SoundUAV: Towards Delivery Drone Authentication via Acoustic Noise Fingerprinting

Soundarya Ramesh
sramesh@comp.nus.edu.sg
National University of Singapore

Thomas Pathier
pathiert@comp.nus.edu.sg
National University of Singapore

Jun Han
junhan@comp.nus.edu.sg
National University of Singapore

ABSTRACT

Drones are gaining a lot of traction in a wide spectrum of applications. This popularity makes them attractive attack surfaces, which necessitates the need for ensuring their security. Specifically, in the case of drone delivery, an attacker drone may impersonate the legitimate one in order to steal packages, which makes drone authentication important. Recent efforts have pushed to incorporate digital certificates as an authenticator for drones. However, such software-based techniques are often compromised and can be launched on a large scale, making them a bigger threat. To this end, we propose *SoundUAV* as an additional factor of authentication that leverages differences in the acoustic noise characteristics of drones to *fingerprint* them. These differences are caused due to manufacturing defects in their motors, making them hard to replicate. Moreover, *SoundUAV* does not require any hardware modifications to existing drones as they leverage the freely available sound information, and it is also robust to large-scale attacks as the attacks involve hardware alterations. To test the feasibility of *SoundUAV*, we evaluate it on 54 motors, and 11 drones of the same make and model, and report fingerprinting accuracy of 99.48%.

CCS CONCEPTS

• **Security and privacy → Authentication**; • **Hardware → Sensor applications and deployments**; **Sound-based input / output**.

KEYWORDS

Drones, Authentication, Acoustics, Fingerprinting

ACM Reference Format:
Soundarya Ramesh, Thomas Pathier, and Jun Han. 2019. *SoundUAV*: Towards Delivery Drone Authentication via Acoustic Noise Fingerprinting. In *The 5th Workshop on Micro Aerial Vehicle Networks, Systems, and Applications (DroNet'19), June 21, 2019, Seoul, Republic of Korea.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3325421.3329768

1 INTRODUCTION

Drone-based delivery is gaining considerable attention due to their cost effectiveness and timeliness, with a market projection of $29B within the next decade [4, 48]. In this regard, online retailers such as Amazon and Alibaba are prototyping systems to deliver goods from their warehouse to customers via drones [3, 27]. Courier service companies including UPS and DHL, in addition to postal services are also initiating the use of drones for their expedited delivery [16, 43, 45, 46].

With this soaring popularity of drone delivery comes the downside of numerous attack possibilities. Among many attacks, we envision a likely attack in a drone-based delivery setting, namely drone impersonation attack. Specifically, in the case of drone-based courier services where a delivery drone collects package from a sender and delivers it to designated recipient, an attacker drone may impersonate the legitimate one in order to steal the package. This is analogous to a real-world human-based delivery impersonation attack where adversaries pose themselves as delivery personnel for monetary benefits [10, 22, 32]. With autonomous drone delivery becoming closer to reality, authentication of drones is critical for delivery services in order to prevent such impersonation attacks.

Several companies and government organizations have put forth preliminary techniques for the drone authentication problem, such as engraving of registration number on the drone's exterior and broadcasting unencrypted identity information [28, 30]. As these techniques are susceptible to copy attacks, DigiCert and Airmap proposed utilizing Public Key Infrastructure (PKI), specifically leveraging digital certificates for drones [9]. Digital certificates enable publicly verifiable identity, which in turn serves as a "virtual license plate" for drones. Unfortunately using such software-based solutions may still pose potential risks as we witness numerous attacks which compromise certificates, by attacking certificate authorities [6, 8, 24] and web servers [12, 51], in addition to issuing fake certificates [19], ultimately resulting in successful impersonation.

In order to defend against the aforementioned software-based impersonation attacks, we ask the question: "Can we enable a second factor of authentication for delivery drones that – *(1) is difficult to replicate*, *(2) is robust to large-scale attacks*, and *(3) requires no hardware modifications to drones*?". To answer this question, we explore the possibility of utilizing acoustic noise of drones to uniquely identify or *fingerprint* them. To this end, we present *SoundUAV*[1], an acoustics-based fingerprinting system, as an additional factor of authentication, that leverages hardware imperfections of brushless motors, which are a major contributor for noise in drones.

Figure 1 illustrates an exemplary scenario of *SoundUAV*'s two-factor authentication for drone delivery services. In this case, ① sender requests for a delivery drone from the courier company's app, which ② sends a drone to the docking station outside the sender's residence. On the drone's arrival, the sender verifies its digital certificate (i.e., first factor of authentication). Subsequently, ③ the microphone in the station captures the drone's sound, which is

[1] pronounced as "*sound wave*"

DroNet'19, June 21, 2019, Seoul, Republic of Korea

ACM ISBN 978-1-4503-6772-1/19/06…$15.00
https://doi.org/10.1145/3325421.3329768

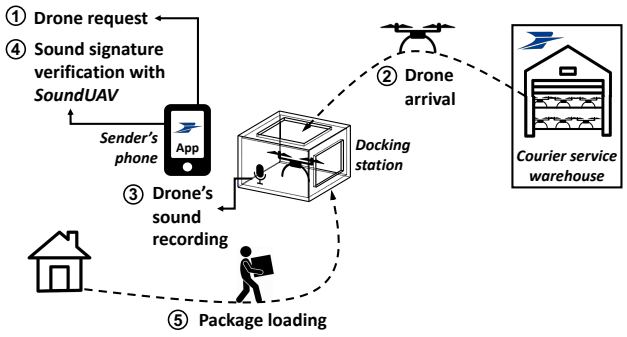


Figure 1: Figure depicts an exemplary scenario of *SoundUAV*'s two factor authentication for drone delivery. ① Sender requests for a drone through the delivery app. ② A drone arrives at the docking station closest to the sender. ③ The microphone in the station captures the drone's sound. ④ The recording is verified by *SoundUAV* on the app. ⑤ On successful verification, the sender loads the package.

④ utilized by *SoundUAV* to perform acoustics-based fingerprinting (i.e., second factor of authentication). Upon successful verification, ⑤ the sender hands over the goods to the drone.

Designing *SoundUAV* comes with the key challenge of finding hardware imperfections of motors from acoustic signals of drones that are sufficiently distinguishable even across drones of same make and model. We address this challenge by extracting features from electromagnetic and mechanical noise of motors to train a classification model of legitimate drones (e.g., drones that belong to a courier service). *SoundUAV* uses the trained model for authentication of drones during delivery.

Utilizing acoustic noise characteristics of drones is advantageous for several reasons. First, it is hard to forge the acoustic fingerprints as *SoundUAV* leverages the manufacturing irregularities which are difficult to replicate. Second, *SoundUAV* is robust to large-scale attacks as the attacks on *SoundUAV* would require alterations to the motors in drones. Third, *SoundUAV* takes advantage of the acoustic noise that is already prominent in drones, thereby requiring no hardware modifications on them.

To evaluate *SoundUAV* we collect audio data from 54 motors across six different makes and models. We further collect recordings from 11 quadcopter drones within the same make and model. We extract relevant features that exhibit uniqueness of drones from the recordings and use them to train an SVM classifier. With this trained model, we report drone fingerprinting accuracy of 99.48%.

The rest of the paper is organized as follows. In Section 2, we define our system and threat models, and provide necessary background information in Section 3. Subsequently, we present *SoundUAV*'s design and evaluation in Sections 4 and 5, respectively. We discuss deployment considerations and related work in Sections 6 and 7, respectively, and conclude in Section 8.

2 SYSTEM AND THREAT MODEL

In this section, we present *SoundUAV*'s system and threat models.

System Model. The main *goal* of *SoundUAV* is to provide authentication of delivery drones by leveraging the hardware imperfections of their motors that are reflected in the drones' acoustic emanations. To provide such an authentication system, we *require* *SoundUAV* to be (1) difficult to forge, (2) robust to large-scale attacks, and (3) free of any hardware modifications on drones. In order to meet these requirements, we *assume* that the drone is authenticated inside a courier service docking station with a built-in microphone.

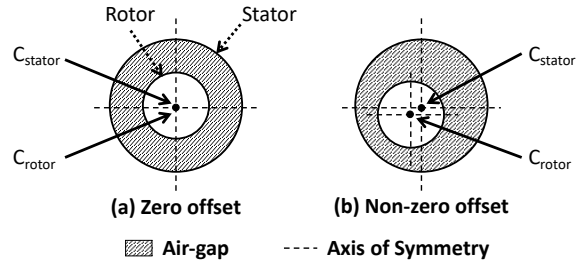


Figure 2: (a) Ideal scenario consisting of zero offset between rotor and stator centers. (b) The non-zero offset between stator and rotor centers is one the main causes for uniqueness in electromagnetic noise across different motors.

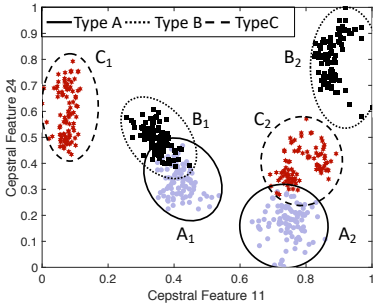


Figure 3: Plot depicts feasibility of sufficiently distinguishing individual motors within the same make and model using cepstral features. We observe two clusters, A_1 and A_2, representing the two motor instances within Type A.

Threat Model. Attacker's *goal* is to launch an impersonation attack to authenticate its drone, $\mathcal{A}_d$, as a legitimate drone, $\mathcal{L}_d$, where $\mathcal{L}_d \in \mathcal{L}$, denoting the set of all legitimate drones. We assume that the attacker is *capable* of compromising the digital certificate of $\mathcal{L}_d$. We also assume that $\mathcal{A}_d$ is of same make and model as $\mathcal{L}_d$.

3 BACKGROUND

In this section, we provide some relevant background for *SoundUAV*. We briefly describe the inner workings of brushless motors and the noise sources in them, along with providing preliminary evidence on the feasibility of fingerprinting motors.

3.1 Brushless Motors and the Noise Sources

Drones are commonly equipped with brushless motors due to their high efficiency [49]. These motors have multiple stationary windings (stator), and rotating permanent magnets (rotor). When the current flows through the stator, a rotating magnetic field is created, and the interaction of this magnetic field with the magnets, causes the rotor to rotate. Electronic Speed Controller (ESC) obtains constant feedback about the rotor's position and helps maintain steady rotation of the rotor.

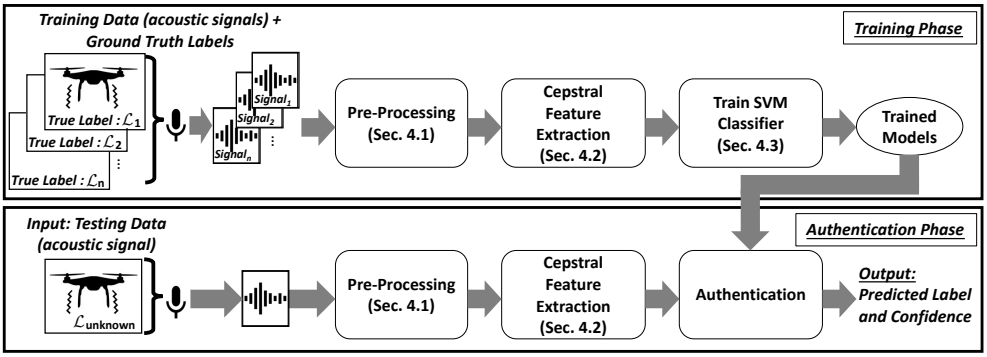


Figure 4: Flowchart depicts overall design of *SoundUAV*. In the Training Phase, *SoundUAV* obtains audio samples from n legitimate drones, extracts cepstral features, and input them along with corresponding true labels (i.e., $\mathcal{L}_1, \ldots, \mathcal{L}_n$) into SVM to obtain a set of trained models, $\mathcal{T}$. During the Authentication Phase, *SoundUAV* extracts features from a drone with unknown label, i.e., $\mathcal{L}_{unknown}$, and uses $\mathcal{T}$ to obtain its predicted label as well as confidence scores.

We leverage two sources of noise in motors for the task of fingerprinting — *electromagnetic* noise and *mechanical* noise. Electromagnetic noise is produced by changes in electromagnetic forces with the varying angular positions of the rotor, which causes vibrations to the motor's body [29]. Such forces occur due to the presence of non-uniform air-gap between stator and rotor, which is a result of non-zero offset between their centers as depicted in Figure 2. This offset occurs due to manufacturing defects such as incorrect placement of rotor during assembly [23, 39]. On the other hand, mechanical noise is caused due to rotor unbalance, misalignment, and looseness which produces additional vibrations [25, 34]. *SoundUAV* leverages the above two noise sources caused by manufacturing defects to accurately fingerprint drones.

3.2 Feasibility of Motor Fingerprinting

We present preliminary evidence on the feasibility of uniquely fingerprinting motors (thereby fingerprinting drones). Specifically, in Figure 3, we plot two cepstral features (Section 4.2) from sound recordings of two motors of three types (six in total) to demonstrate sufficient separation. We observe two distinct clusters within each motor type, indicating the feasibility of fingerprinting a motor even within the same type. We present detailed results on motor fingerprinting in Section 5.2.

4 SYSTEM DESIGN AND IMPLEMENTATION

In this section, we present the design and implementation of *SoundUAV* and illustrate the steps involved as a flowchart in Figure 4. In the training phase, *SoundUAV* pre-processes the audio samples obtained from n legitimate drones (Section 4.1), extracts cepstral features (Section 4.2), and trains an SVM classifier (Section 4.3) together with the true labels (i.e., drone labels: $\mathcal{L}_1, \ldots, \mathcal{L}_n$) to obtain a set of trained models, $\mathcal{T}$. During the authentication phase, i.e., the testing phase, *SoundUAV* takes as input the acoustic signal of an unknown drone to fingerprint (i.e., $\mathcal{L}_{unknown}$), repeats the above steps to extract the relevant features, and inputs them into $\mathcal{T}$, to obtain the predicted label and confidence scores.

4.1 Pre-processing

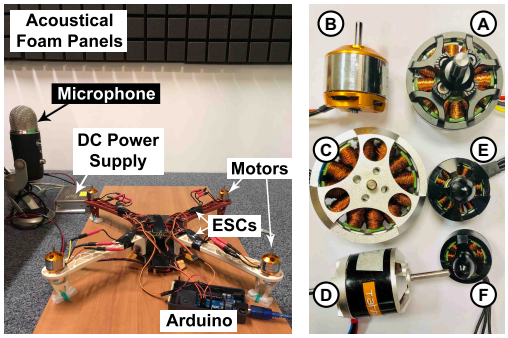
Pre-processing consists of *DC Offset Removal* and *Peak Normalization* steps. In *DC Offset Removal* module, we remove the non-zero mean by subtracting the mean of the signal from all samples, in order to prevent clipping of high amplitude regions in the audio and low-frequency distortions [7]. In *Peak Normalization* module, we set all maximum amplitudes to the same level for more accurate feature extraction as drone recordings may have differing amplitudes.

4.2 Cepstral Feature Extraction

We partition the pre-processed signal into frames of fixed length and repeat the following steps for each frame. First, we perform a Hamming window operation to smoothen the signal boundaries and compute the absolute value of the Discrete Fourier Transform, which gives the magnitude spectrum $\mathcal{M}$ of the windowed signal. We then apply t overlapping triangular bandpass filters (or filterbanks), $f_0, \ldots, f_{t-1}$, over $\mathcal{M}$ and obtain energies $E_0, \ldots, E_{t-1}$ correspondingly. Each energy term E_i, $0 \leq i < t$, is computed as the logarithm of the sum of amplitudes of $\mathcal{M}$ on applying filter f_i. Lastly, we decorrelate the energy terms by applying Discrete Cosine Transform over them to obtain cepstral coefficients/features [37]. The lower coefficients of the cepstral features contain information about the *spectral shape*, while the higher coefficients describe the *finer details in the spectrum.*

From our analysis of the magnitude spectrum of the drone's acoustic signal, we make two observations — (1) the energy variation patterns across the various frequency bands (i.e., spectral shape) are unique to each drone; and (2) there exists certain frequency bands in which a drone consistently has higher or lower energies compared to all other drones (i.e., combination of spectral shape and details). These two observations make cepstral features suitable for drone fingerprinting. For extracting cepstral features, we apply filterbanks over the entire frequency range from 0-22 kHz, with bandwidth of 500 Hz and overlap of 250 Hz. We consider the entire range as the harmonics due to the drone's rotation have considerable energies even at high frequencies.

The task of drone fingerprinting is analogous to that of human speaker identification, as in one case we identify the uniqueness



(a) (b)

Figure 5: Figures depict (a) experimental setup in sound booth with drone, microphone, Arduino and power supply; and (b) 6 different make and model motors from Types A-F.

in the structure of the motor, while in the other we identify the structure of the vocal tract. However, the Mel-frequency Cepstral Coefficients (MFCC) filterbanks [37], commonly used for speaker identification, are not suitable for our task as they focus on frequencies only upto 7 kHz.

4.3 Classifier

We implement Support Vector Machines (SVM) classifier with radial basis function as the kernel for drone fingerprinting. During training, we construct models, $\mathcal{T} = \{\mathcal{T}_1, \ldots, \mathcal{T}_n\}$, where n corresponds to the number of drone labels in the training data. Each model, $\mathcal{T}_i$, learns to differentiate drone label, $\mathcal{L}_i$, from all other labels. We empirically choose the SVM parameters — soft-margin parameter and kernel parameter by grid search on the cross-validation data, common to all models. During authentication, we output the predicted label as the index of the trained model that outputs the maximum confidence score and all the confidence scores.

5 EXPERIMENTAL EVALUATION

In this section, we describe the experimental setup and evaluate the performance of *SoundUAV* for drone fingerprinting.

5.1 Experimental Setup

We conduct our experiments in a sound booth as shown in Figure 5(a). We firmly affix the drone frame containing motors and Electronic Speed Controllers (ESCs) onto a wooden frame in order to keep the drone stationary during the experiments.

We use the DJI $f450$ frame [17] and four EMAX SimonK 12A ESCs [21]. Also, we have a total of 54 motors of six different makes and models (Types A-F) as illustrated in Figure 5(b). We provide the details in Table 1. We use an Arduino Uno [5] to provide input to the ESCs, which are powered by 12 V constant DC power supply.

We collect data from single motors as well as drones (i.e., an assembly of four motors), by operating them for 30-60 seconds at a constant speed of 6045 rotations per minute (RPM), which represents normal flight RPM. We conduct the experiment over three days in order to ensure that the results obtained are not influenced by any specific physical arrangement or ambient conditions. For the same reason, we choose data from different days for training and testing, except in Section 5.2.1 where we perform training and testing on different motors. We record using an omnidirectional Blue Yeti Pro microphone [50] with frequency response of 20 Hz - 20 kHz and sampling rate of 44.1 kHz. We partition each recording into frames containing 2^{14} samples each, corresponding to 0.37 seconds of audio. Detailed experimental results can be found in https://bit.ly/2VfkEgZ.

Motor type	Motor Make and Model	No. of motors
Type A	HengLi W42-20 [1]	2
Type B	XXD A2212/13T [2]	44
Type C	Singahobby 4008 [41]	2
Type D	Tahmazo ER221612d [42]	2
Type E	EMAX MT2204 [20]	2
Type F	Siglo 1804 [40]	2

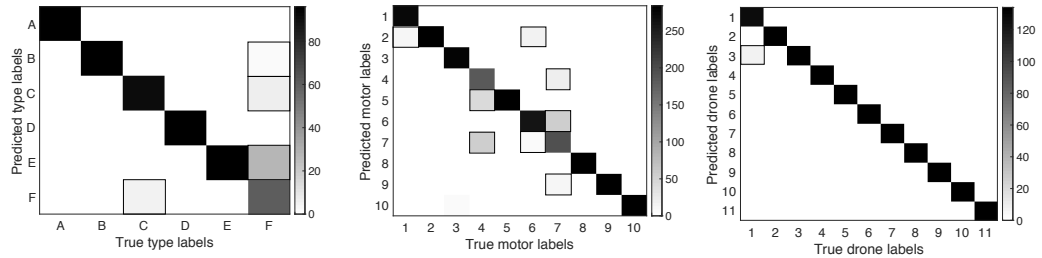
Table 1: Table presents distribution of motors across different motor types used in our experiments.

5.2 Motor Fingerprinting

As a precursor to drone fingerprinting, we present the results of motor fingerprinting, as motors are a major contributor for noise in drones (as discussed in Section 3.1). Specifically, we evaluate (1) motor type identification (i.e., make and model) and (2) motor fingerprinting within a motor type.

5.2.1 Motor Type Identification. In order to identify the type of motors, we collect 36 seconds of data from twelve motors, consisting two motors each of Types A-F. We partition these motors into two sets, each containing one motor per type, and alternatively use both sets for training and testing. On testing, we obtain a classification accuracy of 92.65% for type identification of motors. The corresponding confusion matrix is shown in Figure 6(a) and its table format can be found in the link provided in Section 5.1. Occasional misclassifications occur between Types E and F, which could be due to their similar physical structures as illustrated in Figure 5(b). From the results obtained, we infer that the distinct acoustic patterns produced by different motor types can be utilized to appropriately identify the make and model, i.e., type of a motor.

5.2.2 Motor fingerprinting within a single type. We further evaluate the possibility of *fingerprinting*, or distinguishing unique motor instances among same motor types. Hence, we randomly choose ten Type B motors (labeled $B_1, \ldots, B_{10}$) and collect 106 seconds of data per motor for two days. We alternatively train and test with data obtained from both days and obtain an average accuracy of 91.83%. The confusion matrix for the ten different motors is shown in Figure 6(b) with the corresponding table format available in the link provided in Section 5.1. To understand the few misclassifications (i.e., the non-diagonal elements), we conduct physical examination of motors and observe that B_4 and B_5 produce additional vibrations on rotation due to improper placement of the rotor in both motors. We believe that the other misclassifications can also be explained through correlation in physical structure. The takeaway point from this experiment is that the *subtle variations in physical structure of motors of the same type can produce distinct acoustic patterns.*



(a) Motor make and model (i.e., type) identification.

(b) Motor fingerprinting within same make and model.

(c) Drone fingerprinting within same make and model.

Figure 6: Figures depict confusion matrices representing performance of (a) motor type identification for six different types from Type A-F; (b) motor fingerprinting on ten motors $B_1, \ldots, B_{10}$ of same make and model; and (c) drone fingerprinting on eleven drones $\mathcal{L}_1, \ldots, \mathcal{L}_{11}$, each consisting of four motors of the same make and model.

5.3 Drone Fingerprinting

We further present the results on *fingerprinting* of drones, which constitutes an assembly of four motors. We evaluate how the interplay between motors, each with its own unique acoustic pattern, contributes towards the overall noise characteristics of the drone and to its fingerprinting. We evaluate on eleven drones, $\mathcal{L}_1, \ldots, \mathcal{L}_{11}$, where each drone is an assembly of four Type B motors, i.e., $\mathcal{L}_i = \{B_i, B_{i+11}, B_{i+22}, B_{i+33}\}$, $1 \leq i \leq 11$. We collect 50 seconds of data per drone for three days. We perform training on data collected over two days and utilize the rest for testing. We evaluate over all possible train-test combinations and obtain an average accuracy of 99.48%. The confusion matrix for the eleven drones is as shown in Figure 6(c), with the corresponding table format provided in the link specified in Section 5.1. The test data are predicted correctly for all cases except $\mathcal{L}_1$, which is misclassified as $\mathcal{L}_3$ for eight of the 134 test data points corresponding to $\mathcal{L}_1$.

An interesting observation from Figures 6(b) and 6(c) is that the accuracy for drone fingerprinting (99.48%) is *superior* to that of motor fingerprinting (91.83%). This improvement in performance is because each motor in a drone acts as an independent source of uniqueness, hence finding two drones with four pairs of motors with similar defects (or uniqueness) is less likely than finding just one pair of motors with similar defects, which makes *drones more viable to fingerprinting in comparison to individual motors.*

6 DEPLOYMENT CONSIDERATIONS

We now discuss practical considerations of deploying *SoundUAV*.

Unseen Drone Classification. In a real world scenario, we may encounter drones that are not part of the training process. Hence, we need an *open-world classifier* that can tell apart a drone encountered during training from a *unseen* one. To create such a classifier, we modify our existing system to output "*unseen*" when the confidence scores of all training models fall below a certain threshold. We conduct a preliminary evaluation of this modified system by choosing different number of *unseen* drones, n_{unseen}, where $n_{unseen} \in \{1, 2, 4\}$ and obscuring them from the training process. On testing with all the 11 drones for different values of n_{unseen}, we obtain an average accuracy of 90.8% (threshold = 0.3). While a more comprehensive evaluation is needed, this result hints at the feasibility of *SoundUAV* accurately classifying *unseen* drones.

Effects of adding propellers. In our experiments, we consider drones without propellers and exploit the uniqueness in brushless motors for drone fingerprinting. While both motors and propellers contribute to the drone's noise, as a first step towards fingerprinting, we examine the effects of motors in this work. Moreover, there are evidences for manufacturing defects in propellers [38, 47], and we plan to investigate the role of these defects towards uniqueness of drone's sound as part of future work.

Effects of increasing the number of drones. We report a prediction accuracy above 99% on fingerprinting *eleven* drones, but this number may drop as we increase the number of drones. While we will evaluate this aspect in our future work, current results may still be relevant for authentication in cases involving small number of legitimate drones such as small-scale parcel delivery services. Furthermore, we hint at the possibility of fusing across other sensing modalities such as RF to improve fingerprinting accuracy [33].

Controlled Experimental Setup. Recall from Section 5.1 that we perform our experiments in a sound booth by placing a microphone (around $130) in proximity to the drone. This setup resembles the docking station as depicted in Figure 1, where the drone is placed adjacent to the built-in microphone. Furthermore, our preliminary results on inexpensive microphones, such as those in laptops (around $15) is encouraging, hence making it possible to reduce the deployment costs of such a station.

7 RELATED WORK

We now present related work on device and drone fingerprinting.

Device Fingerprinting. Researchers demonstrate the feasibility of fingerprinting various devices including loudspeakers, cameras, 3D printers and smartphones, by leveraging their manufacturing defects [11, 15, 26, 31, 36]. In particular, work by Das et al. [13], which demonstrates that speakers and microphones can be fingerprinted to uniquely identify mobile phones, is closely related to our work. However, *SoundUAV* addresses more difficult challenges due to the interplay between multiple noise sources (i.e., four motors).

Drone Identification and Fingerprinting. Several drone detection systems exist utilizing RF, audio, and video signals [14, 18, 35]. For example, Matthan detects drones by observing their physical characteristics from the transmitted wireless signal [33].

However, these works differ from *SoundUAV* as we focus on fingerprinting of drones rather than detection. Gyrosfinger [44], the first work to investigate the problem of drone fingerprinting to the best of our knowledge, utilizes gyroscope offset values to differentiate drones. Their technique, however, is constrained to work only on drones that have an unencrypted telemetry channel. Contrarily, *SoundUAV* is independent of the underlying protocols and works on any drone as it leverages the noise characteristics of drones.

8 CONCLUSION

We propose *SoundUAV* as a second factor of authentication for drones, specifically for the application of drone delivery. *SoundUAV* authenticates drones by fingerprinting them based on the differences in their acoustic noise characteristics produced by the manufacturing defects in their brushless motors. As we leverage the hardware imperfections of motors, it is hard for an adversarial drone to replicate the acoustic signals. Moreover, *SoundUAV* is robust to large-scale attacks and requires no modifications to existing drones. We evaluate *SoundUAV* for the tasks of motor and drone (i.e., four motor assembly) fingerprinting, and conclude that drones are more viable to fingerprinting, as they have four independent sources of uniqueness, making it less likely for two drones to be similar. Further, we evaluate on 54 motors, and eleven drones of the same make and model, and obtain a fingerprinting accuracy of 99.48% for drones, demonstrating the feasibility of our approach.

9 ACKNOWLEDGEMENTS

This research was partially supported by a grant from Singapore Ministry of Education Academic Research Fund Tier 1 (R-252-000-A26-133).

REFERENCES

[1] AliExpress. 2019. HengLi BLDC. https://bit.ly/2FFAdI7.
[2] AliExpress. 2019. XXD BLDC. https://bit.ly/2Uh8vLb.
[3] Amazon. 2016. Amazon Prime Air. https://amzn.to/2oFPnmj.
[4] Ayoub Aouad. 2018. Delivery companies are embracing drone technology. https://www.businessinsider.com/delivery-companies-embracing-drone-technology-2018-6/?IR=T.
[5] Arduino. 2019. Arduino Uno. https://store.arduino.cc/usa/arduino-uno-rev3.
[6] Ionut Arghire. 2018. 23,000 Digital Certificates Revoked in DigiCert-Trustico Spat. https://www.securityweek.com/23000-digital-certificates-revoked-digicert-trustico-spat.
[7] Audacity. 2019. DC offset. https://manual.audacityteam.org/man/dc_offset.html.
[8] Tony Bradley. 2012. VeriSign Hacked: What We Don't Know Might Hurt Us. https://www.pcworld.com/article/249242/verisign_hacked_what_we_dont_know_might_hurt_us.html.
[9] Jeff Chandler. 2016. AirMap, DigiCert Introduce First-Ever Digital Identity Certificate for Drones. https://www.digicert.com/news/2016-12-13-digicert-partners-with-airmap-for-drone-id/
[10] NBC Chicago. 2009. UPS Impersonator Robs Homeowner. https://www.nbcchicago.com/news/local/Fake-UPS-Deliverymen-Rob-Skokie-Man-52474932.html.
[11] William Banks Clarkson. 2012. *Breaking assumptions: distinguishing between seemingly identical items using cheap sensors.* Ph.D. Dissertation. Princeton University.
[12] Lucian Constantin. 2016. Cyberespionage groups are stealing digital certificates to sign malware. https://www.computerworld.com/article/3044728/cyberespionage-groups-are-stealing-digital-certificates-to-sign-malware.html.
[13] Anupam Das, Nikita Borisov, and Matthew Caesar. 2014. Do you hear what I hear?: Fingerprinting smart devices through embedded acoustic components. In *ACM Conference on Computer and Communications Security (CCS)*.
[14] Dedrone. 2019. Dedrone Homepage. https://www.dedrone.com.
[15] Sanorita Dey, Nirupam Roy, Wenyuan Xu, Romit Roy Choudhury, and Srihari Nelakuditi. 2014. AccelPrint: Imperfections of Accelerometers Make Smartphones Trackable. In *Network and Distributed System Security Symposium (NDSS)*.
[16] DHL. 2018. Parcelcopter 3.0. https://discover.dhl.com/business/business-ethics/parcelcopter-drone-technology.
[17] RC Drones. 2019. DJI f450 frame. http://www.rc-drones.com/-DJI-F450-Multirotor-Quad-Flame-Wheel-450-Frame_p_282.html.
[18] DroneShield. 2019. DroneShield Homepage. https://www.droneshield.com.
[19] John Dyer. 2015. China Accused of Doling Out Counterfeit Digital Certificates in Serious Web Security Breach. https://bit.ly/2D53FH8.
[20] EMAX. 2019. EMAX BLDC. https://www.emaxmodel.com/emax-multicopter-motor-mt2204-kv2300.html.
[21] EMAX. 2019. EMAX SimonK ESC. https://www.emaxmodel.com/emax-simon-series-12a-for-multirotor.html.
[22] Social Engineer. 2019. Delivery Person. https://www.social-engineer.org/framework/general-discussion/common-attacks/delivery-person/.
[23] Alfonso Fernandez. 2017. Eccentricity. https://power-mi.com/content/eccentricity.
[24] Dennis Fisher. 2012. DigiNotar Hack Shows Total Compromise of CA Servers. https://threatpost.com/final-report-diginotar-hack-shows-total-compromise-ca-servers-103112/77170/.
[25] Jacek F Gieras, Chong Wang, and Joseph Cho Lai. 2018. *Noise of polyphase electric motors.* CRC press.
[26] Miroslav Goljan, Jessica Fridrich, and Tomáš Filler. 2009. Large scale test of sensor fingerprint camera identification. In *Media forensics and security*, Vol. 7254. International Society for Optics and Photonics, 72540I.
[27] Leo Kelion. 2015. Alibaba begins drone delivery trials in China. https://www.bbc.com/news/technology-31129804.
[28] Haye Kesteloo. 2018. New proposed French drone regulation requires remote drone identification. https://dronedj.com/2018/04/11/french-drone-regulation/.
[29] Hong Joo Lee, Shi Uk Chung, and Sang Moon Hwang. 2008. Noise source identification of a BLDC motor. *Journal of Mechanical Science and Technology* (2008).
[30] Alan Levin. 2018. Drones May Need License Plates Soon. https://bloom.bg/2klauuv.
[31] Zhengxiong Li, Aditya Singh Rathore, Chen Song, Sheng Wei, Yanzhi Wang, and Wenyao Xu. 2018. PrinTracker: Fingerprinting 3D Printers using Commodity Scanners. In *ACM Conference on Computer and Communications Security (CCS)*.
[32] Mayra Moreno. 2016. Man posed as UPS driver to rob Galleria-area home. https://abc13.com/news/homeowner-brutally-beaten-by-fake-ups-delivery-driver/1636109/.
[33] Phuc Nguyen, Hoang Truong, Mahesh Ravindranathan, Anh Nguyen, Richard Han, and Tam Vu. 2017. Matthan: Drone presence detection by identifying physical signatures in the drone's RF communication. In *ACM MobiSys*.
[34] Michael Peter Norton and Denis G Karczub. 2003. *Fundamentals of noise and vibration analysis for engineers.* Cambridge university press.
[35] Orelia. 2019. Drone-Detector. http://droneboucher.com/en/orelia-drone-detector.
[36] Senthilkumar Chinnappa Gounder Periaswamy, Dale R Thompson, and Jia Di. 2011. Fingerprinting RFID tags. *IEEE Transactions on Dependable and Secure Computing* (2011).
[37] Lawrence R Rabiner and Ronald W Schafer. 2011. *Theory and applications of digital speech processing.* Vol. 64. Pearson Upper Saddle River, NJ.
[38] Tony Rogers. 2015. Injection Molding Defects. https://www.creativemechanisms.com/blog/what-cause-injection-molding-defects-and-how-to-fix-them.
[39] MA Samonig and Th M Wolbank. 2017. Exploiting rotor slotting harmonics to determine and separate static and dynamic air-gap eccentricity in induction machines. In *2017 IEEE SDEMPED*.
[40] Singahobby. 2019. Siglo BLDC. http://shop.singahobby.com/?q=node/36309.
[41] Singahobby. 2019. Singahobby 4008 BLDC. http://shop.singahobby.com/?q=node/32508.
[42] Singahobby. 2019. Tazmazo ER-221612d. https://www.singahobby.com/index.php/tahmazo-er-221612d-brushless-motor.html.
[43] Skycart. 2016. Swiss Post Parcel Delivery With Drones from Skycart. https://www.youtube.com/watch?v=gLx34DrQFO4.
[44] Yunmok Son, Juhwan Noh, Jaeyeong Choi, and Yongdae Kim. 2018. GyrosFinger: Fingerprinting Drones for Location Tracking Based on the Outputs of MEMS Gyroscopes. *ACM Transactions on Privacy and Security (TOPS)* (2018).
[45] Kelly Tay. 2015. SingPost completes successful test flight of drone for mail delivery. https://www.businesstimes.com.sg/companies-markets/singpost-completes-successful-test-flight-of-drone-for-mail-delivery.
[46] UPS. 2017. UPS Tests Residential Delivery Via Drone. https://www.youtube.com/watch?v=xx9_6OyjJrQ.
[47] Loraine Vinot. 2015. Drone Propeller Manufacturing. https://www.youtube.com/watch?v=D40CCaiLwPQ.
[48] PR News Wire. 2018. Global Forecast 2027. https://prn.to/2UKbigt.
[49] Padmaraja Yadamale. 2003. Brushless DC Motor Fundamentals. http://ww1.microchip.com/downloads/en/AppNotes/00885a.pdf.
[50] Yeti. 2019. Blue Yeti Pro. https://www.bluedesigns.com/products/yeti-pro/.
[51] Kim Zetter. 2013. Gaming company certificates stolen and used to attack activists, others. https://www.wired.com/2013/04/gaming-company-certs-stolen/.