International Journal of Communication Networks and Information Security
ISSN: 2073-607X, 2076-0930
Volume 15 Issue 02 Year 2023

Assessing the Feasibility of RF Fingerprinting for Security in Unmanned Aerial Vehicles

Ernest Kwadwo Adomako*
Assistant Scholar, Department of Mechanical Engineering, Kwame Nkrumah University of Science and Technology-Kumasi, Ghana-West Africa
ekadomako@gmail.com
Abdul-Rahman Ahmed
Associate Professor, Kwame Nkrumah University of Science and Technology-Kumasi, Ghana
aarahman.soe@knust.edu.gh
Sani Mubarak Ellis
Doctor, Department of Telecommunication Engineering, Kwame Nkrumah University of Science and Technology-Kumasi, Ghana
smellis.coe@knust.edu.gh
Justice Owusu Agyemang
Doctor, Department of Telecommunication Engineering, Kwame Nkrumah University of Science and Technology-Kumasi, Ghana
justice.agyemang@knust.edu.gh
Griffith Selorm Klogo
Doctor, Department of Computer Engineering, Kwame Nkrumah University of Science and Technology-Kumasi, Ghana
gsklogo.coe@knust.edu.gh

Article History

Received: 14 September 2023
Revised: 28 October 2023
Accepted: 11 November 2023

Abstract

The wireless network of consumer drones is particularly vulnerable to remote attacks due to the weak encryption scheme involving the exchange of a Global Unique Identifier (GUID) between transceiver pairs using the binding process, thus exposing the technology to a host of attack vectors such as *data spoofing and malicious authentication,* among others, leading to security breaches that threaten the prospects of the consumer drone. This study assesses the feasibility of RF fingerprinting as a complementary layer of security devoid of cryptography in the wireless network of unmanned aerial vehicles for enhanced resilience. We evaluate the feature performance of the toy-grade and the universal-grade drone RC transmitters to discern the prospects for device identification in inexpensive, low-end device and the high-end device. Instantaneous amplitude and phase features extracted from the transient phase of time-domain signals acquired off-the-air in the near-field show a high recognition rate in a support vector machine and k-Nearest Neighbour, suggestive of device classification in unmanned aerial vehicle RF hardware, irrespective of built quality.

Keywords: RF Fingerprinting, Physical-Layer, UAV, RC Transmitter.

1. Introduction

The popularity of consumer drones in diverse fields of human endeavour in recent times has attracted a host of malicious activities targeting the radio frequency (RF) control and data link employed in remote operations for flight control and real-time data/payload streaming.

Given the limited processing resources resulting from the drone's power constraints, which restrict the choices of computing devices and, consequently, the level of encryption that could be implemented without slowing down system operation, this raises real concerns about security threats to the weak encryption scheme involving the exchange of Global Unique Identifiers (GUIDs) between transceiver pairs.

Vulnerability to remote attacks is aggravated by the susceptibility of *MAC and upper-layer* security features to malicious modification through software that could be exploited by an attacker to perform a man-in-the-middle attack and consequently take over the drone from the legitimate user [1]. These security limitations thus expose the drone to a host of attack vectors, such as data spoofing and malicious authentication, among others, with the potential to result in remote vehicle hijack and data or payload interception by an attacker whose motive could be an act of terror, mischief, or burglary [2], [3]; that implies the intent to commit a heinous crime, crash the drone or vector away to a hide-out, along with any sensitive payload.

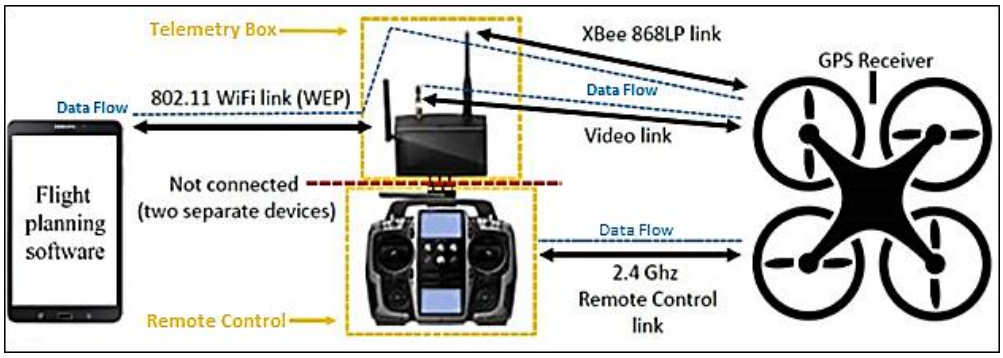


Figure 1. Wireless Network Setup of a Typical Consumer Drone

Figure 1 shows the wireless connectivity of a typical consumer drone secured by a cryptographic-based encryption scheme between transceiver pairs. Of prime concern to vehicle security are (i) the Radio Control (RC) Transmitter, which is the primary control channel that facilitates basic vehicle setup as well as manual flight control typically within 100 meters of Visual Line of Sight (VLOS), and (ii) the telemetry channel, which enables advanced flight modes, including autonomous operation through flight planning software installed on a PC, tablet, or phone connected via the Mavlink or Wi-Fi link, aiding safe flight beyond visual line of sight. The vulnerability of these vehicle controls and data links to malicious activities thus presents uncertainty about the prospects of drone technology. The physical (PHY) layer, however, presents good prospects for a non-cryptographic authentication scheme that imposes a minimum burden on processing resources and is difficult to mimic remotely [4].

In this study, we assess the feasibility of RF fingerprinting in a transmitter-receiver pair [5] as an additional layer, non-cryptographic, physical-layer authentication solution in the wireless network of UAVs for enhanced robustness in the face of ever-increasing security threats. The scheme of work is for a specific receiver to authenticate a given legitimate transmitter using the fingerprints formed by the receiver based on its front-end impairments. The resilience of the scheme draws on the non-portability of RF fingerprints across different receivers [6] due to differences in receiver front-end impairments. As was demonstrated in [6], the RF fingerprint created in one receiver cannot serve as a universal sample for the given transmitter, thus making it difficult to mislead the authenticating receiver with fingerprints of the legitimate transmitter acquired with a rogue receiver.

RF fingerprinting in the context of transient signals is a technique for identifying a transmission device by the rise-time signature that characterizes its signal at power-on. This unique turn-on transient signal behaviour is mainly due to random differences in the intrinsic characteristics of device hardware, particularly in the RF circuitry, resulting in transmitter-specific characteristics that can be exploited to form a non-cryptographic, physical-layer authentication

solution. The technique has been successfully deployed in identified wireless networks, for example, in cellular networks, to prevent cell phone cloning and related fraud [7].

This research delves into the RF fingerprinting technique for distinct device classification in unmanned aerial vehicle (UAV) RF hardware, irrespective of built quality while considering the device's computing constraints. The remaining sections of the paper are structured as follows: Section 2 reviews related work, Section 3 describes our proposed methodology, Section 4 discusses the results, and Section 5 presents the conclusion.

2. Related Works

Recent work demonstrates the effectiveness of the technique in drone detection and profiling. The approach is used in [8] to discriminate between multiple UAV transmissions and co-existing RF signals on the same frequency band in the environment, using features extracted from the energy transient derived from the time-domain transient of the acquired signal. Similarly, in [9] and [10], the scheme's potential as an early warning system for curbing security threats posed by rogue drones is investigated. The scheme is to profile legitimate drones by their RF fingerprints in a database; any out-of-library signature detected from a drone approaching the restricted area is then classified as an intruder, consequently triggering prompt countermeasures. The authors in [11] also demonstrated, with a remarkable success rate, a multi-classifier approach to improving the detection accuracy of identical drones transmitting non-standard signals.

Recent trends seek to improve feature extraction techniques without manual intervention and reduce computational time due to feature dimension and algorithm complexity [12]. To detect and identify UAVs based on their radio fingerprints, a novel approach is presented in [13]. Unlike previous studies, this approach utilizes an end-to-end deep-learning-based model and a multiscale feature extraction method to achieve good generalization of the signal capability for quick decision-making, thus reducing computational time. It is also proposed under the scheme AirID [14] for the intentional insertion of a custom RF fingerprint in a UAV transmission at the physical layer to forestall the effects of environmental and channel-induced instability on inherent radio signatures as a means to improve drone detection and identification.

2.1 Traditional Approach to RF Fingerprinting

Figure 2 presents a simplified overview of the varied approaches to RF fingerprinting. In principle, subtle features that uniquely characterize the transmission device are extracted either from the region of interest (ROI) of the transmitted signal or the channel response with respect to its environment and subsequently profiled and classified to identify a given transmitter.

The concept may be viewed from the perspective of channel fingerprinting, in which channel state information such as scatter, multi-path fading, power decay over distance, and received signal strength indicator (RSSI) that describes the response of the channel and its environment is extracted to uniquely characterize the channel for the identification of a given transmitter and its location [15], [16], or device fingerprinting utilizing features extracted from either transmitter turn-on transient *(transient-state)* [7] or frequency and constellation symbol imperfections from the steady-state portion of the transmitted signal [17] as shown in Figure 2.

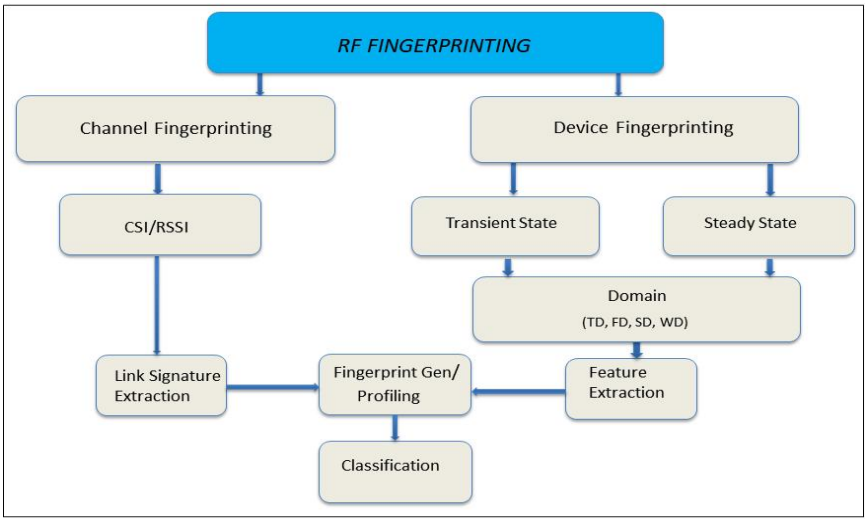


Figure 2. Simplified Overview of RF Fingerprinting

The concept of device authentication using RF fingerprints is to capture and process wireless transmission of the legitimate device for the distinctive features that characterize its signals and use this to generate fingerprints that uniquely identify the transmission device. The fingerprints are profiled and stored for comparison with a feature set from any device seeking authentication; a profile match then results in "Access Granted" and a mismatch, "Access Denied", as shown in Figure 3.

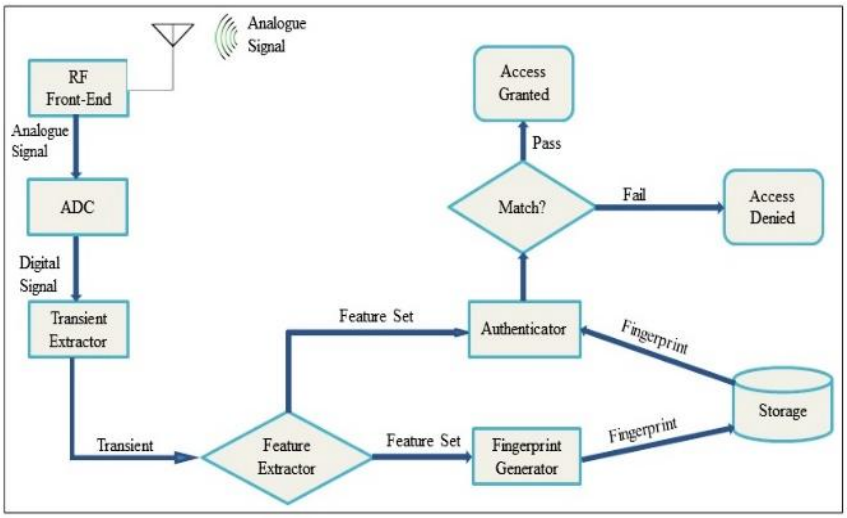


Figure 3. RF Fingerprint Authentication Scheme

The technique has evolved to the most recent deep learning DL-based algorithms [18] that are computationally demanding but flexible enough for adaptation to varied scenarios. Such new schemes in physical-layer authentication from an information theoretic approach may help establish unique parameters for secure wireless transmission [19] and further reinforce the potential of the technique to enhance wireless network security. Innovative application domains of the future, such as healthcare, the Internet of Things (IoT), vehicle-to-everything (V2X) and autonomous UAV, Smart Grid 2.0, and extended reality (XR) envisioned for 6G networks, will require lightweight, fast, and resilient device authentication schemes to guarantee user security and privacy [18] in such a dense and ever-challenging network environment, RF fingerprinting thus offers a viable option for such stringent security requirements.

Transient-state fingerprinting was thought to have the demerit of a higher sampling rate $\geq 4\ GS/s$ [20] for signal acquisition, thus requiring a high-end, very expensive setup to accomplish, a disincentive that had the technique relegated to the background, while *steady-state* enjoyed greater attention for research over time. Contrary to this, it has been demonstrated in recent works, for example, in [21], that lower sampling rates equally yield transients of high signal integrity and classification accuracy, leading to a refocus of research into transient-state fingerprinting. Research has accelerated in this direction in recent times with novel approaches to domain fusion [22] techniques for noise-resilient fingerprints that yield higher classification accuracy compared to the existing single-domain fingerprints.

3. Methodology

The work was conducted experimentally in hardware and set to exploit instantaneous amplitude and phase features extracted from the transient portion of time domain signals acquired off-the-air in the near field. For higher accuracy and reliability and to factor in the possible effects of component instability on transients as they undergo repeated on-off cycles, a high acquisition of one thousand (1000) waveforms from each drone RC transmitter under test was chosen. Four transmitters, top-grade labelled Tx1, top-ranking labelled Tx2, both 27 MHz FM toy-grade devices, and Futaba Skysport 6A labelled Tx3, Futaba Skysport T4YF labelled Tx4, both 72 MHz FM universal-grade devices, were selected based on availability and similarity in the signal waveform of the device pair.

Typically, transmitters of the same brand and type exhibit different transient characteristics [7]. However, similarity in signal characteristics has the tendency to increase the classification error rate, hence the need to factor this into transmitter selection. The acquired signals are then processed in MATLAB to generate profile fingerprints for classification in SVM and k-NN models. The choice of the two models was influenced by the need for high classification accuracy using a low-complexity algorithm [23], given the toy-grade device's lack of resources to process complex algorithms under the practical implementation of the scheme.

3.1 Experimental Setup

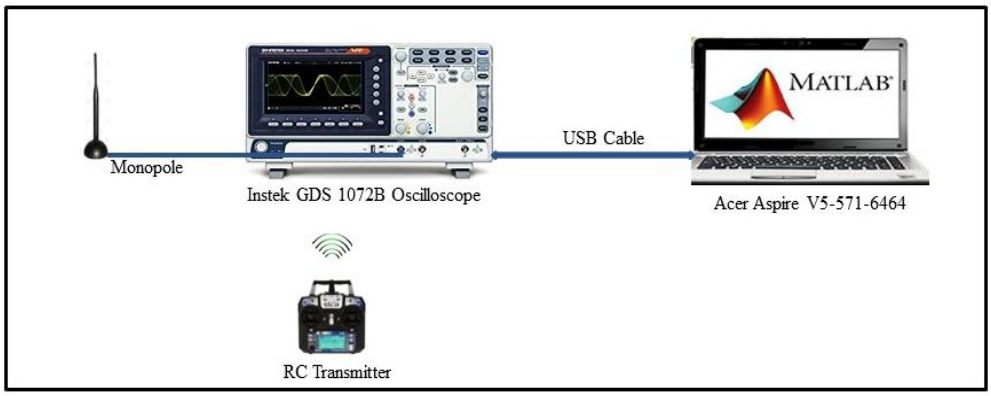


Figure 4. Setup for Signal Acquisition

The setup for capturing wireless signals from the RC transmitters under investigation is shown in Figure 4. At the core is a 70 MHz, 1 GSa/s Instek GDS 1072B digital storage oscilloscope fitted with a monopole antenna for off-the-air signal acquisition in the near field. With the transmit antenna placed 4 cm from the receiving monopole and the instrument set to single trigger acquisition mode, RF transients are then acquired at a sampling rate of 1 GSa/s and stored on a flash drive in *.CSV format for processing in MATLAB.

It was demonstrated in [21] that sampling rates much lower than the 4 GSa/s preference in the literature equally yield transients of high signal integrity and classification accuracy. The entire signal acquisition work was carried out in an office environment, shown in Figure 5, at the same time of day when EMI from adjourning sources is deemed low. Sample waveforms of the acquired signal are presented in Figure 6, 7, 8, and 9 for the respective transmitters. A detailed procedure for the transient signal acquisition is provided in the appendix.

Figure 5. Experimental Setup in an Office Environment

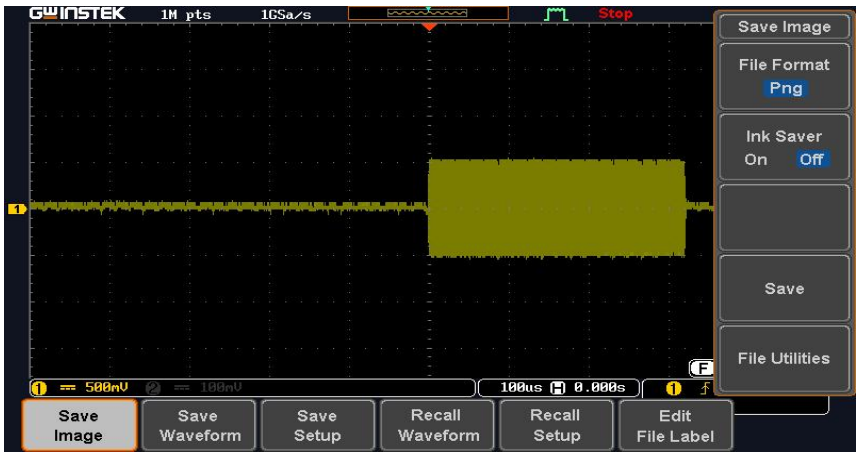


Figure 6. Transient Waveform of Tx1

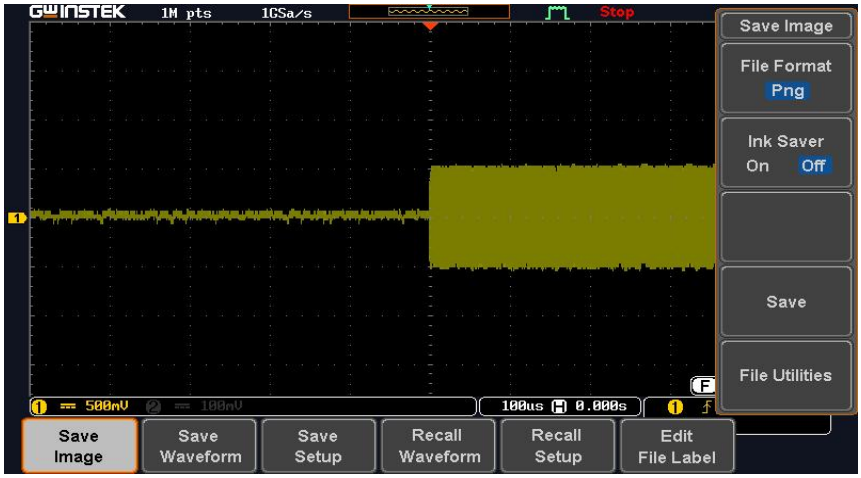


Figure 7. Transient Waveform of Tx2

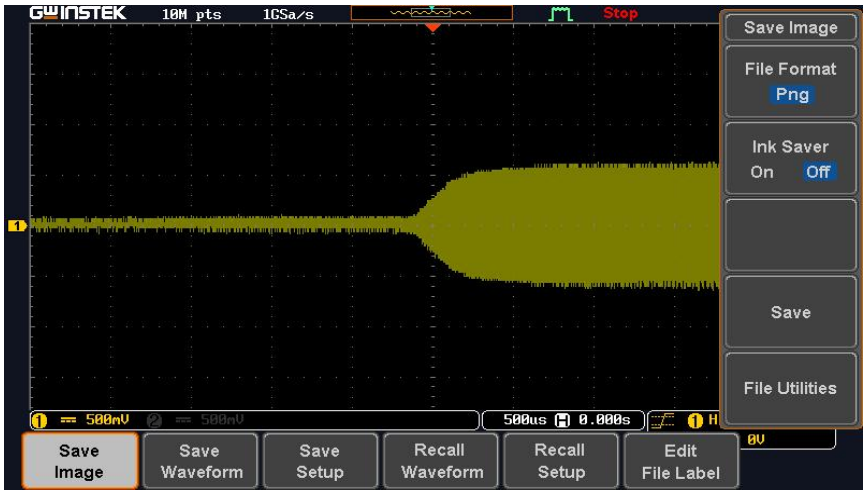


Figure 8. Transient Waveform of Tx3

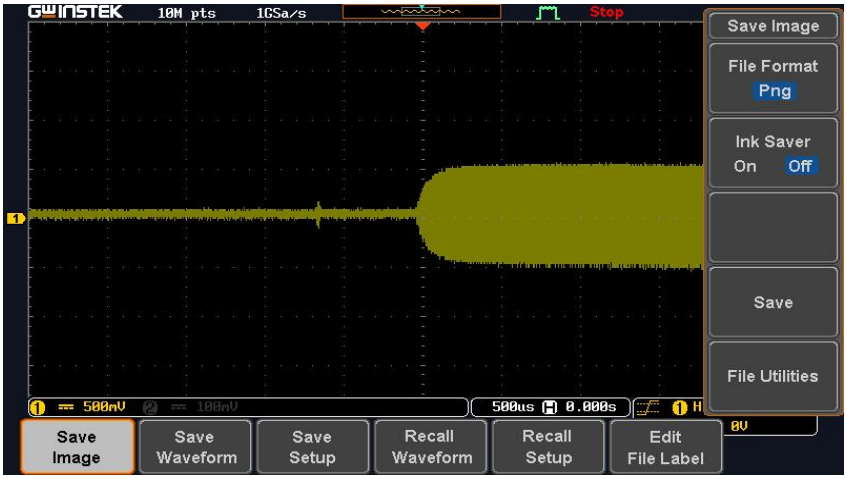


Figure 9. Transient Waveform of Tx4

Figure 6 and 7 show sample waveforms for Tx1 and Tx2 toy-grade RC transmitters, while Figures 8 and 9 show those for universal-grade devices Tx3 and Tx4.

3.2 Sigal Processing

3.2.1. Transient Detection

An amplitude-based variance detection approach using the threshold technique [24] is adopted for the detection of the transient start and end points on the premise that (i) the amplitude characteristics of channel noise and that of the transient differ and (ii) the start of the transient is abrupt, although some signals may exhibit a gradual transition between channel noise and the start of the transient [25].

A similar approach in [24] is applied to detect the transient phase of the signal by first defining a new discrete variance signal V_i as:

$$V_i = K\frac{1}{w-1}\sum_{n=1}^{w}(S_{i-n} - \overline{X}_w)^2 \qquad (1)$$

Where:

V_i is a new variance signal created from the input signal S (Acquired Signal), w is the sliding window size, $\overline{X}_w$ is the mean of sample values S_{i-w}, S_{i-1},

K is the scaling factor for making V_i comparable to S.

The variance signal V_i can be considered an indicator of the degree to which the incoming signal S deviates from the average of the previous w sample; thus, at the onset of the transient, S increases rapidly, leading to a higher deviation, hence detecting the transient. Once the signal is detected and its variance computed, the start and end of the transient become a change point problem, which is then solved using the cumulative sum (CUSUM) algorithm [24]. Thus, for transients, the variance of the signal for a given window size w would increase rapidly as compared to the variance of the previously measured w sample. For the start of the transient, the change point is where V_i begins to increase rapidly, and the end of the transient is the point at which V_i flattens out [24]. Signal regions of the input waveforms obtained using the algorithm in Equation 1 are shown in Figures 10, 11, 12, and 13.

Signal regions of Tx1 and Tx3 are shown in Figure 10 and 11, respectively. Similar results are obtained for Tx2 and Tx4.

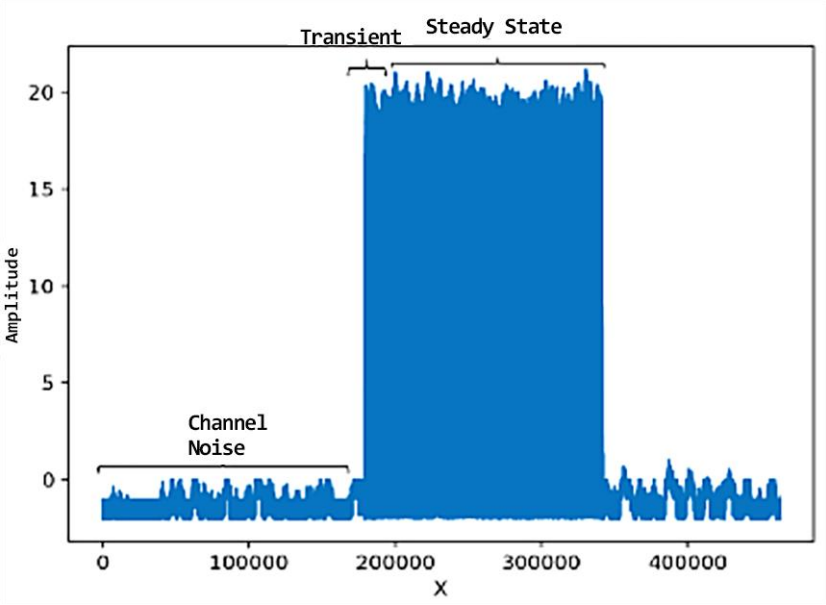


Figure 10. Signal Regions of Tx1

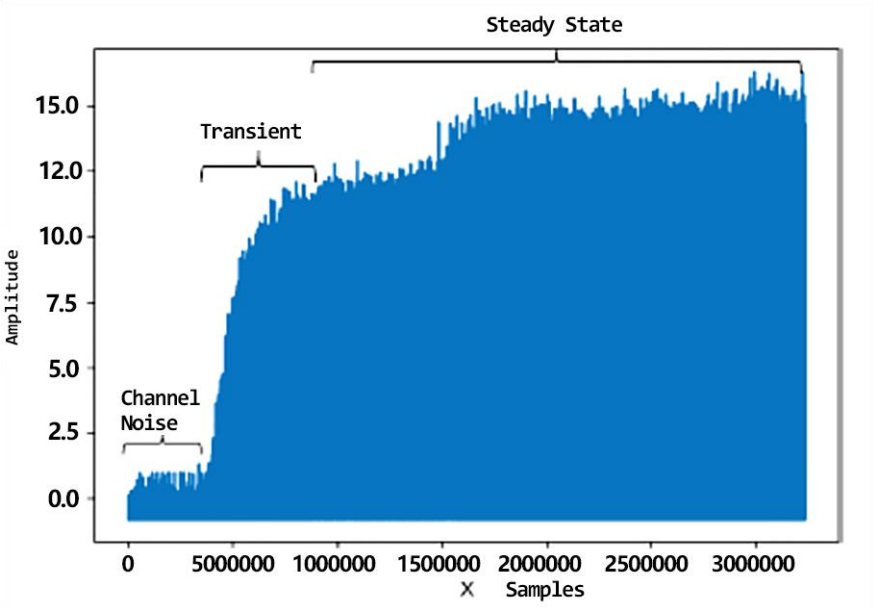


Figure 11. Signal Regions of Tx3

The extracted transient phases of Tx1 and Tx3 are shown in Figure 12 and 13, respectively. Similar results are obtained for Tx2 and Tx4.

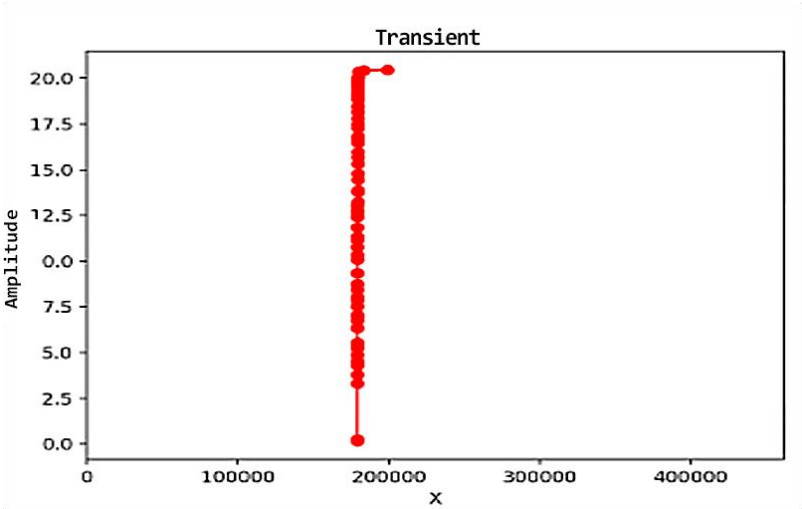


Figure 12. Detected Transient Phase for Tx1

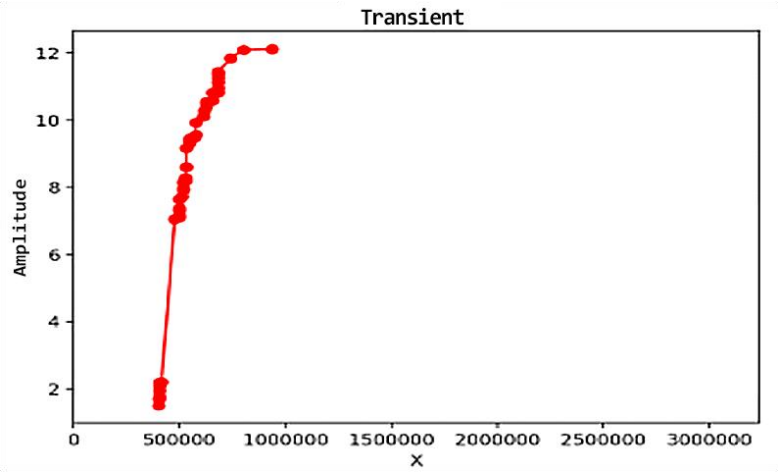


Figure 13. Detected Transient Phase for Tx3

3.2.2. Feature Extraction

Once the transient is detected, discrete wavelet transform (dwt) [26] is applied to extract the energy envelope, which is then converted to an in-phase and quadrature I/Q sample, given as:

$$S_C(n) = H\big(a(n)\big) = S_I(n) + S_Q(n) \qquad (2)$$

Instantaneous Amplitude (a) and Phase ∅ features are extracted from the complex I/Q characteristics [20] of the signal as follows:

$$a[n] = \sqrt{I[n]^2 + Q[n]^2} \qquad (3)$$

$$\phi[n] = \tan^{-1}\left[\frac{Q[n]}{I[n]}\right] \text{ for } I[n] \neq 0 \qquad (4)$$

Where:

a is the instantaneous amplitude of the acquired signal; ϕ, the instantaneous phase; I being the in-phase amplitude of the input signal; and Q is the quadrature amplitude.

3.2.3. Fingerprint Generation

Statistical fingerprints are then generated as variance σ^2, skewness γ, and kurtosis k as follows:

$$\sigma^2 = \frac{1}{N_x}\sum_{n=1}^{N_x}(x(n) - \mu)^2 \qquad (5)$$

$$\gamma = \frac{1}{N_x\sigma^3}\sum_{n=1}^{N_x}(x(n) - \mu)^3 \qquad (6)$$

$$k = \frac{1}{N_x\sigma^4}\sum_{n=1}^{N_x}(x(n) - \mu)^4 \qquad (7)$$

Where N is the sample size, μ is the sample mean, and X_n is the n^{th} element in the sample

3.2.4. Machine Learning & Fingerprint Classification

A total of four thousand (4000) samples, 1000 from each transceiver under test, are used in a 4:1 ratio between the test and training samples for the inter-device classification test in a Support Vector Machine SVM in comparison with the performance of K-Nearest Neighbour k-NN. The SVM and k-NN classifiers were modelled based on the three test scenarios, and the data was structured accordingly, with the class or label appended. From a data set of 4000 per scenario, the model is instructed to use 20% of the data for training and 80% for testing. This choice was informed by [21], in which it was demonstrated that an increase in training sample size beyond 20% for sizable datasets yields negligible improvement in classification performance.

4. Results and Discussion

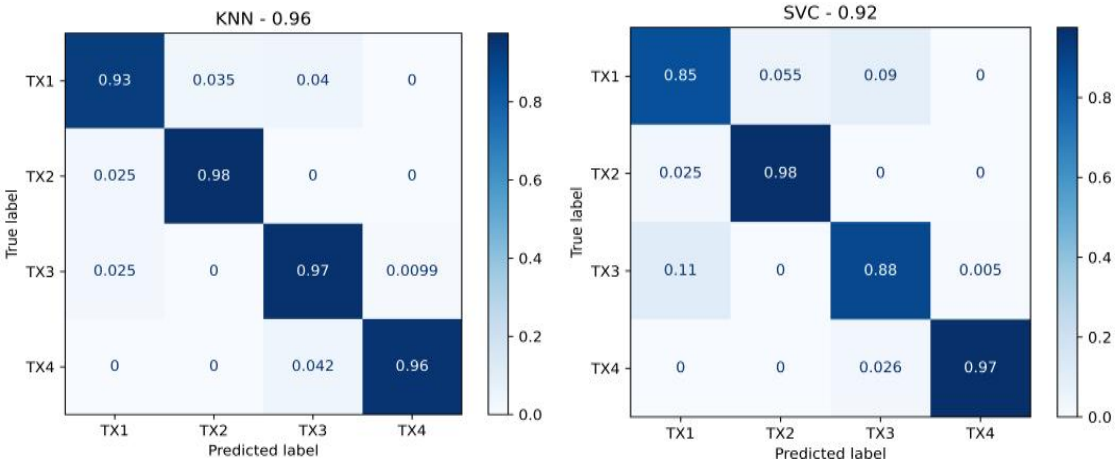
The result is presented for three scenarios:

1. Instantaneous Phase-Only feature
2. Instantaneous Amplitude-Only feature, and
3. Combine (full dimensional) feature set, followed by a comparison of the three scenarios in terms of accuracy.

4.1 Classification Results

Inter-device classification results for the three scenarios in both k-NN and SVM are presented in Figures 14, 15, and 16.

4.1.1. Scenario 1: Amplitude-Only Feature Set

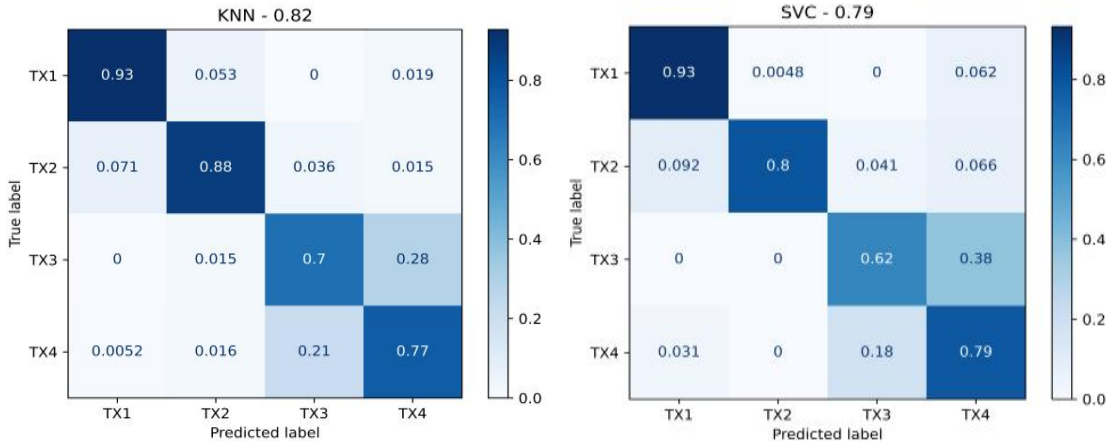


(a) *(b)*

Figure 14. Confusion Matrix for Amplitude-Only Feature Classification Test in Both Models

The results of Figure 14 show high classification accuracy achieved in both the toy-grade device Tx1, Tx2 and the universal-grade device Tx3, Tx4. All four devices are thus distinguished by an overall accuracy rate of 96% for the k-NN and 92% for the SVM. The stated accuracy is computed on the test sample by the embedded performance metrics of the model.

4.1.2. Scenario 2: Phase-Only Feature Set



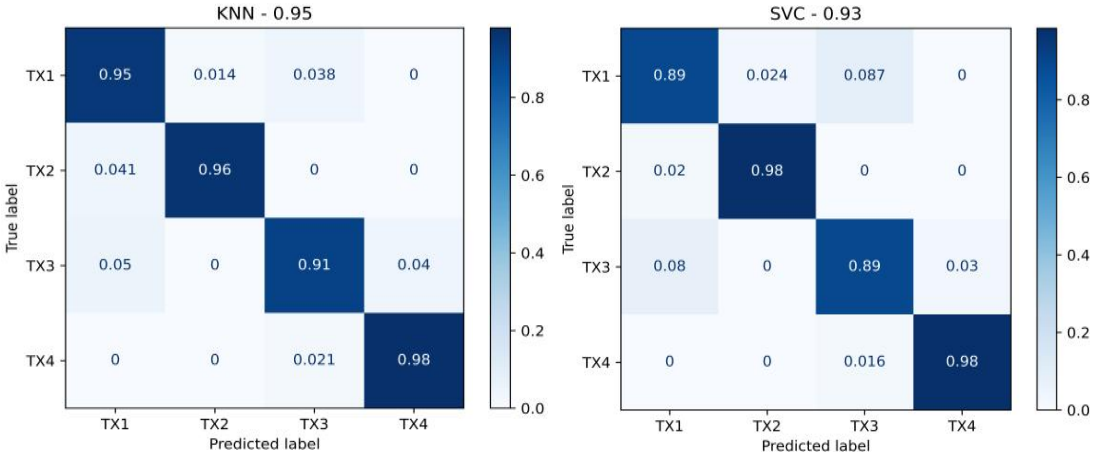
(a) *(b)*

Figure 15. Confusion Matrix for Phase-Only Feature Classification in Both Models

Although the phase feature underperformed the amplitude feature set, it shows a good accuracy rate in the individual transmitters except for Tx3, which was mostly misclassified as Tx4 in both models.

The overall accuracy rate is in the order of 82% for k-NN and 79% for the SVM, as recorded in Figure 15.

4.1.3. Scenario 3: Combine (full dimensional) Feature Set

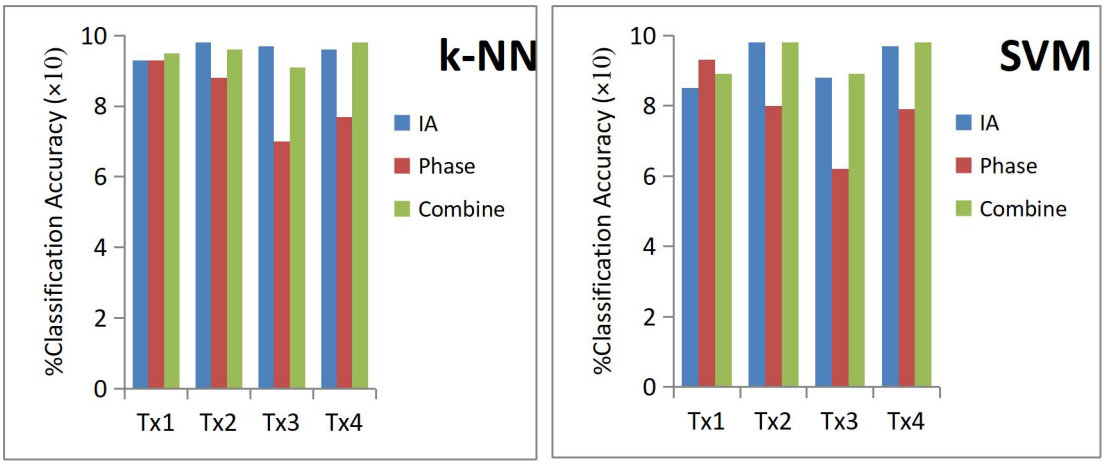


(a) *(b)*

Figure 16. Confusion Matrix for the Combine (full dimensional) Feature Set in Both Models

As shown in Figure 16, the combined feature set also recorded a high accuracy rate comparable to the amplitude feature in both classifiers, with an overall performance accuracy of 95% for the k-NN and 93% for the SVM.

4.2 Discussion



(a) *(b)*

Figure 17. Classification Performance Chart in Both Models: (a) k-NN and (b) SVM

The performance of the three distinct feature sets is seen in Figure 17. Amplitude and the combined feature set for all four transmitters show high recognition rates in both classifiers. Comparatively, it is observed that the combined (full dimensional) feature set does not necessarily result in any significant improvement or otherwise in classification performance over the amplitude feature; it does, however, outperform the phase feature. Though the phase feature, except that of Tx1, underperformed the amplitude and the combined feature in both classifiers, understandably due to its smaller dynamic range as reported in [7], it does, however, offer a good recognition rate in the order of 82% in the k-NN and 79% for the SVM, making the phase feature reasonably useful in the fingerprinting process.

5. Conclusion

This work has used toy-grade and universal-grade drone RC transmitters to evaluate RF fingerprints at sub-GHz to discern the prospects for device identification. The uniqueness of signal features of interest has been explored with a high success rate for the validation of an alternate approach to device authentication devoid of cryptography using simple algorithms that do not impose a high burden on processing resources and thus present a viable option for strengthening the security of UAV wireless networks against malicious activities. Hardware quality invariably influences the attributes of a transmitter, for example, the requisite properties of the fingerprints, uniqueness, and robustness. However, it was found in this study that the toy-grade RC transmitter built with inexpensive hardware equally exhibits unique signal features with a high recognition rate comparable to the high-end universal grade. The results thus demonstrate that RF fingerprinting is feasible in drone RF hardware, irrespective of built quality.

6. Acknowledgement

Appreciation for the TME Education Africa-sponsored electronics laboratory at the faculty of Electrical and Computer Engineering-K.N.U.S.T. for the invaluable technical support.

References

[1] NM. Rodday, R.O. De Schmidt and A. Pras, "Exploring security vulnerabilities of unmanned aerial vehicles," In *NOMS 2016-2016 IEEE/IFIP Network Operations and Management Symposium* (pp. 993-994). IEEE, 2016, April.

[2] K. Moskvitch, "Are drones the next target for hackers - BBC Future.", 2014. https://www.bbc.com/future/article/20140206-can-drones-be-hacked Accessed, April, 2019.

[3] D. Maloney, "Hacker Says He Can Hijack a $35K Police Drone a Mile Away WIRED." 2016. https://www.wired.com/2016/03/hacker-says-can-hijack-35k-police-drone-mile-away/ Accessed, April, 2019.

[4] C. Zhao, M. Huang, L. Huang, X. Du and M. Guizani, "A robust authentication scheme based on physical-layer phase noise fingerprint for emerging wireless networks," *Computer Networks*, vol. 128, pp. 164-171, 2017.

[5] SU. Rehman, K.W. Sowerby, S. Alam and I. Ardekani, "Radio frequency fingerprinting and its challenges," *In 2014 IEEE conference on communications and network security* (pp. 496-497). IEEE, 2014, October.

[6] SU. Rehman, K.W. Sowerby, S. Alam and I. Ardekani, "Portability of an RF fingerprint of a wireless transmitter," *In 2014 IEEE Conference on Communications and Network Security* (pp. 151-156). IEEE, pp. 151-156, 2014, October.

[7] O. Ureten and N. Serinken, "Wireless security through RF fingerprinting," *Canadian Journal of Electrical and Computer Engineering*, vol. 32, no. 1, pp. 27-33, 2007.

[8] M. Ezuma, F. Erden, C.K. Anjinappa, O. Ozdemir and I. Guvenc, "Micro-UAV Detection and Classification from RF Fingerprints Using Machine Learning Techniques," *In 2019 IEEE Aerospace Conference* (pp. 1-13). IEEE, 2019, March.

[9] H. Li, G. Johnson, M. Jennings and Y. Dong, "Drone profiling through wireless fingerprinting," *In 2017 IEEE 7th Annual International Conference on CYBER Technology in Automation, Control, and Intelligent Systems (CYBER)* (pp. 858-863). IEEE, 2018, July.

[10] O.O. Medaiyese, M. Ezuma, A.P. Lauf and I. Guvenc, "Wavelet transform analytics for RF-based UAV detection and identification system using machine learning," *Pervasive and Mobile Computing*, vol. 82, p. 101569, 2022.

[11] N. Soltani, G. Reus-muns, B. Salehi, J. Dy, S. Ioannidis and K. Chowdhury, "RF Fingerprinting Unmanned Aerial Vehicles with Non-standard Transmitter Waveforms," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 12, pp. 15518-15531, 2020.

[12] G. Baldini, I. Amerini and F. Bonavitacola, "Convolutional neural networks combined with feature selection for radio-frequency fingerprinting," *Computational Intelligence*, vol. 39, no. 5, pp. 734-758, 2023.

[13] S.S. Alam, A. Chakma, M.H. Rahman, R. Bin Mofidul, M.M. Alam IBKY Utama, and Y.M. Jang, "RF-Enabled Deep-Learning-Assisted Drone Detection and Identification: An End-to-End Approach," *Sensors*, vol. 23, no. 9, p. 4202, 2023.

[14] S. Mohanti, N. Soltani, K. Sankhe, D. Jaisinghani, M. Di Felice and K. Chowdhury, "AirID: Injecting a Custom RF Fingerprint for Enhanced UAV Identification using Deep Learning," *In GLOBECOM 2020-2020 IEEE Global Communications Conference* (pp. 1-6). IEEE, 2020, December.

[15] L. Xiao, L. Greenstein, N. Mandayam and W. Trappe, "Fingerprints in the Ether: Using the Physical Layer for Wireless Authentication," *In 2007 IEEE International conference on communications* (pp. 4646-4651). IEEE, 2007, June.

[16] N. Patwari and S. K. Kasera, "Robust Location Distinction using Temporal Link Signatures," *In Proceedings of the 13th annual ACM international conference on Mobile computing and networking* (pp. 111-122), 2007, September.

[17] V. Brik, S. Banerjee, R. South, N. Brunswick, M. Gruteser and S. Oh, "Wireless Device Identification with Radiometric Signatures," *In Proceedings of the 14th ACM international conference on Mobile computing and networking* (pp. 116-127), 2008, September.

[18] A. Jagannath, J. Jagannath and PSPV Kumar, "A Comprehensive Survey on Radio Frequency (RF) Fingerprinting: Traditional Approaches, Deep Learning, and Open Challenges," *Computer Networks*, vol. 219, pp. 1-30, 2022.

[19] M.E. Sone, "Physical Layer Security for Wireless Networks Based on Coset Convolutional Coding," *International Journal of Communication Networks and Information Security*, vol. 12, no. 1, pp. 95-100, 2020.

[20] B.W. Ramsey, T.D. Stubbs, B.E. Mullins, M.A. Temple and M.A. Buckner, "Wireless infrastructure protection using low-cost radio frequency fingerprinting receivers," *International Journal of Critical Infrastructure Protection*, vol. 8, pp. 27-39, 2015.

[21] S. Taşcıoğlu, M. Köse and Z. Telatar, "Effect of sampling rate on transient based RF fingerprinting," *In 2017 10th International Conference on Electrical and Electronics Engineering (ELECO)* (pp. 1156-1160). IEEE, 2018, November.

[22] Y. Jin, M. Wei, and Q. Li, "An RF Fingerprint Extraction Method based on Time-frequency Domain Feature Fusion," vol. 2424, no. 1, p. 012030, 2023.

[23] Y. Li, L. Chen, J. Chen, F. Xie, S. Chen and H. Wen, "A low complexity feature extraction for the rf fingerprinting process," *In 2018 IEEE Conference on Communications and Network Security (CNS)*, pp. 1-2, IEEE, 2018, May.

[24] K.B. Rasmussen and S. Capkun, "Implications of radio fingerprinting on the security of sensor networks," In *2007 Third International Conference on Security and Privacy in Communications Networks and the Workshops-SecureComm 2007*, pp. 331-340, IEEE, 2007, September.

[25] J. Hall, M. Barbeau and E. Kranakis, "Detection of transient in radio frequency fingerprinting using signal phase," *Wireless and Optical Communications*, vol. 9, p. 13, 2003.

[26] C. Zhao, X. Wu, L. Huang, Y. Yao and Y. C. Chang, "Compressed sensing-based fingerprint identification for wireless transmitters," *The Scientific World Journal*, vol. 2014, 2014.