Artifact Evaluation of Drone Authentication via Acoustic Fingerprint

Aryan Puri
University of Adelaide
Australia
a1914021@adelaide.edu.au

ABSTRACT

This project scope paper is an outline of my plan for evaluating the acoustic fingerprint-based drone authentication system presented in the paper "Drone Authentication via Acoustic Fingerprint." The evaluation will assess function, performance and reliability under various working conditions. The attached artifacts like code and machine learning models will be tested rigorously to verify the claims made in the original paper. The ultimate objective is to understand how viable it is as a security measure for drones and its robustness against noise.

1 INTRODUCTION

In the drone industry, we can see their applications becoming increasingly crucial in sensitive areas like surveillance, delivery, and emergency response. This sensitivity of applications raises a greater demand for reliable, safer and more “unhackable” methods of authentication.

Proper authentication prevents unauthorized access, helping to protect both the drone and the data it collects or transmits and ensures access is through verified operators. It also prevents drones from accessing resources and areas they are not authorized to use or enter.

Before the parent paper was published, solutions focused on drone detection and drone classification. Also, software-level digital certificates were used to indicate the individual identity of each drone. This left them vulnerable to impersonation.

Authors realized if physical attributes, deeply embedded in each drone, were used there was room for improvement through the inherence factor to authentication. This motivated them to research and develop the acoustic fingerprinting via MFCC based authentication method.

2. PAPER REVIEW

The parent paper is proposing a sound-differentiation based authentication method, specifically through features like Mel-frequency cepstral coefficients (MFCC) and their derivatives. It builds upon previous works in the domain of drone detection, classification and their sounds features. The established research highlighting MFCC as an effective method for extracting features from drone audio, led them to choose it. They have not only performed authentication, but also provide a reference to set feature extraction parameters for further research.

2.1 Gathering and Processing Data:

For creating the dataset, DJI’s Mini2 drones were used in a recording room, approximately 5m in width, 8m in length and 3m in height. The mic was a multi-pattern condenser type and recorded to a WAV format as a mono-channel.

The datasets, **DS1, DS2, DS1N and DS2N** were created from the collected data. DS1 contained drone audio from just 8 variations of drone configurations while DS2 contained all samples.

Additive White Gaussian Noise (AWGN) was then added to the above datasets, one with 0dB SNR, forming DS1N a*nd* other with 93 levels of SNR ranging from -8.00dB to15.00dB with a step of 0.25dB created DS2N. DS1andDS1N were tested upon to select appropriate configuration for feature extraction. Additionally, 60 minutes of indoor noise audio was used with DS2 for security studies in the authentication experiment.

AWGN is useful as it approximates the kind of background noise many systems face in real-world applications, such as thermal noise in electronics or background hum in audio signals. Adding AWGN, simulated the surrounding of systems under noisy conditions, allowing tests for resilience and accuracy.

Then investigate for the proper setting of the MFCC parameters for authentication began, using accuracy as a performance indicator:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN},$$

where TP is true positive, TN is true negative, FP is false positive, and FN is false negative.

Analysis of the dataset showed that almost 95% of the energy is located within the frequency range of 0-8 kHz, also used for other similar studies. Small frames were extracted from this, based on length determined by testing the eight machine learning methods on drone audio in DS1. Longer frames, enhanced features but are not used due to practical limitations. 1000ms was chosen to have a good balance between accuracy and the size of the extracted feature data

Three main factors influence the accuracy of this authentication scheme. the number of filters, the number of features used, and the inclusion of higher-order derivatives.

Filters in the MFCC process split the frequency spectrum into multiple bands, capturing different audio characteristics across frequencies. By varying the number of filters from 26 to 271, the researchers observed that more filters allow for finer resolution of sound features, improving the ability to capture subtle differences in drone sounds.

Features generated by each filter, which are coefficients, are typically kept between 13 and 40 in related studies. However, for drone authentication, the study found that using a greater number of features improves accuracy due to the complex sound patterns that drones produce. Therefore, configurations with one-third, two-thirds, and all available features were tested to determine if more features consistently enhance accuracy.

Including **high-level features**: While these derivatives can improve sensitivity to changes, they may also introduce noise or redundancy, impacting model performance negatively in certain cases.

Based on the above work the study concluded, optimal settings for drone authentication are1000ms frames with a 50% overlap between frames. Using,201 filters, extracting MFCC features from 2 to 201. Also, due to their unclear benefit and potential for reducing accuracy, they are not used in the final configuration. This helped them achieve higher accuracy.

2.2 Authentication Experiments:

The study tried experiments testing authentication with and without AWGN. Starting with proving, a drone with replaced propellers has unique acoustic fingerprints and can be identified separately.

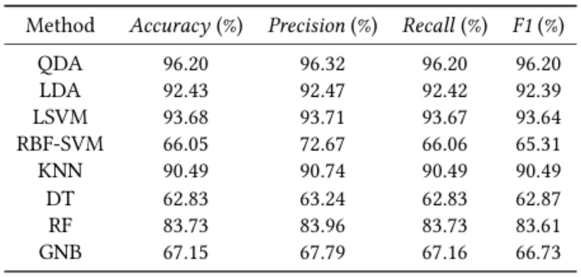
While evaluating the performance of eight machine learning methods for the authentication of 24 drones, the study examined accuracy, precision, recall, and F1-score to provide insights into how well the models identify registered drones without mistakenly classifying unregistered ones.

Accuracy measures the percentage of correctly classified drones out of the total, while **precision** is calculated as the proportion of true positive classifications (correctly authenticated drones) out of all positive predictions (both true and false positives).

Recall, on the other hand, measures proportion of true positives among the total actual positives (both true positives and false negatives).

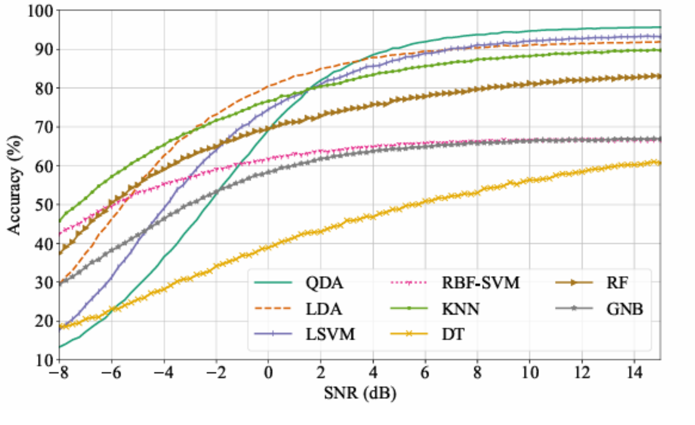
F1-score, the harmonic means of precision and recall, is crucial for evaluating the models' overall effectiveness, particularly in situations where there is a trade-off between precision and recall.

In experiment one, all models tried to authenticate 24 drones without applying AWGN. Dataset D2 was used to train and test models. It resulted in the justification of using acoustics for authentication.



Method	*Accuracy* (%)	*Precision* (%)	*Recall* (%)	*F1* (%)
QDA	96.20	96.32	96.20	96.20
LDA	92.43	92.47	92.42	92.39
LSVM	93.68	93.71	93.67	93.64
RBF-SVM	66.05	72.67	66.06	65.31
KNN	90.49	90.74	90.49	90.49
DT	62.83	63.24	62.83	62.87
RF	83.73	83.96	83.73	83.61
GNB	67.15	67.79	67.16	66.73

Once the feasibility of audio for authentication was established, the next experiment tried to test the influence of noise. While we continue to use the models trained in DS2, testing was performed on DS2N that has added AWGN. They found SNR and accuracy increased proportionally. QDA and LSVM were found to be better at high SNR, but very sensitive to low SNR. When below 0, accuracy took a hit. At 4dB SNR their accuracy plateaued and slowed growth. Assumption was drawn that at 2dB, a good performance can be achieved from all models.



2.3 Security Testing:

After success in the authentication experiments, focus was given to designing a robust drone attack study by formulating a threat model, designing an experiment and implementing it. This was to provide clarity on effectiveness in open set problems, which includes "unregistered" drones that were not in the training data.

Priority was given to determining whether registered drones can be properly authenticated and unregistered drones can be authenticated as unregistered by the system.

The researchers proceeded with the assumption that the attacker has access to a similar drone and can navigate it to a target location they are not authorized to access. The attacker would try to use it to pass authentication.

As a solution, researchers added background noise as a separate "unregistered" class to distinguish real drone sounds from potential background noise. Implementation included using DS2 with 60 minutes of real indoor noise to train a background class. The process involved running ten rounds of authentication, with each round using randomly assigned drones to the registered, background, and attack categories. For instance, drones numbered from 1-24 were shuffled so that each round had a unique combination of drones as registered, background, or attack drones. This approach ensured the system's performance was not dependent on specific drones and could generalize well across different types and combinations of sounds.

The results achieved by this experiment demonstrated that the authentication system, when optimized with MFCC features and a model like QDA, could accurately and reliably differentiate between registered and unregistered drones. The structured testing process, incorporating randomized drone assignments, noise resilience checks, and open-set configurations, established a solid foundation for future real-world implementations of acoustic-based drone authentication. This layered approach also helps ensure the system can reject unauthorized drones even when these are close copies of known models, supporting its feasibility in environments where drone impersonation threats are prevalent.

3 PROJECT PLAN

Objective: A critical evaluation of the implementation, performance, and reliability of the proposed drone authentication system based on acoustic fingerprints as detailed in the parent paper. I will focus on reproducing the experiment results, verifying the robustness of the method, and assessing its viability as a security measure against drone impersonation.

Proposed Phases:

Phase 1: Artifact Setup and Familiarization

- **Objective:** Obtain, set up, and understand the provided artifact which is available on the authors' GitHub repository.
- **Milestone:** Successfully configure the environment, including dependencies for Python, machine learning libraries, and audio processing tools as specified by the authors.
- **Deliverable:** A well-documented environment setup and verification of the code functionality on a test dataset.

Phase 2: Data Collection and Preprocessing Validation

- **Objective:** Reproduce the data collection and preprocessing steps as outlined in the paper, focusing on the extraction of Mel-frequency cepstral coefficient (MFCC) features and the application of delta and delta-delta MFCCs.
- **Milestone:** Validate the preprocessing pipeline by reproducing sample audio feature extractions and confirming alignment with the authors' reported results.
- **Deliverable:** Pre-processed datasets, with metrics matching those reported in the paper, such as accuracy of feature extraction configurations.

Phase 3: Model Re-training and Testing

- **Objective:** Re-train all 8 machine learning models using the paper's configurations and parameters on the dataset to verify the performance metrics claimed.
- **Milestone:** Try to achieve reported performance benchmarks
- **Deliverable:** A comparison table documenting the accuracy, precision, recall, and F1-score of each machine learning model against reported values.

Phase 4: Robustness Testing under Noise Conditions

- **Objective:** Test the models under simulated noisy environments using Additive White Gaussian Noise (AWGN) at varying Signal-to-Noise Ratios (SNRs) to assess the system's noise resilience.
- **Milestone:** Measure performance degradation and compare it to the noise resilience results reported by the authors (e.g., accuracy under SNR > 2 dB).
- **Deliverable:** A noise-resilience report showing performance metrics across different SNR levels, demonstrating model stability under varying noise conditions.

Phase 5: Security Testing against Impersonation and Replay Attacks

- **Objective:** Evaluate the system's ability to detect impersonation by unregistered drones and explore its susceptibility to replay attacks using pre-recorded drone audio.
- **Milestone:** Successfully reproduce results for unregistered drone detection, measuring recall for registered vs. unregistered drones. Test replay attacks to assess any vulnerabilities in the authentication process.
- **Deliverable:** A security report analyzing the system's robustness against impersonation and replay attacks,

with recommendations for mitigating any observed weaknesses.

Phase 6: Documentation and Artifact Analysis

- **Objective:** Compile a comprehensive evaluation report detailing the findings, challenges, and any discrepancies between the reproduced results and those reported in the paper.

- **Milestone:** Complete an artifact evaluation report highlighting the reproducibility of the study, challenges encountered, and suggested improvements for the authors.

- **Deliverable:** Final artifact evaluation report summarizing key insights, with conclusions on the viability and robustness of the drone authentication method.

At any point during testing, if the system's performance significantly deviates from the paper's claims under noisy conditions, I will experiment with different noise filters or alternative audio processing techniques to improve results.

REFERENCES

[1] Yufeng Diao, Yichi Zhang, Guodong Zhao, and Mohamed Khamis. 2022. DroneAuthentication via Acoustic Fingerprint. In Annual Computer Security Applications Conference (ACSAC '22), December 5–9, 2022, Austin, TX, USA. ACM,NewYork,NY,USA,11pages.https://doi.org/10.1145/3564625.3564653

[2] Chen, C.-H., & Hu, J.-C. (2019). **"Acoustic signal-based UAV recognition for secure access control."** *IEEE Access, 7*, 84365–84374. doi:10.1109/ACCESS.2019.2923293

[3] Davis, S. B., & Mermelstein, P. (1980). **"Comparison of parametric representations for monosyllabic word recognition in continuously spoken sentences."** *IEEE Transactions on Acoustics, Speech, and Signal Processing*, 28(4), 357–366. doi:10.1109/TASSP.1980.1163420

[4] Rasel, M. R., Shibata, T., & Kajiwara, Y. (2021). **"UAV authentication and security based on acoustic features."** *Sensors, 21*(17), 5682. doi:10.3390/s21175682

[5] Bouabdallah, F., & Bouzouita, R. (2019). **"UAV security and privacy: An overview."** *IEEE Communications Surveys & Tutorials, 21*(4), 3846–3880. doi:10.1109/COMST.2019.2932572

[6] Gupta, L., Jain, R., & Vaszkun, G. (2016). **"Survey of important issues in UAV communication networks."** *IEEE Communications Surveys & Tutorials, 18*(2), 1123–1152. doi:10.1109/COMST.2015.2495297

[7] Lim, H., Yoon, Y., Lee, S., & Lee, D. (2017). **"Drone sound detection using a deep convolutional neural network."** *IEEE Transactions on Emerging Topics in Computational Intelligence, 2*(1), 18–25. doi:10.1109/TETCI.2017.2787142

[8] Chaves, H. M., & Freitas, E. P. (2021). **"Machine learning approaches for noise-robust speech recognition: A review."** *IEEE Access, 9*, 74456–74475. doi:10.1109/ACCESS.2021.3081229

[9] Loukas, G., et al. (2020). **"Cyber-physical systems security for drone applications."** *Computers & Security, 89*, 101682. doi:10.1016/j.cose.2019.101682

[10] Zhang, S., et al. (2022). **"A survey on anti-spoofing and secure authentication for UAVs."** *ACM Computing Surveys, 54*(4), Article 82. doi:10.1145/3456710

[11] Bishop, C. M. (2006). "Pattern recognition and machine learning." Springer.

[12] Kotsiantis, S. B., Zaharakis, I., & Pintelas, P. (2007). **"Supervised machine learning: A review of classification techniques."** *Emerging Artificial Intelligence Applications in Computer Engineering, 160*(1), 3-24.

[13] Varghese, T., & George, M. (2017). **"Improving the robustness of UAV signal recognition in noisy environments."** *IEEE Transactions on Signal Processing, 65*(12), 3036–3048. doi:10.1109/TSP.2017.2670937

[14] Mahmood, R., & Khan, I. (2019). **"Enhancing noise resilience in UAV audio authentication."** *Journal of Applied Acoustics, 145*, 107271. doi:10.1016/j.apacoust.2018.12.011