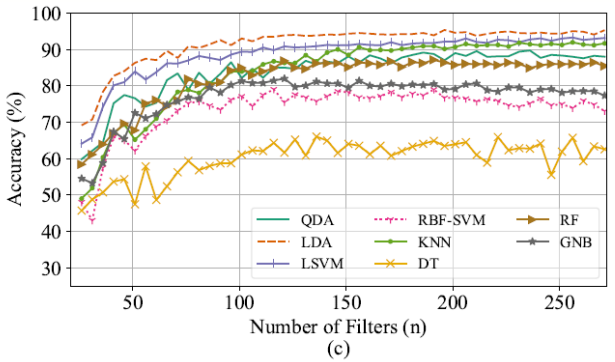
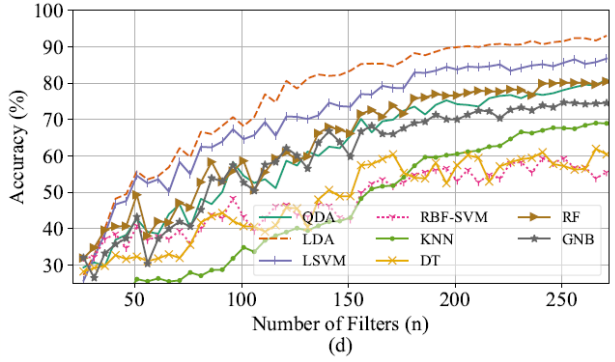
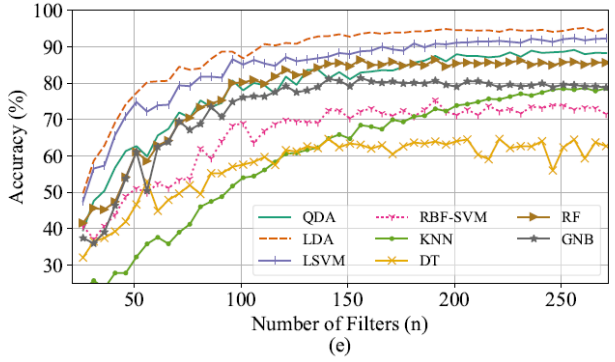
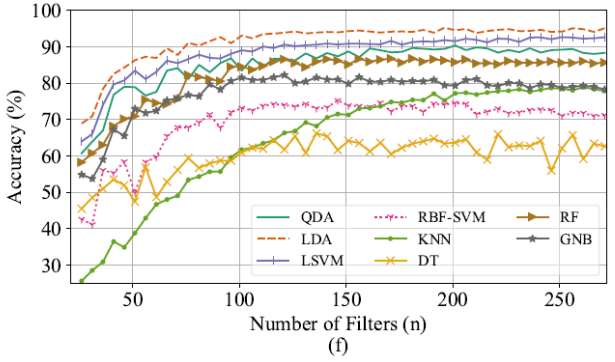
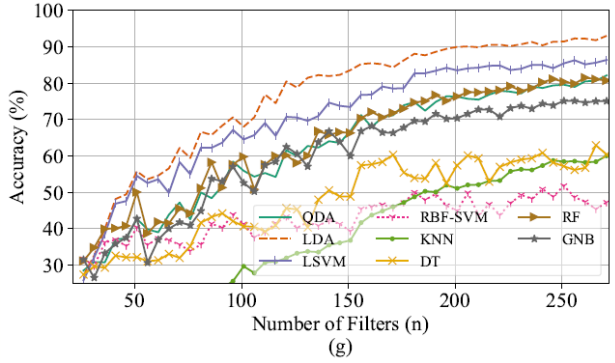
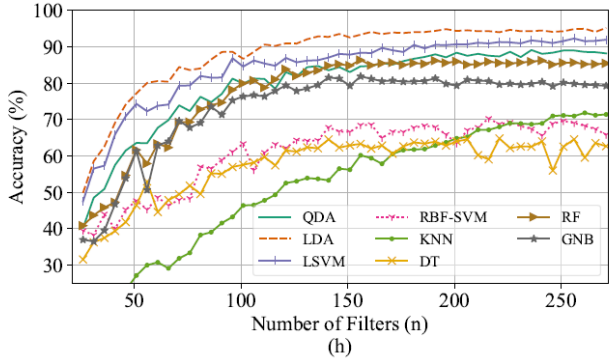
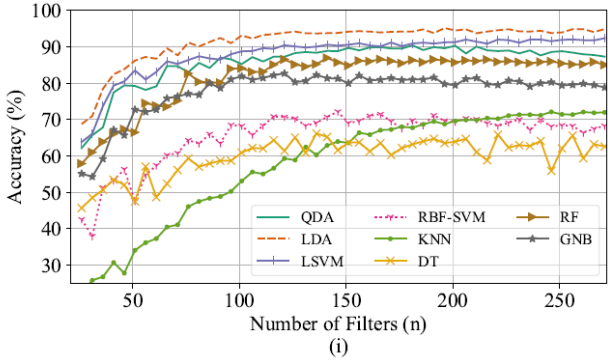
50 filters and 49 features (from 2 to 50) of MFCC are used

# Filter-varying Experiment – DS1

| | One-third | Two-thirds | All |
|---|---|---|---|
| MFCC |  |  |  |
| MFCC + DMFCC |  |  |  |
| MFCC + DMFCC + DDMFCC |  |  |  |

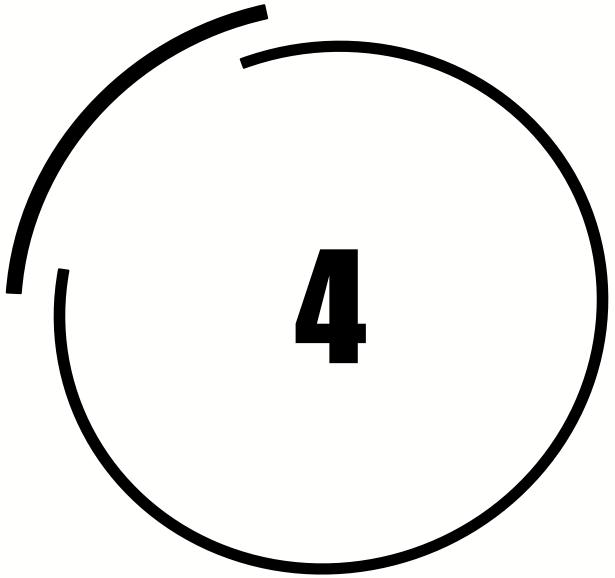
University of Glasgow

# Filter-varying Experiment – DS1N

| | One-third | Two-thirds | All |
|---|---|---|---|
| MFCC |  |  |  |
| MFCC + DMFCC |  |  |  |
| MFCC + DMFCC + DDMFCC |  |  |  |

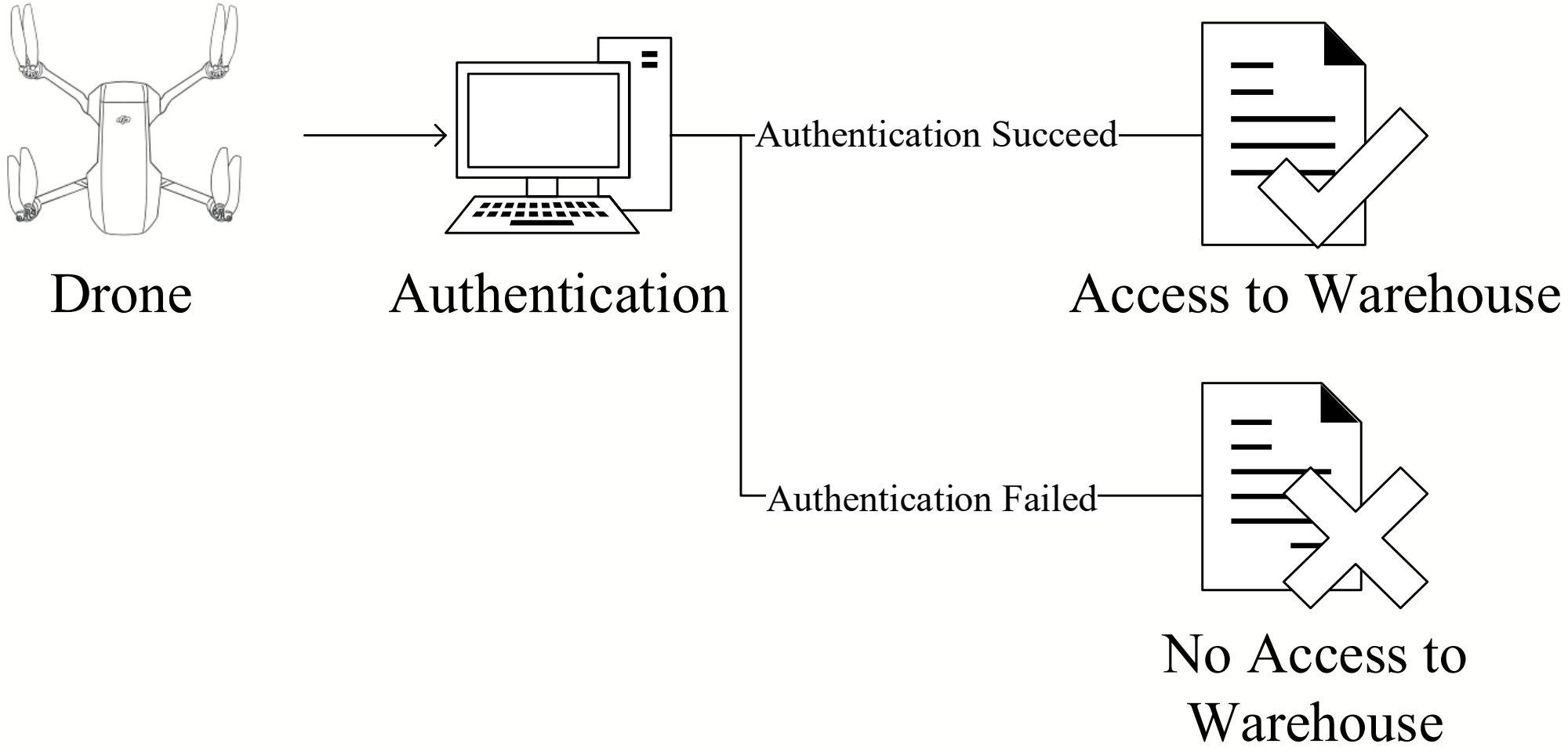
# Feature Extraction Configuration

- Frame length: 1000ms
- Frame overlap: 50%
- Number of filters: 201
- Number of used features: from 2 to 201 features
- Type of features: only MFCC




# Security Study

# Security Study – Threat Model



# Security Study – Design

- Background drones
  - 60 minutes of real indoor noise
  - 8 drones
- Registered drones
  - 8 drones
- Attack drones
  - 8 drones
- No overlap between different types

University of Glasgow

# Security Study – Setup

| Experiment No. | Registered Drone No. | Background Drone No. | Attack Drone No. |
|---|---|---|---|
| 1 | 1, 2, 3, 4, 5, 6, 7, 8 | 9, 10, 11, 12, 13, 14, 15, 16 | 17, 18, 19, 20, 21, 22, 23, 24 |
| 2 | 1, 2, 4, 7, 10, 16, 17, 20 | 3, 5, 6, 14, 15, 18, 19, 21 | 8, 9, 11, 12, 13, 22, 23, 24 |
| 3 | 3, 5, 9, 14, 16, 17, 19, 24 | 2, 6, 8, 11, 12, 15, 18, 21 | 1, 4, 7, 10, 13, 20, 22, 23 |
| 4 | 3, 12, 13, 16, 20, 21, 22, 24 | 6, 7, 8, 9, 14, 15, 17, 18 | 1, 2, 4, 5, 10, 11, 19, 23 |
| 5 | 2, 5, 6, 8, 14, 17, 18, 20 | 1, 4, 7, 9, 10, 12, 19, 23 | 3, 11, 13, 15, 16, 21, 22, 24 |
| 6 | 1, 10, 11, 15, 17, 18, 23, 24 | 3, 5, 8, 9, 12, 13, 19, 20 | 2, 4, 6, 7, 14, 16, 21, 22 |
| 7 | 2, 3, 4, 5, 11, 12, 15, 24 | 1, 6, 7, 10, 16, 18, 21, 22 | 8, 9, 13, 14, 17, 19, 20, 23 |
| 8 | 4, 5, 7, 8, 10, 17, 18, 21 | 1, 3, 11, 13, 15, 19, 23, 24 | 2, 6, 9, 12, 14, 16, 20, 22 |
| 9 | 4, 5, 6, 11, 12, 13, 14, 23 | 1, 2, 3, 17, 19, 20, 22, 24 | 7, 8, 9, 10, 15, 16, 18, 21 |
| 10 | 5, 9, 10, 12, 17, 18, 21, 23 | 1, 6, 7, 13, 15, 16, 20, 22 | 2, 3, 4, 8, 11, 14, 19, 24 |

Table: Attack Experiment Setup

University of Glasgow

# Security Study – Registered Drones

| Experiment No. | QDA (%) | LDA (%) | LSVM (%) | RBF-SVM (%) | KNN (%) | DT (%) | RF (%) | GNB (%) |
|---|---|---|---|---|---|---|---|---|
| 1 | 97.16 | 95.24 | 97.28 | 35.41 | 95.53 | 75.24 | 89.30 | 83.80 |
| 2 | 95.66 | 91.69 | 92.49 | 9.92 | 93.78 | 70.12 | 77.84 | 83.84 |
| 3 | 94.23 | 87.78 | 90.76 | 2.68 | 93.05 | 64.50 | 71.89 | 80.60 |
| 4 | 94.30 | 90.32 | 91.34 | 10.71 | 91.91 | 65.09 | 74.86 | 85.12 |
| 5 | 94.56 | 88.21 | 89.19 | 10.94 | 93.67 | 69.93 | 76.02 | 85.16 |
| 6 | 92.53 | 86.85 | 88.74 | 6.14 | 90.44 | 57.52 | 67.96 | 72.48 |
| 7 | 95.56 | 94.54 | 94.85 | 23.84 | 95.99 | 72.64 | 83.30 | 87.67 |
| 8 | 92.97 | 86.14 | 88.64 | 7.06 | 90.00 | 58.48 | 69.31 | 69.70 |
| 9 | 94.29 | 92.24 | 92.42 | 18.53 | 95.52 | 69.98 | 82.34 | 88.72 |
| 10 | 90.60 | 83.39 | 85.40 | 5.31 | 87.28 | 54.80 | 60.21 | 66.05 |
| Average | 94.19 | 89.64 | 91.11 | 13.05 | 92.71 | 65.83 | 75.30 | 80.31 |

Table: Recall of Authentication on Registered Drones

University of Glasgow

# Security Study – Unregistered Drones

| Experiment No. | QDA (%) | LDA (%) | LSVM (%) | RBF-SVM (%) | KNN (%) | DT (%) | RF (%) | GNB (%) |
|---|---|---|---|---|---|---|---|---|
| 1 | 99.78 | 98.51 | 99.69 | 100.00 | 97.96 | 87.45 | 99.88 | 79.21 |
| 2 | 77.93 | 60.90 | 57.64 | 99.43 | 46.57 | 56.23 | 73.85 | 20.64 |
| 3 | 73.85 | 63.79 | 68.06 | 99.71 | 42.60 | 59.74 | 85.33 | 16.52 |
| 4 | 90.95 | 84.81 | 84.50 | 100.00 | 73.82 | 73.98 | 94.05 | 44.09 |
| 5 | 75.89 | 60.10 | 67.33 | 99.95 | 52.77 | 60.60 | 72.40 | 16.23 |
| 6 | 87.64 | 67.85 | 72.71 | 96.74 | 65.12 | 74.06 | 90.16 | 60.47 |
| 7 | 77.86 | 63.19 | 60.98 | 98.76 | 55.03 | 60.11 | 80.46 | 16.72 |
| 8 | 84.50 | 58.08 | 56.49 | 95.58 | 55.02 | 56.06 | 91.33 | 41.40 |
| 9 | 65.93 | 53.98 | 45.34 | 96.94 | 29.71 | 38.56 | 70.34 | 8.64 |
| 10 | 89.19 | 53.75 | 51.62 | 93.85 | 50.55 | 57.99 | 88.95 | 35.52 |
| Average | 82.35 | 66.50 | 66.44 | 98.10 | 56.92 | 62.48 | 84.68 | 33.94 |

Table: Recall of Authentication on Unregistered Drones

University of Glasgow

# Conclusion


- First work to authenticate flying drones via acoustic fingerprints
- Find effective feature extraction settings
- Address open set authentication problem
  - QDA outperformed other methods
    - highest average recall (94.19%) in registered drones
    - third-highest average recall (82.35%) in unregistered drones

https://github.com/Eidos1970/Drone-Authentication-via-Acoustic-Fingerprint

Reach me via y.diao.1@research.gla.ac.uk


University of Glasgow
Thanks for listening
Q & A