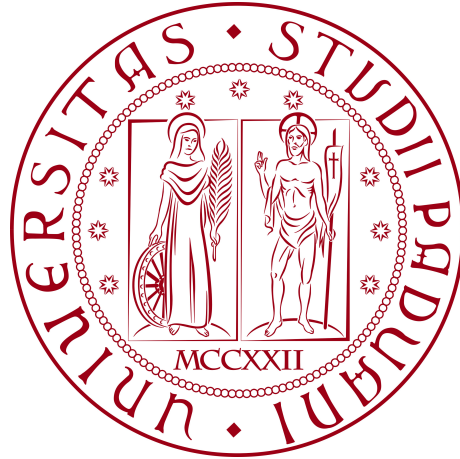


Università degli Studi di Padova

DIPARTIMENTO DI MATEMATICA “TULLIO LEVI-CIVITA”

CORSO DI LAUREA IN INFORMATICA



**Drone Wireless Charging Profiling and
Fingerprinting**

Tesi di Laurea Triennale

Relatore

Professor

Alessandro Brighente

Laureanda

Eleonora Amadori

Matricola 2089254

ANNO ACCADEMICO 2023-2024

Acknowledgements

I would like to thank professor Alessandro Brighente, for this opportunity, the support, the freedom of choice and leeway he gave me throughout these last months. But mostly for making me believe even more in what I am doing with his passion for the topics I had the privilege to discuss and learn from and with him.

I would like to thank my family and my dearest friends, the ones that are here and the ones I can only remember, that supported me during the journey that led me here.

Padova, Luglio 2024

Eleonora Amadori

Summary

This thesis describes the work done during my internship period, carried out within the University of Padua in the SPRITZ Research Group, an acronym that stands for Security and Privacy Research Group, of the Department of Mathematics, under the guidance of professor Alessandro Brighente. The work was divided into three parts: the study of the literature on UAV security with Threat Models and Scenarios, Wireless Charging Protocols (Qi) and their areas of use, taking over a Codebase of a temporarily stopped project, and finally the implementation of codes dedicated to introduce a model with the intention of fingerprinting, profiling, to be used with ad hoc Machine Learning algorithms: this study assesses the feasibility of profiling and fingerprinting drone firmware and executed operations by analyzing the current flow in various charging states. The findings reveal a distinct correlation between different software on board the drone and current behavior, which can be easily distinguished using various machine learning algorithms, the results demonstrate the possibility to accurately identify both the firmware and communication protocol of a drone. This research, and the ones prior, serve as a foundation for exploring the security and privacy of wireless power transfer in drone technology, with implications for both novel attack vectors and defense strategies.



Figure 1: Group Logo

Contents

1	Introduction	1
1.1	Importance	2
1.2	Drones Description	3
1.3	Charging Protocols	3
1.4	Document structure	4
2	Security	7
2.1	Drones Security	7
2.2	The actual drone in use	9
2.3	Applied Security over WPT	9
2.4	Setup and Code Interactions	12
2.5	Python	14
2.6	The experiment	16
2.6.1	Tools:	16
2.6.2	Procedure	18
2.6.3	Use the Bitcraze software and change the firmware	19
2.6.4	Custom firmware upload	19
2.7	Drone Profiling	20
2.7.1	The fingerprinting requires the manual procedure to up- load the custom firmware for the:	20
2.7.2	Results	20
3	Internship description	22
3.1	Introduction to the literature	22
3.1.1	Introductory model	22

CONTENTS

3.1.2	The idea	23
3.2	Understanding Ohm's law with real world applications	24
3.2.1	Formula	24
3.2.2	Explanation	24
3.3	Model	26
3.4	Coding and Debugging	27
3.4.1	Libraries:	27
3.5	Our work	28
3.5.1	Coding	28
3.6	Graphical Results	29
4	Reflections	32
4.1	Conclusions on the Project	32
4.2	Future work	32
4.3	Threats and Mitigation	33
5	Conclusions	37
5.1	Final Accounts	37
5.2	Achievements	37
5.3	Acquired knowledge	39
5.4	Personal evaluation	40
	Bibliography	i
	Webliography	iv

List of Figures

1	Group Logo	v
1.1	Unmanned Aerial Vehicle: an aircraft without any human pilot ¹	2
1.2	Qi system ²	4
2.1	Drone schemes based on flying typology ³	11
2.2	Example of the biggest military UAV: RQ-4B ⁴	11
2.3	Scheme of the circuit setup	16
2.4	Setup	17
2.5	Wireless power transfer using Qi	17
3.1	Wireless power transfer curves using Qi	25
3.2	Data Table from the queues of various firmwares	29
3.3	Plot of the queues of various firmwares	30
4.1	Military Drones ⁵	35

¹*UAV*. URL: <https://www.animalia-life.club/qa/pictures/the-drones-are-located-where.html>.

²*P-cons*. URL: <https://www.wirelesspowerconsortium.com/qi/>.

³*Drones*. URL: <https://marieladesnhkline.blogspot.com/2022/04/the-different-types-of-drones-explained.html>.

⁴*RQ-4B*. URL: <https://loredaily.com/this-is-americas-biggest-uav-meet-the-rq-4-global-hawk/>.

⁵*Military Drones*. URL: <https://www.evergladesuniversity.edu/blog/guide-different-types-drones-unmanned-aerial-systems/>.

List of sourcecodes

2.1	Ciao mondo!	15
2.2	Usage of minicom	18
2.3	Create a Virtual Enviroment	19
2.4	Start the software	19
2.5	Upload the custom firmware	19
3.1	Reading Data, creating a DataFrame	28
3.2	Extraction of Current and Time Series	28
3.3	Unpacking the list of lists, using x as an index of the list of firmware names	28
3.4	Application of Moving Average Filter to smoothen the function curve	29
3.5	Function to find the queue, where the feature are found	30
5.1	Main	39

Chapter 1

Introduction

The use of Unmanned Aerial Vehicles or "drones" has significantly increased across various sectors, including agriculture, logistics, surveillance, and aerial photography. These devices require advanced technologies for communication and charging, which are essential for their effective and continuous operation. An *Unmanned Aerial Vehicle*_G (UAV) is defined as a "powered, aerial vehicle that does not carry a human operator, uses aerodynamic forces to provide vehicle lift, can fly autonomously or be piloted remotely, can be expendable or recoverable, and can carry a lethal or nonlethal payload".¹

Drones have taken the world by storm, revolutionizing various industries and capturing the imagination of enthusiasts. With over 1.7 million drone registrations in the US alone, it's clear that drones have become a popular choice for both recreational and commercial purposes. The global drone market is projected to reach over \$42 billion by 2025, reflecting the significant growth and opportunities in the industry. China dominates the drone production market, accounting for 79.8% of global production. Consumer drones hold the majority market share, but the agriculture sector is expected to be the driving force behind future drone usage. The drone services market is valued at \$4.4 billion, and delivery businesses are increasingly looking to incorporate drone delivery methods. Law enforcement agencies and the construction industry have also

¹UAV. URL: <http://www.thefreedictionary.com/Unmanned+Aerial+Vehicle>.

witnessed substantial growth in drone usage.²

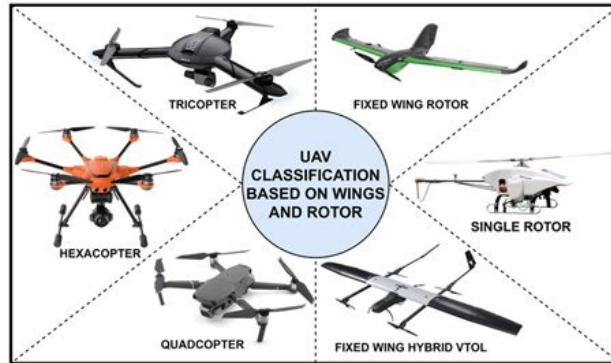


Figure 1.1: Unmanned Aerial Vehicle: an aircraft without any human pilot³

1.1 Importance

In recent years, flying drones have become increasingly functional and popular for various tasks such as surveillance and goods delivery. Concurrently, researchers have developed advanced charging technologies for unmanned and autonomous drones to meet the rising electricity demands. Among these, wireless power transfer is gaining attention for its usability and potential integration into autonomous flights. However, this technology introduces new challenges and security risks. The privacy and security implications of public or unsecured charging pads for flying drones, or unauthenticated drone-to-drone charging, require further investigation and mitigation. In this study, we introduce a novel side channel that leverages the current flow in the wireless charging circuit to deduce the drone’s operational capabilities and internal state. We assess the ability to profile and fingerprint drone firmware and operations by analyzing the current flow during various charging states. The findings reveal a distinct differentiation between different onboard software and current behaviors, which can be easily identified using various machine learning algorithms. The results demonstrate how to accurately identify both the firmware and the communication protocol of a drone.

²Statistics. URL: <https://www.dronebrands.org/drone-statistics/>.

1.2 Drones Description

Drones use various communication protocols for remote control and data transmission. The most common include: Wi-Fi for short-range operations, allowing real-time video and data transmission, and Bluetooth, suitable for short-distance communications and often used for initial setups or local controls. RF (Radio Frequency) ensures stable communication even at longer distances, while LTE/5G allows for drone control over very long distances, even in dense urban environments where Wi-Fi signals might be insufficient⁴. But there are many challenges to be tackled, communication being the chief one. Encryption and optimization techniques for ensuring longlasting and secure communications, as well as for power management. Moreover, applications of UAV networks for different contextual uses ranging from navigation to surveillance, *Ultra-reliable and lowlatency communications*_G⁵, edge computing and work related to artificial intelligence are examined. In particular, the intricate interplay between UAV, advanced cellular communication, and internet of things constitutes one of the focal points of the literature.⁶.

1.3 Charging Protocols

Charging protocols for drones, for an efficient battery recharging, can be either wired or wireless. Wired charging includes USB-C and Micro-USB ports, common in consumer drones for direct recharging, and proprietary connectors used by some professional drones for faster and safer charging. Wireless charging involves methods like magnetic induction, which uses electromagnetic fields

⁴Haris Gacanin and Amir Ligata. «Wi-Fi Self-Organizing Networks: Challenges and Use Cases». In: *IEEE Communications Magazine* 55.7 (2017), pp. 158–164. DOI: [10.1109/MCOM.2017.1600523](https://doi.org/10.1109/MCOM.2017.1600523).

⁵Jihong Park et al. «Extreme ultra-reliable and low-latency communication». In: *Nature Electronics* 5 (Mar. 2022), pp. 1–9. DOI: [10.1038/s41928-022-00728-8](https://doi.org/10.1038/s41928-022-00728-8).

⁶Abhishek Sharma et al. «Communication and networking technologies for UAVs: A survey». In: *Journal of Network and Computer Applications* 168 (2020), p. 102739. ISSN: 1084-8045. DOI: <https://doi.org/10.1016/j.jnca.2020.102739>. URL: <https://www.sciencedirect.com/science/article/pii/S1084804520302137>.

to transfer energy without wires. This is convenient for drones landing on dedicated charging platforms, with the Qi protocol being widely used. Qi systems operate through electromagnetic induction between planar coils, consisting of a Base Station connected to a power source that provides inductive power and Mobile Devices that consume this power. The Base Station contains a power transmitter with a transmitting coil that generates an oscillating magnetic field, inducing an alternating current in the receiving coil of the Mobile Device by Faraday's law of induction⁷. Magnetic resonance, still in development for commercial applications⁸, offers a greater charging distance compared to magnetic induction, showcasing the evolving landscape of drone charging technologies, and the risks they could imply like our work showcases.

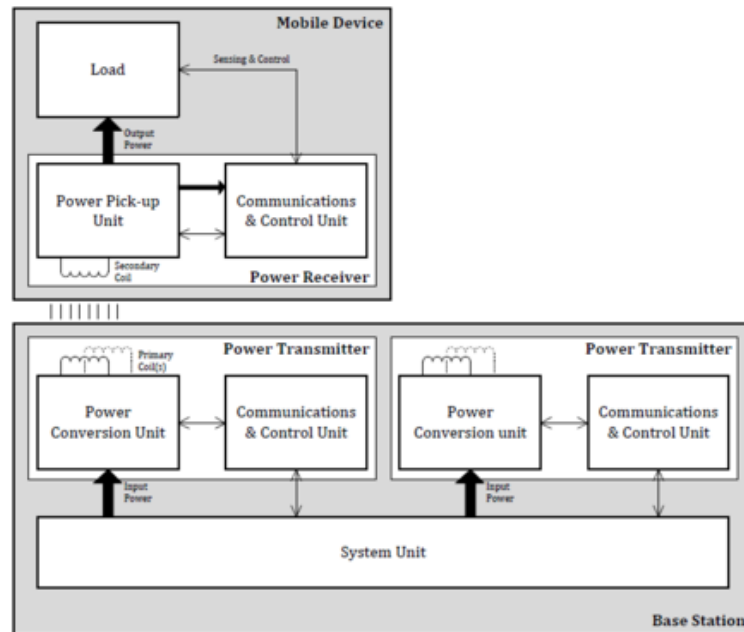


Figure 1.2: Qi system⁹

1.4 Document structure

The second chapter describes the security issues of UAV and introduces the idea of my internship;

⁷*P-cons.* URL: <https://www.wirelesspowerconsortium.com/qi/>.

⁸T. Campi et al. «High efficiency and lightweight wireless charging system for drone batteries». In: *2017 AEIT International Annual Conference*. 2017, pp. 1–6. DOI: [10.23919/AEIT.2017.8240539](https://doi.org/10.23919/AEIT.2017.8240539).

The third chapter delves into the work I did with my supervisor Alessandro Brighente and a PhD student, Tommaso Bianchi, explores also how I interacted with the design of the codebase;

The fourth chapter deepens the acknowledgments on the topic;

The fifth chapter tries to give to the reader a more systemic and relational point of view on the matter of my study;

Regarding the drafting of the text, the following typographical conventions have been adopted in this document:

- Acronyms, abbreviations, and ambiguous or uncommon terms mentioned are defined in the glossary, located at the end of this document;
- For the first occurrence of terms listed in the glossary, the following nomenclature is used: *Unmanned Aerial Vehicle*_G;

Chapter 2

Security

2.1 Drones Security

Drones Security Risks: In this chapter we introduce the potential risks that drones are exposed to as well as the ones they propose: drone technology has revolutionized various industries, from agriculture to surveillance, and has become an essential tool for many organizations. However, with the increasing adoption of drones, concerns about their security have also grown. In this discourse, we will explore the risks associated with drone technology and discuss the mitigations that can be implemented to ensure their secure use. One of the primary risks associated with drone technology is data interception. Unencrypted or weakly encrypted communication channels between drones and their controllers can be vulnerable to eavesdropping attacks, compromising the confidentiality and integrity of transmitted data. This highlights the importance of implementing secure communication protocols, such as SSL/TLS or IPsec, and using encryption algorithms like AES. Another significant risk is unauthorized access to drones. Weak authentication mechanisms, unpatched vulnerabilities, or default credentials can make drones vulnerable to remote control hijacking or takeover. This emphasizes the need for implementing robust authentication and

authorization protocols, and ensuring regular software updates and patching¹². Drone technology also poses physical threats, as they can carry payloads, such as cameras, sensors, or even small explosives. This highlights the importance of implementing physical security measures, such as secure storage and transportation, and conducting regular security audits and risk assessments. Drone technology is also susceptible to malware infections, compromising their functionality and data integrity. This emphasizes the need for implementing robust antivirus software, keeping software up-to-date, and conducting regular security scans and penetration testing³. Drone technology raises concerns about privacy invasions and surveillance. Drones equipped with cameras and sensors can capture sensitive information, potentially violating human rights or compromising privacy. This emphasizes the need for implementing privacy-preserving technologies, such as anonymization and data minimization, and ensuring compliance with relevant data protection regulations, such as GDPR⁴. In conclusion, drone technology poses significant risks, including data interception, unauthorized access, physical threats, cybersecurity concerns, and privacy invasions. However, by implementing robust security measures, such as secure communication protocols, robust authentication and authorization, physical security measures (like the one we explored in this work), robust antivirus software, and privacy-preserving technologies, organizations can mitigate these risks and ensure the secure use of drone technology⁵.

¹Electronic Frontier Foundation. *Drone Privacy: A Guide to Protecting Your Privacy*. 2020.

²Federal Aviation Administration. *Drone Security: A Guide to Protecting Your Drone*. 2020.

³Open Web Application Security Project. *Drone Security Testing: A Guide to Identifying Vulnerabilities*. 2020.

⁴European Union. *European Union General Data Protection Regulation*. 2016.

⁵Jin Han et al. «RANGO: A Novel Deep Learning Approach to Detect Drones Disguising from Video Surveillance Systems». In: *ACM Trans. Intell. Syst. Technol.* 15.2 (Feb. 2024). ISSN: 2157-6904. DOI: [10.1145/3641282](https://doi.org/10.1145/3641282). URL: <https://doi.org/10.1145/3641282>.

2.2 The actual drone in use

In this scenario, the drone is a multicopter integrating different sensors, like a gyroscope, accelerometer, barometer, and magnetometer, all included in a *Inertial Measurement Unit (IMU)_G* central chip managing the drone's flight. This allows the vehicle to hover in a steady position in the air without further actions by a human driver. The drone can equip a camera and other sensors, like *Light Detection and Ranging (LIDAR)_G* and sonar, to detect and map the surrounding environment. Base stations on the ground can collect the data sent by drones to manage a swarm and assist them during flight operations. Therefore, vehicles need antennas and radio equipment to communicate with such base stations or directly with other drones. Some examples are wireless communication over Wi-Fi or Bluetooth in the 2.4GHz band. Virtually all multicopters on the market are fully electric. A power management chip and a battery regulate the power needed by each unit present on the drone. In this context, wireless charging offers multiple benefits. First, it removes the need for a human operator during the process. Secondly, the wireless charging paradigm is primarily operable in the autonomous driving scenario, where drones can land and charge on specific pads.

2.3 Applied Security over WPT

To mitigate these risks, it is crucial to implement strong encryption, secure communication protocols, regular software updates, and adherence to regulatory guidelines. Here begins my journey, the idea of the internship and work proposed by Alessandro Brighente: A novel physical side channel attack that has the goal of profiling and fingerprinting various types of UAV, just by exploiting the *Wireless Power Transfer_G* between the charging pad and the battery of the drone. It is important to mention that drones are also a viable and competitive option with landed vehicles for various applications like search and rescue and

environmental monitoring, other than military and surveillance activities.⁶

⁶Oludare Isaac Abiodun Abiodun Esther Omolara Moatsum Alawida. «Drone cybersecurity issues, solutions, trend insights and future perspectives: a survey». In: *Springer Nature 2023* 35.10 (2023), pp. 23063–23101. DOI: [10.1007/s00521-023-08857-7](https://doi.org/10.1007/s00521-023-08857-7).

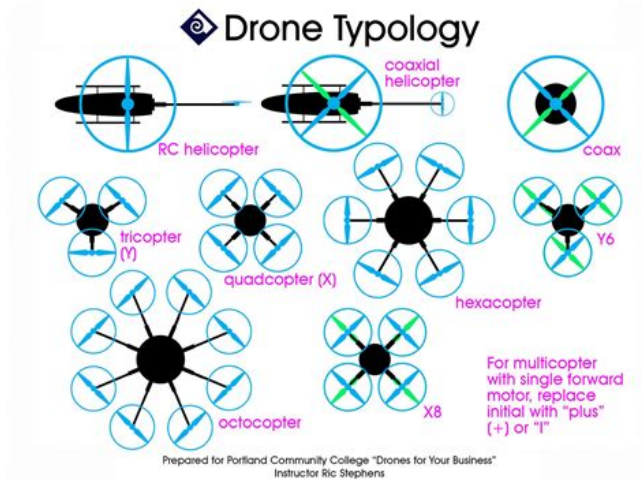


Figure 2.1: Drone schemes based on flying typology⁷



Figure 2.2: Example of the biggest military UAV: RQ-4B⁸

2.4 Setup and Code Interactions

For the prior experiments conducted by Tommaso Bianchi and Alessandro Brighente, the [Bitcraze CrazyFlie 2.1](#) drone was chosen, a small flying drone designed for research purposes, it offers many advantages in drone research for new paradigms and technologies such as autonomous flight: it has open-source firmware, is inexpensive, easy to assemble, and can be expanded with new functionalities. CrazyFlie was designed with the primary goal of offering a platform that aids experimentation and research⁹.

It can be equipped with different decks, among the available ones, the wireless charging expansion was used for the scope of the research. We use the CrazyFlie 2.1 due to the availability of the Qi-compliant wireless charging deck, the ease of modifying the firmware with custom routines, and the absence of actual flight requirements. The drone uses a *LiPo_G* battery. This battery type is light, inexpensive, and physically resilient. The main disadvantages are the short lifespan and the degraded performances after repeated charging cycles, especially if not fully discharged. The benefits make it the best solution for efficiency and energy-to-weight ratio on commercial drones. This kind of battery can also support the energy burst dictated by the spike use of the drone's rotor. The battery model, technical specification, and projected application on such batteries consent to identifying and fingerprinting in the drone environment.

The communication with the drone happens through the Crazyradio 2.0, which establishes the wireless communication channel between the computer software and the drone for firmware flashing and flight commands. Concerning the wireless charging fingerprinting, we adopted the INA219 current sensor available through Adafruit, as explained below . The configuration allows us to measure up to 3.2 A at a 0.8 mA resolution and 1% precision. The sensor is attached to a charging circuit composed of a USB to microUSB cable, connected to the

⁹Wojciech Giernacki et al. «Crazyflie 2.0 quadrotor as a platform for research and education in robotics and control engineering». In: *2017 22nd International Conference on Methods and Models in Automation and Robotics (MMAR)* (2017), pp. 37–42. URL: <https://api.semanticscholar.org/CorpusID:40468941>.

charging pad on one side and a power supply on the other. The charging pad is an Anker Powerwave A2503¹⁰. It is partially compatible with the Qi standard extended power profile updates and can supply up to 10 Watts. This is more than adequate to fulfill the technical specifications of our drone, which can negotiate up to 500 mA at a maximum voltage of 4.2V for its battery. As the distance and the orientation of the two coils can significantly alter the efficiency and response of the power transfer¹¹, the drone was carefully aligned using markings on the charging pad's edge before each trace in an attempt to keep the exact position relative to the charging coil as close as possible.

¹⁰Anker. URL: <https://www.anker.com/eu-en/products/a2503>.

¹¹Jianwei Liu et al. «Privacy Leakage in Wireless Charging». In: *IEEE Transactions on Dependable and Secure Computing* 21.2 (2024), pp. 501–514. DOI: [10.1109/TDSC.2022.3173063](https://doi.org/10.1109/TDSC.2022.3173063).

2.5 Python

Choosing the right programming language is crucial for effective and efficient analysis in technical domains. This section outlines the reasons for selecting Python for our goal.

- **Extensive Libraries:** Python offers a comprehensive ecosystem of libraries such as NumPy, SciPy, and Pandas for numerical and data analysis, as well as Scikit-learn for machine learning. These libraries provide the necessary tools to process and data effectively;
- **Ease of Use:** Python's clear and readable syntax facilitates the writing and understanding of code. This characteristic is particularly beneficial for both rapid prototyping and production-level implementation, allowing researchers and developers to focus on problem-solving rather than syntax intricacies, making it very usable and accessible for everyone;
- **Community Support:** boasts a large and active community that provides extensive documentation, tutorials, and forums. This support network is invaluable for troubleshooting and accelerating the learning process, ensuring that users can find help and resources easily; and this is due to the usability of the language explained above;
- **Integration Capabilities:** integrates seamlessly with other languages and tools, offering flexibility in development and deployment. For example, Python can interface with C/C++ for performance-critical components, allowing for optimized performance where necessary, in our case with Arduino;
- **Visualization Tools:** Python's powerful visualization libraries, such as Matplotlib and Seaborn, enable the creation of detailed and informative visualizations. These tools are essential for interpreting the results and presenting findings clearly, especially for non-insiders;

Code 2.1 Ciao mondo!

```
def main():
    print('Hello World!')
if __name__ == "__main__":
    main()
```

- **Rapid Prototyping:** supports quick development and iteration, which is crucial for testing hypotheses and refining analysis techniques in research and development settings. This capability accelerates the discovery process and helps in developing robust solutions quickly;

<https://www.python.org/>

2.6 The experiment

The [repository](#) "You Are How You Wireless Charge: Drone Wireless Charging Profiling and Fingerprinting" contains the instructions to reproduce the experiments and results for the profiling of drones and fingerprinting its actions during the wireless charging process.

2.6.1 Tools:

- Arduino Micro: to log the data of the current values trough the sensor;
- Current sensor INA219 (available on Adafruit);
- Charging pad: to place our drone and connect it with the arduino aforementioned;
- Bitcraze Crazyflie Drone 2.0: our drone;
- Crazyflie Radio for communication;
- Bitcraze Crazyflie Wireless Charging Dock: needed to wireless charge it;
- Mobile phone with the app or a PS3 controller to fly;

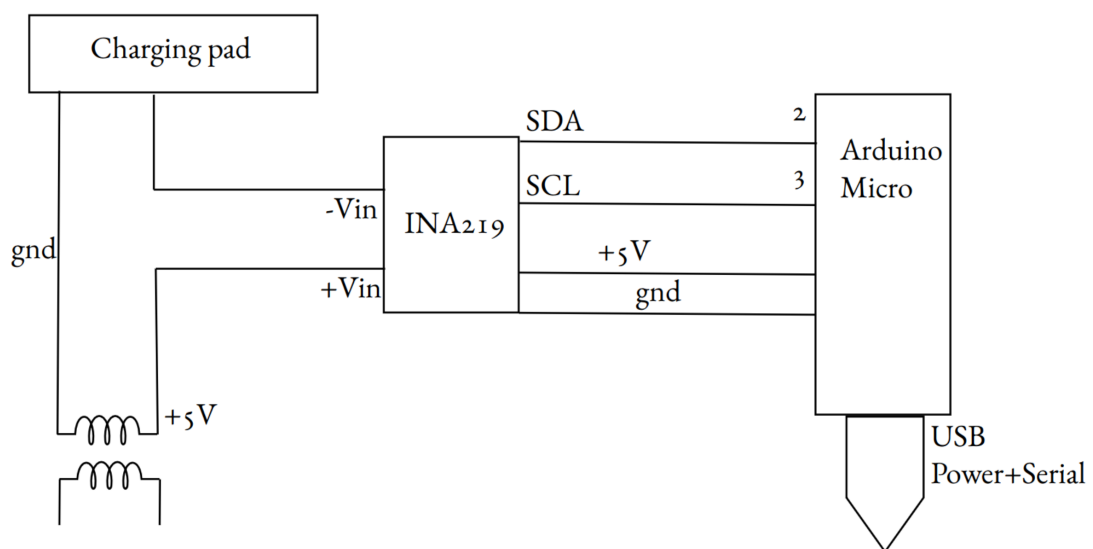


Figure 2.3: Scheme of the circuit setup

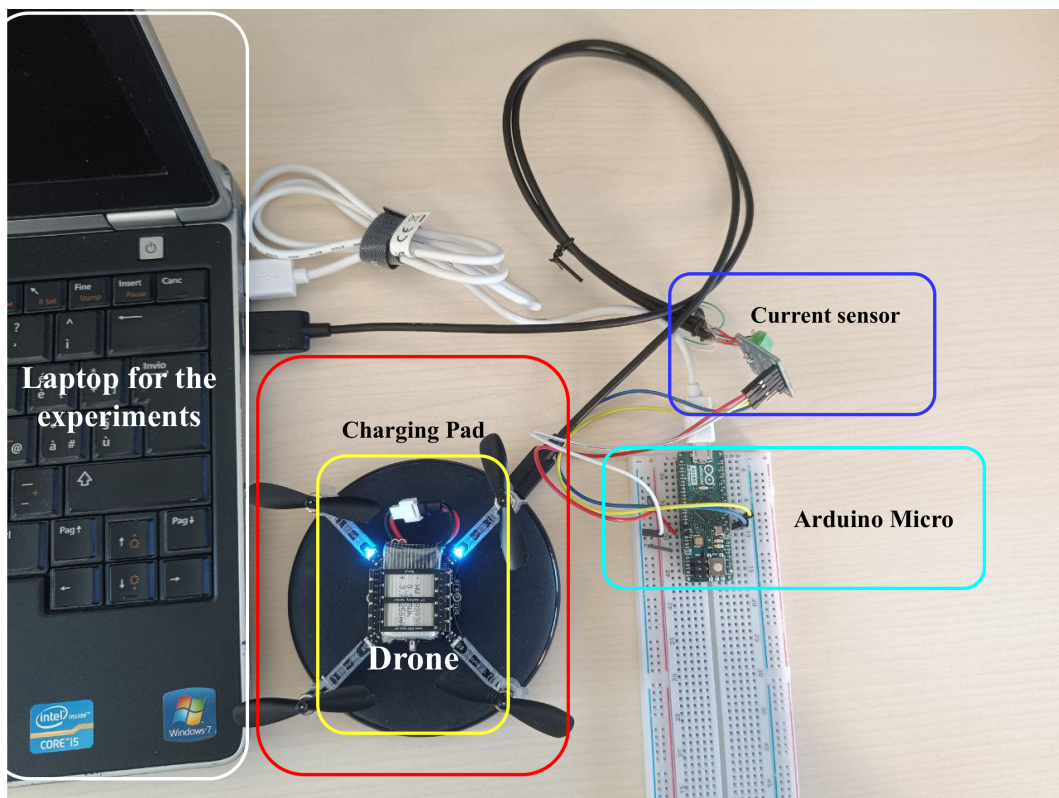


Figure 2.4: Setup



Figure 2.5: Wireless power transfer using Qi

Code 2.2 Usage of minicom

```
minicom -b 115200 -D /dev/ttyACM0 -O timestamp=extended
-z -C path/to/log.log
```

2.6.2 Procedure

In the "arduino" folder, located in the repository are available both the code and the library for the current sensor. To start the script, there is the need to record the logs, this can be done with "minicom" as we did:

- To exit it: CTRL + A, X, Enter;
- The log file is appended and not replaced if restarted;

Code 2.3 Create a Virtual Enviroment

```
$ conda env create -f environment.yml
```

Code 2.4 Start the software

```
$ python3 -m cfclient.gui
```

2.6.3 Use the Bitcraze software and change the firmware

Drone firmware upload through the software: it is possible to easily change firmware through the Bitcraze software "cfclient". Here we used "environment.yml" to create a conda environment:

From the "Connect" menu voice, selecting "bootloader". We selected the drone interface and the stock firmware between the choices or upload a zip file for a custom software. Finally pressing "Program" the experiment will start.

2.6.4 Custom firmware upload

To upload a custom firmware, users can follow the procedure at this page [to upload customized firmware](#) After changing the file of folder we built and uploaded the new firmware. In the firmware folder, while the drone is in bootloader mode, we used:

Code 2.5 Upload the custom firmware

```
$ make clean
```

```
$ make
```

```
$ make cload
```

2.7 Drone Profiling

To profile the drone during the Constant Current phase, you need first to discharge it lower the 3.0 V, more specifically at 2.8 V. In the experiments, we did this procedure with two bootloaders, the stock bootloader and the PX4 bootloader. To install the firmware we used the aforementioned procedure using the software GUI. The zip files are in the "firmwares" folder in the same repository.

2.7.1 The fingerprinting requires the manual procedure to upload the custom firmware for the:

- 1. SHA256 operations
- 2. Radio packet sending

Additionally, we connected the drone through the bluetooth interface for BLE actions. After that, for each action, we recorded the logs while charging at Constant Voltage.

2.7.2 Results

In the "logs" folder, there is the data collected for this work with the analysis scripts. Additionally, the Machine Learning grid search and results are available in the action recognition folder. To create the dataset, we registered 20 samples for each action. Also, we provide an additional script to create the dataset to use with "tsfresh" tool for feature extraction. The machine learning approach is available in a "ipynb" file. The results show a clear distinction between different software on board of the drone and current behavior, which was easily distinguishable with different machine learning algorithms, the results show that we can precisely identify both the firmware and the communication protocol of a drone.

Chapter 3

Internship description

In this chapter I will go through the many aspects of my Internship.

3.1 Introduction to the literature

3.1.1 Introductory model

During the first period of my internship I learned how and why side-channel attacks are portrayed through the reading of many papers about side-channel security on mobile phones¹, vehicles, and anything IoT related that could be exploited². I read documentation regarding the libraries I had to use and implement in the project.

This was followed by many attempts of producing a reliable PoC_G , the main goal was to obtain as many features as I could from the data that was already logged from the various firmwares, based on the idea that extracting those features from the queues of the current series that were stored could lead to an attempt of profiling and fingerprinting various models and types of drones.

One possible threat scenario could be based in a public wireless power transfer base station for drones, where the owning company wants only the paying customers, or the ones with the specific privileges to use the aforementioned pad,

¹10.1145/3460120.3484733.

²Mauro Conti et al. «The Dark Side (-Channel) of Mobile Devices: A Survey on Network Traffic Analysis». In: *IEEE Communications Surveys & Tutorials* 20.4 (2018).

another could be that we do not want the drones to be profiled and fingerprinted by the charging station producing company or a malicious attacker.

3.1.2 The idea

Alessandro Brighente et al. published a paper where a novel side-channel attack on wireless power transfer for Electric Vehicles was introduced; described as follows: after identifying the two phases of a charging session, we discussed how security and privacy research should focus also on the actual charging phase. In particular, we discussed the privacy concerns arising when a user gets access to the physical signals exchanged from EV and EVSE in public premises. We propose EVScout, a profiling attack that exploits the electric current exchanged during the charging process to profile EVs. Together with EVScout, we also proposed a feature extraction algorithm based on the intrinsic characteristics of the EVs' battery. We then tested EVScout on real world-data. By thoroughly numerical evaluation, we showed that EVs can be profiled based on their charging session, with sufficient confidence despite the increasing number of costumers in the network³.

³Izza Sadaf Alessandro Brighente Mauro Conti. «Tell Me How You Re-Charge, I Will Tell You Where You Drove To: Electric Vehicles Profiling Based on Charging-Current Demand». In: *ESORICS 2021, LNCS 12972* 35.10 (2021), pp. 51–667. DOI: [10.1007/978-3-030-88418-5_31](https://doi.org/10.1007/978-3-030-88418-5_31).

3.2 Understanding Ohm's law with real world applications

Ohm's Law is a fundamental principle in the field of electrical engineering and physics. It states that the current through a conductor between two points is directly proportional to the voltage across the two points, this was important to understand how the CC (constant Current) and (CV) Constant Voltage regimes work.

3.2.1 Formula

The mathematical expression of Ohm's Law is given by:

$$V = IR \tag{3.1}$$

where:

- V is the voltage (in volts),
- I is the current (in amperes),
- R is the resistance (in ohms).

3.2.2 Explanation

In this formula:

- Voltage (V) is the electrical potential difference between two points.
- Current (I) is the flow of electric charge.
- Resistance (R) is the opposition to the flow of current.

This of course led to the analysis of the behaviour of the function describing the Current and the Voltage. The power module on board the drone uses the Constant Current/Constant Voltage (CC/CV) strategy: if the partially discharged battery is immediately subjected to large charging currents, it offers optimal charging performance. This approach splits the charging process into two distinct phases. During the constant current phase, the battery is supplied with a specific reference current, and the charging voltage slowly increases to the maximum value. This lasts most of the charging process, typically until the battery has reached 80% of its total capacity. At this point, the battery enters the constant voltage phase, in which the final voltage is applied to the battery, and the current slowly decreases until the battery reaches full capacity. The Constant Current regime persists for most of the charging process. Its progression with the complete analysis of the Constant Voltage regime gives us helpful information to profile the vehicle and discriminating between firmware software. By contrast, focusing only on the Constant Voltage regime, we directly correlated the input current and the drone state. Comparing the instantaneous current draw with a normal baseline can leak the action performed by the drone.

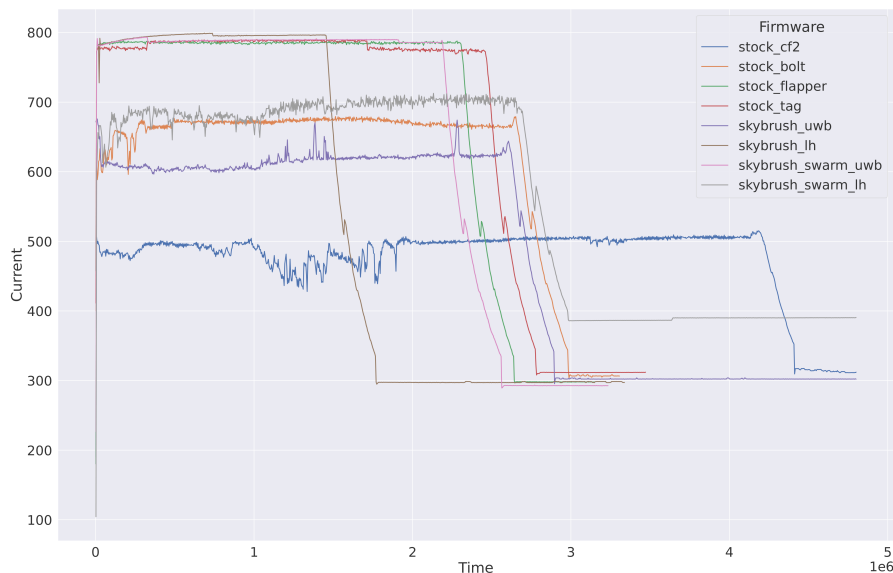


Figure 3.1: Wireless power transfer curves using Qi

3.3 Model

We consider a drone needing a charging session to continue delivering its on-site service. To this aim, we assume that the drone is equipped with a WPT module that allows it to connect to a public WPT charging station to charge its battery.

The charging process involves using a protocol to communicate between the platform and the drone. The WPT base station, i.e., the device delivering the power, might be either a fixed base station connected to the electric grid, or an assistant drone with WPT capabilities and sufficient resources to deliver the charging service⁴.

Depending on the application, the drone can exchange various communications with other drones or with ground stations. Moreover, the on-board systems are continuously processing the input received by the drone's sensors, used for the maneuvers during the normal working behavior or while performing coordinated actions with other drones, e.g, collecting data for surveillance, aerial mapping, or monitoring⁵. Also while making these actions, the drone could be in a charging state thanks to the WPT with a charging pad or another drone. An adversary can aim to recognize the different packets or the action taken by a drone exploiting the wireless charging process through a rogue base station. The fingerprinting of actions or profiling of specific drones can leak information about the process in action and lead to more severe attacks, for example the bypass of drone surveillance system if the attacker can understand where the drone is located through the charging process.

⁴Sandipan Dey et al. «Bidirectional Wireless System for drone to drone opportunity charging in a multi agent system». In: *2023 International Conference on Control, Communication and Computing (ICCC)*. 2023, pp. 1–5. DOI: [10.1109/ICCC57789.2023.10164995](https://doi.org/10.1109/ICCC57789.2023.10164995).

⁵Prithvi Krishna Chittoor, Bharatiraja Chokkalingam, and Lucian Mihet-Popa. «A Review on UAV Wireless Charging: Fundamentals, Applications, Charging Techniques and Standards». In: *IEEE Access* 9 (2021), pp. 69235–69266. DOI: [10.1109/ACCESS.2021.3077041](https://doi.org/10.1109/ACCESS.2021.3077041).

3.4 Coding and Debugging

The major part of my the time I spent working on the project was reading documentation and the code that Tommaso Bianchi had already written, dealing with plenty of new libraries and documentation which taught me a lot, Alessandro Brighente and Tommaso Bianchi helped me troughout the whole process of picking up the codebase they wrote.

3.4.1 Libraries:

- [Numpy](#): is a library for the Python programming language, adding support for large, multi-dimensional arrays and matrices, along with a large collection of high-level mathematical functions to operate on these arrays;
- [Pandas](#): is a software library written for the Python programming language for data manipulation and analysis. In particular, it offers data structures and operations for manipulating numerical tables and time series;
- [Tsfresh](#): is a python package. It automatically calculates a large number of time series characteristics, the so called features. Further the package contains methods to evaluate the explaining power and importance of such characteristics for regression or classification tasks;
- [Library for the Adafruit INA219 high side DC current sensor board](#);
- [Matplotlib](#): is a comprehensive library for creating static, animated, and interactive visualizations in Python;
- [Seaborn](#): is a Python data visualization library based on Matplotlib. It provides a high-level interface for drawing attractive and informative statistical graphics;

Code 3.1 Reading Data, creating a DataFrame

```
df = pd.read_csv('interpolated_logs.csv')
```

Code 3.2 Extraction of Current and Time Series

```
for i, d in df.filter(items=["Current", "Firmware"]).groupby("Firmware"):  
    current_series = d.values.tolist()  
for i, f in df.filter(items=["Time", "Firmware"]).groupby("Firmware"):  
    time_series = f.values.tolist()
```

3.5 Our work

After exposing myself to the new technologies and setup for the experimentation, I mainly wrote code that followed up the main goal of the codebase which was exploring the features of the various logs of data, embedded in a csv that was used in the form of a Pandas DataFrame for matters of convenience. After reading the data I extracted the Time and current series, found the queue of the function and applied a moving average filter: given a series of numbers and a fixed subset size, the first element of the moving average is obtained by taking the average of the initial fixed subset of the number series. Then the subset is modified by "shifting forward"; that is, excluding the first number of the series and including the next value in the subset. It is used with time series data to smooth out short-term fluctuations and highlight longer-term trends in our case.

3.5.1 Coding

Code 3.3 Unpacking the list of lists, using x as an index of the list of firmware names

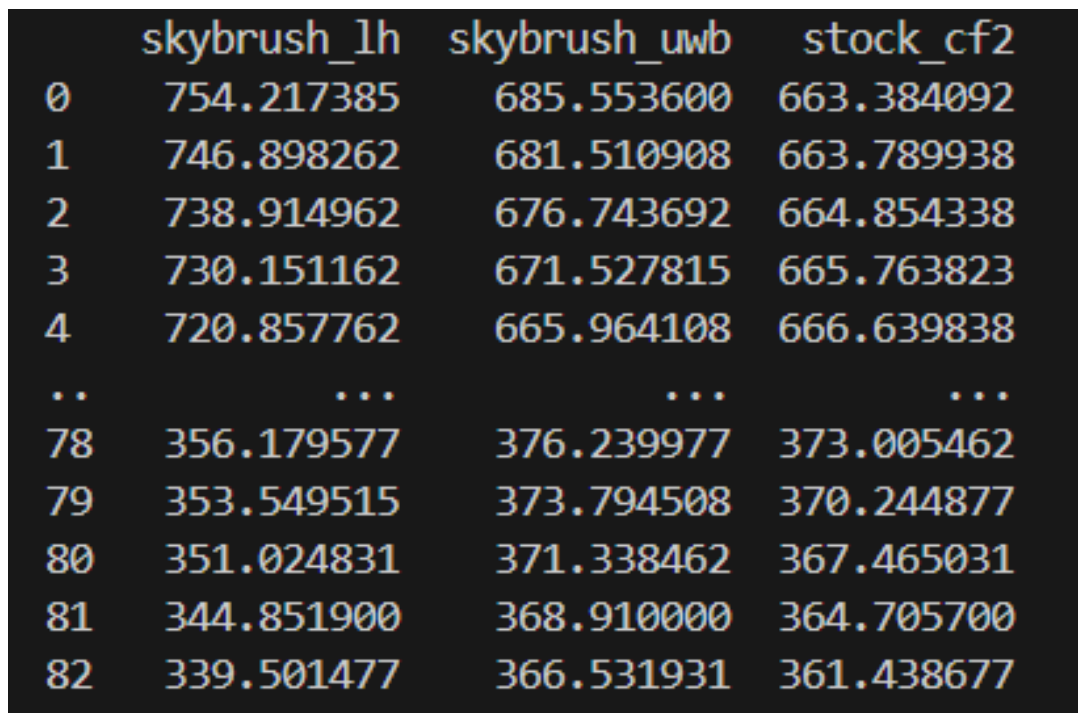
```
def unpack_list(mylist, x):  
    list1 = []  
    for i in mylist:  
        list1.append(i[x])  
    return list1
```

Code 3.4 Application of Moving Average Filter to smoothen the function curve

```
def movingAverage(s, N):
    cumsum, moving_aves = [0], []
    for i, x in enumerate(s, start=1):
        cumsum.append(cumsum[i - 1] + x)
        if i >= N:
            moving_ave = (cumsum[i] - cumsum[i - N]) / N
            moving_aves.append(moving_ave)
    return moving_aves
```

This table represents the queues for each firmware from where we extracted the features we needed for a profiling and fingerprinting point of view.

3.6 Graphical Results



	skybrush_1h	skybrush_uwb	stock_cf2
0	754.217385	685.553600	663.384092
1	746.898262	681.510908	663.789938
2	738.914962	676.743692	664.854338
3	730.151162	671.527815	665.763823
4	720.857762	665.964108	666.639838
..
78	356.179577	376.239977	373.005462
79	353.549515	373.794508	370.244877
80	351.024831	371.338462	367.465031
81	344.851900	368.910000	364.705700
82	339.501477	366.531931	361.438677

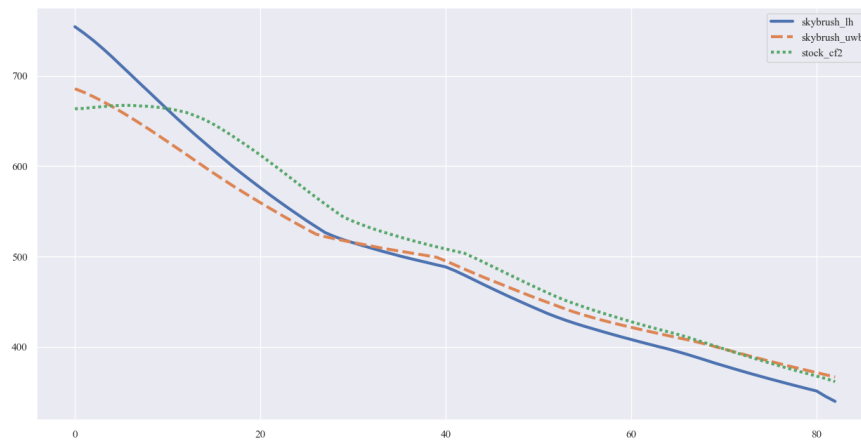
Figure 3.2: Data Table from the queues of various firmwares

This is the actual plot of the queues for the firmwares present in the table 3.2, and found through the shown algorithm:

Code 3.5 Function to find the queue, where the feature are found

```
def find_queue(current_list):
    queue_list = []
    found = False
    for i in range(0, len(current_list)-1):
        diff = abs(current_list[i+1]-current_list[i])
        if diff >= 5:
            queue_list.append(current_list[i])

            j = 1
            zero_counter = 0
            while zero_counter != 5:
                diff = abs(current_list[i+j+1]-current_list[i+j])
                queue_list.append(current_list[i+j])
                if int(diff) == 0:
                    zero_counter += 1
                j += 1
            found = True
            break
    if found:
        break
    return queue_list
```

**Figure 3.3:** Plot of the queues of various firmwares

Chapter 4

Reflections

4.1 Conclusions on the Project

Using only a current sensor, the project presented a profiling and inference attack over drones' wireless charging. The attack is easy to carry out and requires no deep knowledge of this field or peculiar skills. Depending on the attacker's capabilities, more sensors could be placed to reach a greater level of granularity and extend the analysis to other protocols and actions. The accuracy results are auspicious, and a more precise analysis is intended for future work to further extend the profiling analysis and perform critical attacks against privacy and drone usage.

4.2 Future work

This thesis explored the profiling of drones through side channel analysis, a technique that leverages indirect indicators of system operation to infer critical information about the device, to do so we should have access to plenty of different drones and their firmwares. Seeing the potential of the study conducted before with smartphones both Android and iOS, then Electric Vehicles demonstrated that side channel analysis could effectively differentiate between various entities' operating conditions and detect anomalies indicative of potential security breaches. This kind of approaches emphasize the importance of integrating

side channel analysis with existing drone security protocols and highlight the importance that hardware has in security. By incorporating these techniques, it is possible to enhance the detection and prevention of malicious activities such as unauthorized firmware modifications, GPS spoofing, jamming attacks and mitigate the risks mentioned in the Introduction of this work.

4.3 Threats and Mitigation

Due to the increasing prevalence of commercial drones operating in civilian airspace, issues of national security, including those related to privacy, have risen to the forefront of public attention. Therefore, organizations from different sectors (including business, education, industry, the military, and law enforcement) need to collaborate to develop new security frameworks, standards, and rules. The next generation of commercial drones is being released to the market by existing manufacturers right now, but security and privacy concerns are still lagging behind. However, because of the importance of drone applications, security has become a key problem, necessitating the development of effective solutions to safely guide and preserve stolen data. This survey is a useful resource for both manufacturers, and researchers who want to learn more about constructing and designing secure drone designs. Research gaps in the study will provide research focus on how to address the security issues with drones. The major limitation of this research was the lack of co-operation from some stakeholders, like the manufacturers and regulatory organizations, to state out their problems in addressing the issue of flying drone cyberattack detection and prevention. DDoS attacks are predicted to increase in volume and frequency due to the growth of the *IoD_G* technological developments, the demand for access to sophisticated systems, and historical trends. Cyber thieves are likely to continue looking for and exploiting weaknesses in these systems in order to use them in DDoS and RDoS attacks. Plans to deploy 5G capabilities, together with recent developments and the ongoing digital transformation, have created new opportunities for threat actors to infiltrate. Monitoring pre-existing and new technologies,

ensuring new regulations are followed, and adhering to security best practices for managing enterprise networks and remote workforces are all key aspects of securing critical infrastructure. Every internet user has to understand the basics of cyber hazards and risks. Drone technology has sparked a surge in commercial interest that shows no signs of abating. Drones and drone technology, in reality, appear to have a bright and exciting future. Future generations of UAV are expected to have increased autonomy as well as greater safety and regulatory norms. These and other improvements have the potential to have a significant impact on a variety of industries, including commercial transportation, logistics, and the military. On the other hand, the security and privacy aspects of drones require urgent attention from academia, manufacturers, aviation, the military, and the government¹.

¹Abiodun Esther Omolara, «[Drone cybersecurity issues, solutions, trend insights and future perspectives: a survey](#)».

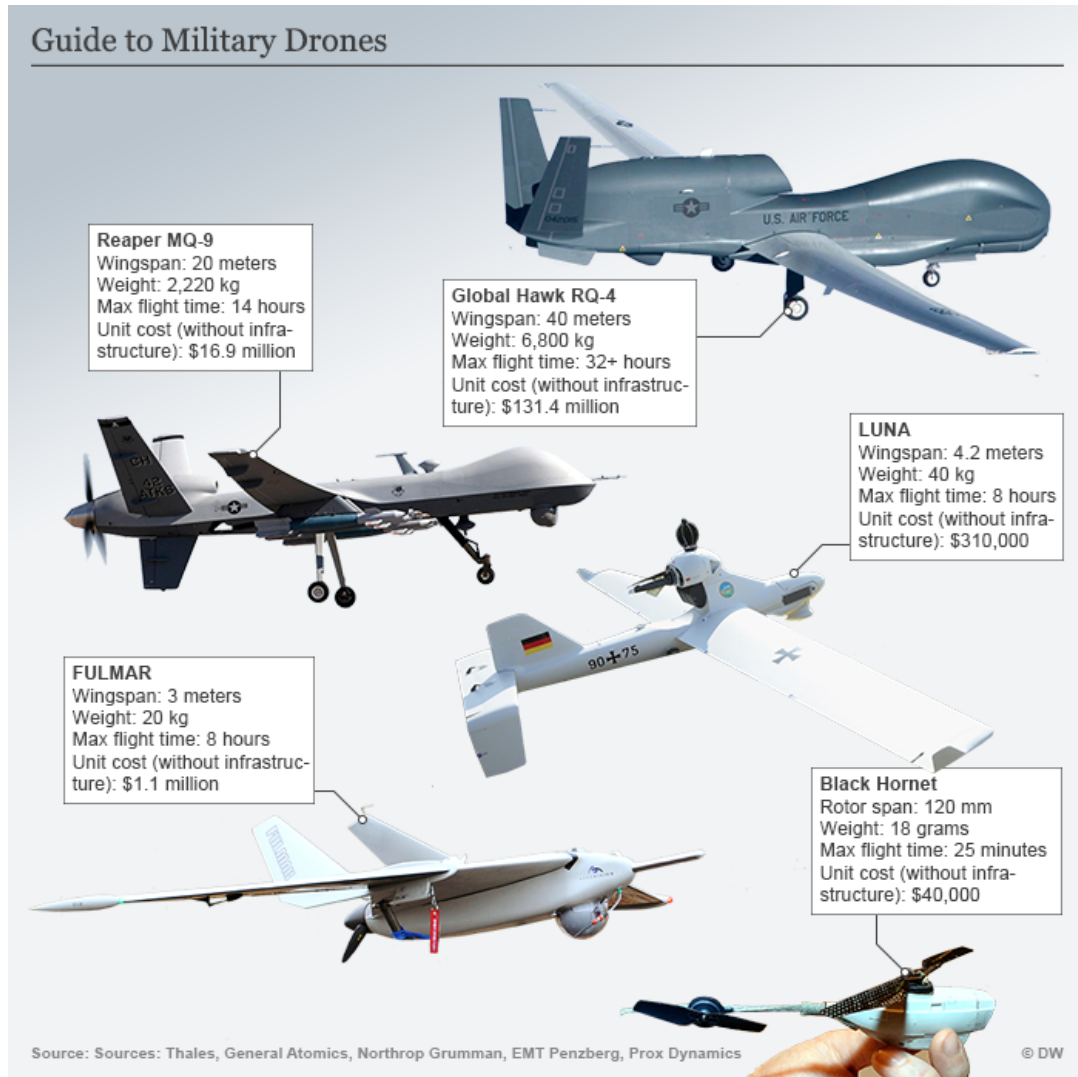


Figure 4.1: Military Drones²

Using only a current sensor, we presented a profiling and inference attack over drones' wireless charging. The attack is easy to carry out and requires no deep knowledge of this field or peculiar skills. Depending on the attacker's capabilities, more sensors could be placed to reach a greater level of granularity and extend the analysis to other protocols and actions. The accuracy of the results are auspicious, and a more precise analysis is intended for future work to further extend the profiling analysis and perform critical attacks against privacy and drone usage.

Chapter 5

Conclusions

5.1 Final Accounts

This intersection field presents a promising approach for advancing security research that could extend this work by exploring additional side channels and developing more sophisticated analytical models. The findings of this thesis lay the groundwork for a more secure and reliable deployment of drones in various critical applications. Testing data from new drones could lead to results that are even more promising in the field of side-channel analysis and drone security, hoping to be part of this ongoing process that interests me and work with the people I had the privilege to learn from, both during the Internship, the group seminars and the work of others before me: thinking outside the box and pursuing yet unknown ideas has always been a dream of mine; now I know for sure it is possible, in the field of research surrounded by empowering people.

5.2 Achievements

During the time spent on this project I learned how to manage my own time and the time to dedicate to group work. Followed all the seminars organized by Professor Conti the research group leader, and mastered my skills of self learning with the approach of both curiosity and duty. The main goal for me was to do a good job, help the project to go further and mainly writing good code and

learning how to use new frameworks and technologies without forgetting the nature of the internship which was learning how to work in a security group at the state of the art in the field. The main achievement for me was the journey of learning.

Code 5.1 Main

```
def main():
    df = pd.read_csv('interpolated_logs.csv')

    queues = []
    firmware_names = []
    for i, d in df.filter(items=["Current", "Firmware"]).groupby("Firmware"):
        vals = d.values.tolist()
        firmware_names.append(vals[0][1])
        current_values = [i[0] for i in vals][::-1]
        queues.append(find_queue(current_values)[::-1])

    queue_df = pd.DataFrame(list(zip((movingAverage(queues[0], N)),
        (movingAverage(queues[1], N)), (movingAverage(queues[2], N)))), columns=firmware_names)

    sns.set_theme()
    plt.figure(figsize=(8,12))
    plt.rcParams['font.family'] = 'serif'
    plt.rcParams['font.serif'] = ['Times_New_Roman'] + plt.rcParams['font.serif']

    ax = sns.lineplot(
        data=queue_df,
        linewidth = 3
    )

    plt.savefig("../code.pdf")
    plt.show()
    return

if name == "main":
    main()
```

5.3 Acquired knowledge

Other than the aforementioned, I read many papers and Surveys that contained not only what I strictly needed to do at the beginning of the internship, this was a choice and a case that led me to have a broader and open point of view on the topic. The intricated relations between the many aspects of this research apply not only in the field of UAV but also in telecommunications and of course strategic studies where humanities and economical works are deeply involved. So I would say that not only my hard skills in coding and security got a great boost from this experience but also my soft ones, needed in my opinion to better understand situations, people and threat models.

5.4 Personal evaluation

At the end of my internship I can only say that it was a more than formative and important experience for myself and my academical journey. It was also very difficult and challenging, this is what made it even more peculiar and special to me, and I hope useful to my colleagues and Professor Brighente. What I believe is that I did everything that was in my power and put all of myself into this project, and this is also because of the enviroment that surrounds the SPRITZ group, not only based on the work I did.

Bibliography

Texts

Administration, Federal Aviation. *Drone Security: A Guide to Protecting Your Drone*. 2020 (cit. on p. 8).

Foundation, Electronic Frontier. *Drone Privacy: A Guide to Protecting Your Privacy*. 2020 (cit. on p. 8).

Organization, International Civil Aviation. *Drone Attacks: A Growing Concern*. 2019.

Project, Open Web Application Security. *Drone Security Testing: A Guide to Identifying Vulnerabilities*. 2020 (cit. on p. 8).

Union, European. *European Union General Data Protection Regulation*. 2016 (cit. on p. 8).

Articles

Abiodun Esther Omolara Moatsum Alawida, Oludare Isaac Abiodun. «Drone cybersecurity issues, solutions, trend insights and future perspectives: a survey». In: *Springer Nature 2023* 35.10 (2023), pp. 23063–23101. DOI: [10.1007/s00521-023-08857-7](https://doi.org/10.1007/s00521-023-08857-7) (cit. on pp. 10, 34).

Alessandro Brighente Mauro Conti, Izza Sadaf. «Tell Me How You Re-Charge, I Will Tell You Where You Drove To: Electric Vehicles Profiling Based on Charging-Current Demand». In: *ESORICS 2021, LNCS 12972* 35.10 (2021), pp. 51–667. DOI: [10.1007/978-3-030-88418-5_31](https://doi.org/10.1007/978-3-030-88418-5_31) (cit. on p. 23).

- Chittoor, Prithvi Krishna, Bharatiraja Chokkalingam, and Lucian Mihet-Popa. «A Review on UAV Wireless Charging: Fundamentals, Applications, Charging Techniques and Standards». In: *IEEE Access* 9 (2021), pp. 69235–69266. DOI: [10.1109/ACCESS.2021.3077041](https://doi.org/10.1109/ACCESS.2021.3077041) (cit. on p. 26).
- Conti, Mauro et al. «The Dark Side (-Channel) of Mobile Devices: A Survey on Network Traffic Analysis». In: *IEEE Communications Surveys & Tutorials* 20.4 (2018) (cit. on p. 22).
- Gacanin, Haris and Amir Ligata. «Wi-Fi Self-Organizing Networks: Challenges and Use Cases». In: *IEEE Communications Magazine* 55.7 (2017), pp. 158–164. DOI: [10.1109/MCOM.2017.1600523](https://doi.org/10.1109/MCOM.2017.1600523) (cit. on p. 3).
- Giernacki, Wojciech et al. «Crazyflie 2.0 quadrotor as a platform for research and education in robotics and control engineering». In: *2017 22nd International Conference on Methods and Models in Automation and Robotics (MMAR)* (2017), pp. 37–42. URL: <https://api.semanticscholar.org/CorpusID:40468941> (cit. on p. 12).
- Han, Jin et al. «RANGO: A Novel Deep Learning Approach to Detect Drones Disguising from Video Surveillance Systems». In: *ACM Trans. Intell. Syst. Technol.* 15.2 (Feb. 2024). ISSN: 2157-6904. DOI: [10.1145/3641282](https://doi.org/10.1145/3641282). URL: <https://doi.org/10.1145/3641282> (cit. on p. 8).
- Liu, Jianwei et al. «Privacy Leakage in Wireless Charging». In: *IEEE Transactions on Dependable and Secure Computing* 21.2 (2024), pp. 501–514. DOI: [10.1109/TDSC.2022.3173063](https://doi.org/10.1109/TDSC.2022.3173063) (cit. on p. 13).
- Park, Jihong et al. «Extreme ultra-reliable and low-latency communication». In: *Nature Electronics* 5 (Mar. 2022), pp. 1–9. DOI: [10.1038/s41928-022-00728-8](https://doi.org/10.1038/s41928-022-00728-8) (cit. on p. 3).
- Sharma, Abhishek et al. «Communication and networking technologies for UAVs: A survey». In: *Journal of Network and Computer Applications* 168 (2020), p. 102739. ISSN: 1084-8045. DOI: <https://doi.org/10.1016/j.jnca.2020.102739>. URL: <https://www.sciencedirect.com/science/article/pii/S1084804520302137> (cit. on p. 3).
- Standards, National Institute of and Technology. «Digital Identity Guidelines». In: *NIST Special Publication* 800-63-3 (2017).

Websites

Anker. URL: <https://www.anker.com/eu-en/products/a2503> (cit. on p. 13).

Drones. URL: <https://marieladesnhkline.blogspot.com/2022/04/the-different-types-of-drones-explained.html>.

Military Drones. URL: <https://www.evergladesuniversity.edu/blog/guide-different-types-drones-unmanned-aerial-systems/>.

P-cons. URL: <https://www.wirelesspowerconsortium.com/qi/> (cit. on p. 4).

RQ-4B. URL: <https://loredaily.com/this-is-americas-biggest-uav-meet-the-rq-4-global-hawk/>.

Statistics. URL: <https://www.dronebrands.org/drone-statistics/> (cit. on p. 2).

UAV. URL: <http://www.thefreedictionary.com/Unmanned+Aerial+Vehicle> (cit. on p. 1).

UAV. URL: <https://www.animalia-life.club/qa/pictures/the-drones-are-located-where.html>.

Webliography

Websites

Anker. URL: <https://www.anker.com/eu-en/products/a2503> (cit. on p. 13).

Drones. URL: <https://marieladesnhkline.blogspot.com/2022/04/the-different-types-of-drones-explained.html>.

Military Drones. URL: <https://www.evergladesuniversity.edu/blog/guide-different-types-drones-unmanned-aerial-systems/>.

P-cons. URL: <https://www.wirelesspowerconsortium.com/qi/> (cit. on p. 4).

RQ-4B. URL: <https://loredaily.com/this-is-americas-biggest-uav-meet-the-rq-4-global-hawk/>.

Statistics. URL: <https://www.dronebrands.org/drone-statistics/> (cit. on p. 2).

UAV. URL: <http://www.thefreedictionary.com/Unmanned+Aerial+Vehicle> (cit. on p. 1).

UAV. URL: <https://www.animalia-life.club/qa/pictures/the-drones-are-located-where.html>.