Investigation on vulnerabilities, threats and attacks prohibiting UAVs charging and depleting UAVs batteries: Assessments & countermeasures
Fadhila Tlili, Lamia Chaari Fourati, Samiha Ayed, Bassem Ouni

To cite this version:

HAL Id: cea-04129711
https://hal-cea.archives-ouvertes.fr/cea-04129711
Submitted on 15 Jun 2023

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
Investigation on Vulnerabilities, Threats and Attacks Prohibiting UAVs Charging and Depleting UAVs Batteries: Assessments & Countermeasures

Fadhila Tlili\textsuperscript{a,b,c}, Lamia Chaari Fourati\textsuperscript{b}, Samiha Ayed\textsuperscript{c} and Bassem Ouni\textsuperscript{d}

\textsuperscript{a}National School of Electronics and Telecommunications of Sfax, Sfax, Tunisia
\textsuperscript{b}Digital Research Center of Sfax (CRNS), Laboratory of Signals, systeMs, aRtificial Intelligence, neTworkS (SM@RTS), Sfax University; TUNISIA
\textsuperscript{c}LIST3N-ERA Laboratory, University of Technology of Troyes, Troyes, France
\textsuperscript{d}The French Alternative Energies and Atomic Energy Commission (CEA), Paris, FRANCE

\textbf{ABSTRACT}

Unmanned aerial vehicles (UAVs) are the current leading devices used by different sectors. They open doors to new opportunities for investors and business service providers. Their exponential growth turns the visibility of attackers to a new target to implement attacks. Researchers aim to fend off these attacks to empower UAVs security. Based on this motivation, this survey stands for UAVs attacks assessments against the based-system and the charging system. Also, the paper highlights UAVs battery depletion attacks. Furthermore, the paper presents different mitigations that stand against UAVs battery depletion attacks and UAVs charging system attacks. Besides, related research projects are explored.

1. Introduction

Unmanned aerial vehicles [1], commonly known as drones, have gained a lot of attention by being increasingly used in many sectors. According to current statistics, UAVs market is expected to grow exponentially at a Compound Annual Growth Rate (CAGR) of 14.1 billion starting from 2020 falling to $ 21.8 billion in 2027 [2]. Based on the Indian federation of Chambers of Commerce and Industry [3], the market is expected to reach 885.7 million USD per year in India. In the first place, UAVs were used to serve military missions. Consequently, they gained the technological power to be used in many disciplines. Therefore, their usability is no longer limited to military applications. UAVs respond to the requirements of various missions over considerable applications areas such as agriculture, media coverage, emergency services, and healthcare, atmospheric mentoring, object detection, tracking, surveillance, and data collection. Recently, UAVs have also served for crowd control and public space sterilization as an actor against the COVID-19 pandemic [4]. Moreover, UAVs are serving the research domain and developers constantly search to offer new services using these aerial vehicles. In this context, a British multinational defense technology company named QinetiQ exposed in 2019 a new banshee next-generation UAV prototype with dual gasoline engines able to reach a high speed of over 900 km/h [5]. However, UAVs-based systems have many vulnerabilities that increase the rate of being exposed to attacks and to different security issues. They share most of all the

\begin{itemize}
\item Fadhila Tlili
\item Lamia Chaari Fourati
\item Samiha Ayed
\item Bassem Ouni
\end{itemize}
same vulnerabilities as manned aircraft [6]. Nowadays, many relevant research studies are devoted to assess UAVs vulnerabilities, threats, and attacks and to propose a countermeasure solution. The goal is to raise and maintain UAVs safety and security.

1.1. General Context: UAVs Systems and Applications

UAVs are a novel emerging "flying IoT" device, a self-operating cyber-physical device designed as autonomous non-board pilots. Due to its mobility, flexibility, and easy deployment, UAVs are being widely used to expand various IoT services. To maintain the desired environment under the Ground Control Station (GCS) control with the remote-control operation, four critical components of the UAV system must coordinate and operate. They are precisely the sensors, hardware, software, and the communication system [7]. In addition, they could carry payloads like cameras and others. There are different sensors where each one is responsible for a defined mission to correlate the internal and the external state of the UAV safety. e.g., The Inertial Measurement Unit (IMU) used to calculate the UAV force and to define its direction. Also, the global position system (GPS) sensor sets up the path and locates the drone.

1.1.1. UAVs Categories Classification

In general, UAVs could be classified into three categories based on their size, maximum range, and altitude (see Figure 1):

Size-based classification: there are very small UAVs and small UAVs with superior image diffusion, reasonable speed control, and low power consumption. One of the best small UAVs in the market is the DJI Mavic 2 pro [8]. Medium UAVs include parrot airborne cargo mini-UAVs. Also, large UAVs are highly secured and used in the military and surveillance context.

Maximum range-based classification: there are close-range UAVs like quadcopters. These UAVs cover 50Km from 45 minutes to 12 hours in the air. Also, mid-range UAVs like raven cover 150Km for 12 hours. But these UAVs are not optimally secure due to the vulnerable associated resources. Also, endurance UAVs are similar to predator drones that cover 450Km for hours in the air.

Altitude-based classification: there are two main types which are high altitude platforms (HAP) and low altitude platforms (LAP). The first occupies a large region and has a powerful, long-lasting battery. The other type is fast and easy to deploy with quick mobility, but it has high-cost batteries.
In this context, John F. et al. [9] classified UAVs based on a similar category in addition to the power classification. Power classes are divided based on power consumption and sources. The first one is related to UAVs size, weight, and range. At the same time, the second group is classified based on many sources like battery, Wireless Power Transfer (WPT), and other power sources.

1.1.2. Potential UAVs Deployment Domains

UAVs achieved significant technical advancements in their software and hardware components. As a result, their civilian usage has increased dramatically. In 2016, UAVs global commercial market size was estimated by $5.8 Billion and is anticipated to reach $130 Billion by 2025 (Grand View Research and Worth, 2025). Based on [10], UAVs predicted value of business services is estimated by 127$ billion in 2020 coming from the investment. They are increasingly being used in various areas, including public security and safety, infrastructure, transport, agriculture, and green lands services, insurance, mining, media, and telecommunication. The incomes of these applications are illustrated in Figure 2.

UAVs offer a new vision for these applications to solve various problems in real time[11]. It provides many advantages which have been used in these applications as follows:

- Security and disaster relief prevent a significant increase in the proportion of humanity loss, damages, and public safety. In [12], UAVs are used to monitor soldiers’ safety through UAVs in war or terrorist attacks. The author used UAVs above the battlefield to collect data from a system mounted on the soldiers’ jackets to monitor their health. Hence, UAVs provide connectivity between connected soldiers and the remote control system.

- Monitoring inaccessible areas and disasters using swarms of UAVs to check in real-time the area status. In [13], the study monitors forest disasters such as firefighting by distributing separate UAVs to distinct fire areas based on their relative distances. The author applies a particle swarm optimization (PSO) algorithm to effectively schedule its path to its appointed fire area.

- Anticipating smart cities and city-wide IoT infrastructure that provided wireless sensor networks, real-time data, and relay networks. [14] studied the potential of UAVs to enable intelligent transportation...
systems for smart cities. Many services cases are reviewed, such as providing an advance report to the rescue team, real-time accidents reports, and transmitting warnings about road potential dangers.

- Photography and cinematography domains used UAVs in aerial filming to get a high grade of creativity with the angle of the bird’s eye. [15] proposes a novel approach for autonomous cooperative planning for cinematography. The main feature of this system is the ability to reproduce autonomous smooth shots under rules for both static and mobile targets.

- Agriculture applications used UAVs in scheduling irrigation, plant pathology, soil mapping, and helping farmers in instant insights. [16] reviews UAVs usability in precision agriculture. The paper describes the usage of UAVs to respond to crop growth progress in real-time.

- Traffic and Transport uses UAVs to collect real-time information about the road traffic conditions. [17] evaluates a system of multiple UAVs for traffic management to identify the vehicles on road segments. Therefore, it aims to detect and identify driver behaviour and vehicle rating.

1.1.3. **UAVs Communication Systems**

UAVs continuously communicate with the GCS via a downlink dedicated to telemetry, which operates in a protected spectrum. This communication requires establishing a bidirectional link between the UAV and the GCS to exchange data. As a result, it will guarantee the ability to make changes and transmit instructions during the flight. UAVs integrate eight communication links counting satellite and cellular links (see Figure 3), which are:

- **L1**: communication link between an UAV with another, which is commonly based on IEEE 802.11.
- **L2**: communication the UAV and the BS.
• **L.3**: correspond to the connection link between the BSs
• **L.4**: correspond to the connection link between the GCS and the BS
• **L.5**: communication between the WSNs and the BS.
• **L.6**: corresponds to the connection link between ground users (GUEs) with the UAV.

Furthermore, maintaining communication between Multi-UAVs to guarantee cooperation is tough. In addition, the available frequencies of UAV-enabled wireless communication networks are limited as described in [18]. The most suitable solution is to use an ad hoc network to link UAVs [19]. The authors in [20] evaluated distinct communication architectures (direct, cellular, UAV Ad-hoc Networks (UAANET)) then concluded that the best communication architecture is UAANET.

### 1.2. Problem Statement

UAVs technology provides many benefits. However, several vulnerabilities are associated with these advantages. Especially vulnerabilities that complicate the security effectiveness. These security issues should be addressed properly, if not UAVs will be an easy target for attacks. Principally, the attacks on the charging system are fatal. Based on that, the UAVs-based system require high security to prevent malicious attacks that lead to fatal failures. Indeed, battery depletion attacks are a noteworthy constraint that could impede the system performance and go as far as to crush the aerial vehicle. Depletion attacks drain the battery power while the UAVs mostly need a good charging state. The power system is linked to all UAV composites, especially the motors to provide relevant energy to lift. UAVs motors need elevated capacity batteries to provide long-time operations. Also, UAVs cannot intuitively be overloaded with large batteries. This fact constrains the potential and reflects the need for regular recharging and battery replacement. Additionally, the battery power depends on the weight factor to stretch the flight time [21], e.g., heavy Quadcopter with 3.7v 1800mAH battery maximum flight time is between 16 and 17 minutes. Thus, the trick of affecting the charging system and depleting the battery is ideal for attackers. The goal is to reduce the flight time or completely damage it by crashing. Therefore, it is important to enhance the system security to prevent these kinds of attacks due to the importance of the battery. A study [22] analysed the battery life that covers the needs of UAVs operations such as wireless communications. The authors reported the limited energy of UAVs affects performance. They proposed real-time decisions taken on board and analysed them later to reduce the consumed power. Most studies [7] [23] [24] [25] [26] [27] [28] [29] [30] on UAVs vulnerabilities and attacks focus on a single problem. Either Charging problems or battery depletion or also general system attacks. Few works proposed deep investigations regarding cyber-attacks on UAVs-based systems or UAVs charging system taxonomies.

### 1.3. Contributions and Paper Organisation

To the best of our knowledge, this is the first survey that proposes a full divergent study on UAVs architecture basis and open security issues. The innovation keys of this work are:

1. covering UAVs attacks on the base-system and the charging system.
2. expanding a study on UAVs battery depletion attacks.
3. presenting different mitigation approaches against the charging system attacks and battery depletion attacks.

Since this work is addressing specifically UAVs security issues, the contributions are as follows:

- We highlight recent intending UAVs based system attacks and UAVs charging system attacks.
- We propose a taxonomy related to vulnerabilities, threats and attacks on the UAVs based system.
We propose a taxonomy related to vulnerabilities, threats and attacks prohibiting the UAVs charging system.

We analyse attacks that exhaust UAVs energy and battery depletion attacks.

We focus on the mitigation and countermeasures against cyber-attacks in UAVs charging systems and battery depletion mitigations.

Finally, we outline the recent solutions and mitigations related to UAVs based systems and charging systems.

The rest of the paper structure comprises 10 other sections. Section 2 discusses the related works that analysed UAVs attacks. Section 3 presents the methodology of the paper. A brief background on different UAVs architectures in section 4. Thereafter, UAVs security issues are briefly explained in section 5 including UAVs based system and charging system issues. In section 6, a taxonomy on UAVs based system attacks is proposed. In section 7, another taxonomy on UAVs charging systems attacks is presented and analysed. Section 8 provides mitigations and solutions for UAVs battery depletion attacks and UAVs charging system attacks mitigations. Also, issues and future directions are introduced in section 9. Finally, Section 10 concludes the survey. Figure 4 highlights the survey road map.

1.4. List of Acronyms

The Table 1 presents the used list of acronyms along this paper.

2. Related Works: Recent Surveys and Studies Assessing UAVs Attacks

The most important goal to researchers is empowering UAVs security cracks. They aim to prevent attackers from having access to control the drone and damage it. UAVs have different attacks, such as data interception, data manipulation, denial of services, hijacking attacks, and data fabrication. Accordingly, these concerns are grouped into three security properties: availability, integrity, and confidentiality. To overwhelm this gap of security, researchers analysed different UAVs attacks. Within the current section,
we present these existing studies. To fulfill the standards, critical studies concerning UAVs attacks are mentioned below, and this survey classifies them based on four criteria:

1. **Proposed taxonomies** for different UAVs attacks.
2. **Cyber-attacks** threatening the UAVs based system.
3. **Wireless charging system** attacks against UAVs.
4. **Battery depletion and exhaust energy** attacks that targets UAVs.

Many studies on the wireless Internet of Things (IoT) charging systems attacks are increasingly important. UAVs are a subset of the wireless IoT systems, and discharging the device is a relevant stealthy target attack.
However, in certain extensive wireless ad hoc networks, major studies [31] focused on energy efficiency. Therefore, the energy efficiency optimization problem is defined in terms of throughput performance and resource allocation fairness. One of the major concerns of energy efficiency for UAVs is battery depletion. In [32], authors presented battery depletion attacks that target UAVs energy resources. The authors provided defense strategies that could decrease the attack degree of damage. They provided an experimental attack analysis on a quadcopter UAV called “Parrot AR Drone” to explore its security levels. In [22], the authors studied different UAV limits and focused on the issues of energy efficiency in UAVs. For that, they revealed the need for sufficient energy for communication. It represents approximately 20% of the overall energy capacity of UAVs. Still, the network is much lower than the energy used by the UAV to lift and for the motors. Also, the study summarised various threats and issues that limit the power of UAVs, like the extra payloads. In addition, an evaluation of UAVs energy exhaustion is studied in [33]. The paper analysed UAVs power problems in the charging system. The authors evaluated the power gap and provided a comprehensive study on energy management strategies. Moreover, their corresponding threats have also been considered.

UAVs have typical power supplying methods such as battery tethered, swapping, and laser-beam in-flight recharging. Swapping is a method of powering the UAVs depleted battery while on the mission. Hot-swapping is a methodology for swapping a depleted battery with a rechargeable battery while managing to keep the UAV power active. Therefore, this operation could reactivate the battery and resume its functionality. Different security, reliability, and privacy concerns increase the likelihood of recurrent cyber-attacks, which are defined and discussed in [34]. The study provided a methodology for securing the multiple aspects of UAVs. The authors evaluated current cryptographic and non-cryptographic alternatives for UAVs systems. In addition, the review describes the safety of the UAVs by proposing a taxonomy that exposes the risks, the vulnerabilities, and the privacy threats that could be physical, location-based, or behavior privacy related. Based on the wide spectrum of services, we must assume UAV security to be the main priority. In this context, [35] evaluated several types of cyber-attacks such as MitM, spoofing as well as fooling denial of service attacks. The authors focus on the energy exhausting and battery-depleting attacks. In particular, power depletion attacks on UAVs could absorb excessive energy. Every category of battery depletion attack has its sustainability and ruggedness.

Furthermore, they give some countermeasures via an introduction to wireless charging and models that approximate energy distribution and power generation. Paper [36] identified UAVs vulnerabilities in the system itself or the communication system. They exploited attack types such as malware, communication attacks, jamming, and spoofing. The author proposed methodologies that explicitly address how military UAVs can be hijacked and misused by recent attacks and terrorist activities.

In [37], the authors analyzed UAVs attacks that could damage the communication. To improve the efficiency of UAV communication, Software Defined Network (SDN) [38], and Network Functions Virtualization (NFV) are used to facilitate flexible deployment and management.
<table>
<thead>
<tr>
<th>Ref/Year</th>
<th>Studied Points</th>
<th>Strength</th>
<th>Weakness</th>
<th>Proposed Taxonomy</th>
<th>Proposed Attack</th>
<th>Attacks Based System</th>
<th>Charging System Attacks</th>
<th>Battery Depletion Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>[34] / 2020</td>
<td>A review on UAVs attacks. They study attacks some types based on their classes Provide some countermeasures for UAVs cyber-attacks</td>
<td>+ Work on UAVs safety and security against various threats + Analyse few UAVs vulnerabilities and attacks.</td>
<td>- limited studied cyber-attacks already solved</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[35] / 2020</td>
<td>Identifies UAVs cyber-attacks including battery depletion attacks</td>
<td>+ Battery depletion attacks on UAVs are examined + Provide a full scheme on energy exhausting attacks</td>
<td>- Address limited forms of battery depletion attack - Only a few types of cyber-attacks are assessed</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[36] / 2020</td>
<td>Present preliminary study on UAVs. Analyze the global scenario of military attacks and malware detection UAVs attacks</td>
<td>+ Review some attacks and their classifications + Present several defense techniques against UAVs cyber-attacks</td>
<td>- Limited few attacks that touch some limited points - The only target suggested is military attacks</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[37] / 2020</td>
<td>Discussed the complexity of network privacy concerns in SDN and NFV-based UAV systems. Propose a taxonomy on UAVs communication channel attacks</td>
<td>+ Highlights the attacks on UAVs based on softwarized networks + Provide countermeasures for some attacks based on blockchain</td>
<td>- Focus only on communication networks threats - Only few attacks is studied</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[22] / 2019</td>
<td>A study on UAVs security attacks Analyse the vulnerabilities against UAVs based system attacks Analyse the vulnerabilities against UAVs charging systems.</td>
<td>+ Present open challenges for UAVs and their future insight + Pay attention to UAVs charging challenges and their management</td>
<td>- Do not solve the vulnerabilities of UAV and their problems of the charging system - A general study that does not give importance to lethal attacks on the charging system - The challenges of UAVs security and their issues in this paper are far from being up to date information</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[33] / 2019</td>
<td>Present a comprehensive review about UAVs charging system and battery power resources and their management Present an overview of batteries, the technique to supply them, and optimize the energy management and the charging system</td>
<td>+ Provide energy management strategies + Optimise the charging system + Solutions for battery depletion</td>
<td>- The attack itself is not clarified. - The scope of the issue is not studied - Does not lay out the ground of the attack and the consequences. - Security issues are not considered</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[32] / 2016</td>
<td>Different vulnerabilities, cyber-attack techniques, and security strategies are explored Provide some solutions to protect UAVs system against cyber-attacks.</td>
<td>+ Review hacking strategies that compromise based-system attacks + Adopt various techniques that support the defense against cyber-attacks + Provide a trustful system security</td>
<td>- Only few attacks of UAVs were not highlighted - A general overview that does not focus on UAVs system vulnerabilities</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>This paper/2021</td>
<td>The paper identifies different UAVs security attacks on the based and charging systems. Proposes two taxonomies and some solutions and countermeasures for both systems.</td>
<td>+ Review and analyse different types of attacks + Highlight the attack on the UAV-based systems and the charging systems. + Study the open issues and future directions.</td>
<td>N/A</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
They disassociate the UAV network control from the collected information and provide efficient communication. Any malicious attack on the central SDN controller can inflict massive devastation to the UAV network or integrate spyware into the system. The NFV operates as well for Virtual Machines (VMs), and the security issues they encounter are a combination of physical networking threats and VM systems attacks. It is valuable to acknowledge that battery depletion attacks on UAVs among all the UAVs charging attacks are currently poorly studied. There are extensive surveys that identify UAVs security issues and vulnerabilities against the base system, the charging system, and battery depletion attacks. To compare our study to others, Table 2 compares the major reviews based on the studied points, their advantages, and their weaknesses. This paper presents a study on UAVs vulnerabilities and attacks such as battery depletion attacks. In addition, we evaluate these classes of attacks and the corresponding protection mechanisms. Among the work’s standout aspects there are:

- UAVs topology and the charging functionality.
- Security concerns the based system, the charging system, and the battery.
- Attacks on UAVs-based systems.
- Attacks on UAVs charging systems.
- Attacks that exhaust the energy and deplete UAVs Battery.

3. Research Methodology

To properly serve the actual literature in the field, this section provides a methodology based on a systematic literature technique to mark certain research questions. The methodology used in this study focuses on the existing attacks on UAVs that prevent them from charging and deplete their batteries.

3.1. Research Materials and Selection Method

This research improves the understanding of UAVs security issues by looking over and reviewing previous research in the field. A total of 169 papers were analysed to propose a comprehensive understanding of the existing studies. Relevant data were taken from papers published during the period 2016–2021. The selection methodology is illustrated in Figure 5 that represents the number. Figure 6 shows the considered scientific papers within the scope of this survey. These supreme papers are taken from scientific databases. The
Table 3
Inclusion and Exclusion Criteria of the Study

<table>
<thead>
<tr>
<th>Inclusion Criteria</th>
<th>Exclusion Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>+ Studies published in English language</td>
<td>- Studies published in other languages.</td>
</tr>
<tr>
<td>+ Studies published starting from 2016</td>
<td>- Duplicated papers</td>
</tr>
<tr>
<td>+ Studies in the context of vulnerabilities, threats, and attacks on UAVs</td>
<td>- Studies outside the context of UAVs security concerns.</td>
</tr>
<tr>
<td>+ Studies available in scientific engines and research databases</td>
<td></td>
</tr>
<tr>
<td>+ Reviewed surveys, conference proceeding, and books chapters.</td>
<td></td>
</tr>
<tr>
<td>+ Directions of UAVs security.</td>
<td></td>
</tr>
</tbody>
</table>

The following research sequence is specified after defining relative alternatives and essential keywords, which are: (“Unmanned Aerial Vehicles” OR “UAVs” OR “Drones”) AND (“Security” OR “Vulnerabilities” OR “Attacks” OR “Threats”) AND (“Wireless Charging” OR “Battery Depletion” OR “Energy Exhausting”). According to the paper goals, clear research analytical questions (AQ) are defined to be answered in most survey sections. Therefore, the paper hands over inclusive answers to the following posed AQ in the context of UAVs security to facilitate the understanding of the study:

(AQ1): What are the main UAVs vulnerabilities and security concerns?
(AQ2): What are the attacks and the threats that target UAV-based systems?
(AQ3): Which are the attacks that target UAVs charging systems?
(AQ4): What are the attacks that deplete UAVs battery?
(AQ5): What are the defensive measures against UAVs-charging system attacks?
(AQ6): What are the defensive measures against UAVs battery depletion?
(AQ7): What are the future Research directions and the open perspectives for securing UAVs-based systems?

After clearing the analytical questions, we collected various papers that analyse the UAVs security issues based on the fixed keywords and similar alternatives.

3.2. Findings to research Analytical Question

The key findings of assessed and analysed 119 studies are chronologically sorted and analysed. Our methodology is based on two main steps before analysing data which are:
(i) Papers Collection based on inclusion and exclusion criteria.
(ii) Data Collection

3.2.1. Papers Collection Based on Inclusion and Exclusion Criteria

The collection of papers began with identifying the search strings. Also, they need to satisfy specific conditions to be more objective, as mentioned in Table 3. The table indicates the merged inclusion and exclusion criteria. Three exclusion criteria and six inclusion criteria were defined. Furthermore, they must respect the filtering criteria.

3.2.2. Data Collection

For the papers that correlate with the filtering phases, PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) [39], and the included criteria. Specific data that can be used are collected to answer each AQ listed previously in subsection 3.1. Based on that, the findings of each research question
AQ1: What are the main UAVs vulnerabilities and security concerns?
The data of interest are the detailed studies that gave us a hand to determine the main security concerns. It represents the collected reviews or surveys that identify the most common threats and vulnerabilities in most instances.

(AQ2): What are the attacks and the threats that target UAV-based systems?
The data of interest are the studies that analysed the attacks of the UAVs-based system. These attacks were collected from the papers that study the system attacks from all vectors, specifically from reviews or surveys.

(AQ3): Which are the attacks that target UAVs charging systems?
The interest data are collected from papers that study the charging system attacks from various surfaces and their offenses on the system. They should be distinguished from the rest of the base-system attacks.

(AQ4): What are the attacks that deplete UAVs battery?
The data of interest are collected from surveys and experimental studies enumerated and discussed. They should be identified based on keywords such as battery depletion, energy exhaustion, battery degradation, and other security threats and attacks.

(AQ5): What are the defensive measures against UAVs-charging system attacks?
The data of interest are the summarized solutions for the mentioned research question AQ3. The data are collected from experimental, theoretical, and practical solutions.

(AQ6): What are the defensive measures against UAVs battery depletion?
The data of interest are the mitigations and countermeasures against battery depletion attacks mentioned in AQ4. The collected data are the most related features that the solutions intend to provide.

(AQ7): What are future research directions and open perspectives for securing UAVs-based systems?
The data of interest are several approaches proposed for securing UAV-based systems. These data are collected from the new challenges for research.

The data collected was processed through qualitative research techniques and refined quantitatively. More specifically, the data were analysed using PRISMA as previously reported. Few analyses were conducted to extend an inline study to set objectives and AQScted.

3.3. Literature Analysis
Based on the related survey study, 114 papers were identified to answer the AQs and analyse the literature. Table 5 summarises the filtering phases and describes the criteria. The search is divided into two phases:

(Phase 1): we choose the major papers from bibliographic databases related to UAVs security issues in general. These criteria are based on the title, the abstract, the keywords, the similarities, and the chosen year of the recently published papers.

(Phase 2): filtering manually with hand-operated iterations to check whether the selected papers satisfy the inclusion criteria in the paper contribution related to the field.

We followed these steps to record the process to identify the included papers. Web of Science (WoS), Scopus, Google Scholar, IEEE, and Science Direct were operated as search engines using the preferred reporting items as mentioned in Figure 6. There are four stages involved and schematized in Figure 7. These stages show the flow of the selection procedure. Thus, the primer search database (S1) results in an initial number of surveys and conference papers equal to 165. Then, we apply the filtering first phase
Table 4
The Interest Level of The Relative Surveys and Conference Papers to The Required Analytical Questions

<table>
<thead>
<tr>
<th>AQs</th>
<th>Related Papers</th>
<th>Motivation</th>
</tr>
</thead>
<tbody>
<tr>
<td>(AQ1)</td>
<td>[7] [23] [24] [25] [26] [27] [28] [29] [30] [6]</td>
<td>To investigate cases of attacks and potential threats to UAVs.</td>
</tr>
<tr>
<td>(AQ2)</td>
<td>[23] [24] [25] [26] [27] [28] [29]</td>
<td>To analyse the base systems vulnerabilities within with UAVs target.</td>
</tr>
<tr>
<td>(AQ3)</td>
<td>[29] [30] [40] [41] [42] [43] [44] [45] [46] [47]</td>
<td>To itemize the investigated attacks on the charging systems and their offences on the UAV.</td>
</tr>
<tr>
<td>(AQ4)</td>
<td>[7] [30] [40] [41] [42] [43] [44] [45] [48] [35]</td>
<td>To investigate attacks aimed at draining power and depleting the UAVs battery</td>
</tr>
<tr>
<td>(AQ5)</td>
<td>[49] [50] [46] [51] [52] [53]</td>
<td>to assess the Key solutions and recommendations that stands against the charging systems attacks</td>
</tr>
<tr>
<td>(AQ6)</td>
<td>[54] [55] [44] [41] [56]</td>
<td>To provide solutions published by researchers and developers against the mentioned attacks of battery depletion.</td>
</tr>
<tr>
<td>(AQ7)</td>
<td>[57] [53] [58] [59] [60] [61]</td>
<td>To explore the future potential of UAVs security concerns.</td>
</tr>
</tbody>
</table>

Table 5
Phases Used in the Search Papers Filtering

<table>
<thead>
<tr>
<th>Phases</th>
<th>Filtering Criteria Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(ph1)</td>
<td>IN title AND abstract: &quot;UAVs Security Issues&quot; OR &quot;UAVs Attacks&quot;, AND Keywords AND &quot;Year from 2016 to 2021&quot;</td>
</tr>
<tr>
<td>(ph2)</td>
<td>IN paper contribution: &quot;UAVs security attacks&quot; OR &quot;UAVs cyber-attacks&quot; OR &quot;UAVs System attacks&quot; OR &quot;UAVs sub-system attacks&quot;</td>
</tr>
</tbody>
</table>

(ph1) as described to obtain a mid-number of documents. We compare these stages with the PRISMA flow diagram, which comprises four stages: identification, screening, eligibility, and included. The first stage is identification. Subsequently, we remove the redundancy of the selected papers to have another resulting number of surveys and conference papers. This phase is known as the screening phase in PRISMA. The second filtering phase (phase 2) will be applied considering the relevant criteria of the paper contributions. Finally, we read the full text of the reviewed papers, commonly known by the eligibility phase in PRISMA to have a final number of 93 papers called the included documents in the equivalent procedure.

4. Background

The recent fusion of smart UAVs and IoT gave out a new terminology called the Internet of Drones (IoD) [62][63]. IoD is a devised architecture that has recently become imperative due to the emerging level of intelligence and security. They originate from getting IoT with drones instead of things and support the layered network control architecture. IoD has been addressed in a framework proposed by Lagkas et al. [64]. In general, UAVs can be designed based on many different architectures. Each architecture is used for a specific purpose. This section presents other UAVs based architectures and charging techniques.
4.1. UAVs Architectures

4.1.1. Mono-UAVs based Architectures

Mono-UAV [65] is a distinct node that interacts with a specific level of autonomy classified from Low to high. But the word mono does not mean that the UAV is solo performing on the network. Each mono-UAV communicates with the base station (BS) or with a satellite all the time. Mono-UAVs are deployed to accomplish operational missions and provide widespread system deployment, but that was insufficient due to flexibility. The standard form of operation for mono-UAV systems is assigned to the controller to provide real-time direct system management. Nevertheless, researchers presented mono-UAVs’ abilities and proposed studies to improve them.

In [66], the authors presented a study based on mono-UAVs to optimise its location at a fixed altitude and in other different altitude constraints. This solution is proposed to reduce the system outage likelihood. Besides that, this study showed that some operations do not require more than a mono-UAV to satisfy their requirements, like small space monitoring and bounded zones. Another novel study [67] used mono-UAVs to work on an approach that improves low-resolution image quality using deep learning-based methods. The goal is to enhance the precision of remotely sensed satellites and their cost-effectiveness. For wireless communication, mono-UAV is useful for a variety of cases. Within this context, [68] designed an optimized model for efficient communication. The author employed mono-UAV to improve the trajectory and consider propulsion energy consumption.

4.1.2. Multi-UAVs based Architectures

Previous studies [68] recommended using a group of UAVs rather than a mono-UAV. Meanwhile, other studies like [69] used both mono-UAVs and Multi-UAVs. The authors guarantee the usability of both structured Multi-UAVs and mono-UAVs. The effective cooperation of Multi-UAVs in harmony builds a powerful system. Although, they have more advantages compared to mono-UAVs, such as performance, better efficiency, and rapidity. Hence, Multi-UAVs are used in many applications like improving Quality of service (QoS), wide-area monitoring, disaster assistance, and data acquisition.

In this scope, [70] used Multi-UAVs for disaster management. Multi-UAVs have been linked with big data algorithms to make the right decisions. The goal of using Multi-UAVs is to analyse pre-defined lands and spaces. The study is made for a military case if violent encounters might trigger UAVs to be finally damaged or destroyed. [71] proposed a study to improve smart cities using Multi-UAVs. They were assigned to collect data from IoT devices with low transmit power using efficient communication. The communication between Multi-UAVs keeps them synchronized during the mission. If one of the UAVs crashes during the
Short Title of the Article

task, the mission continues with the safe group and cuts off the crashed UAV connection. There are diverse types of connections [72] usually used in Multi-UAVs. Multi-UAV communication is established between UAVs and between the UAVs and the ground station. These connection types are as follows:

1. **UAV-to-Ground (U2G)**: this connection allows the UAV to communicate directly with the ground station to send and/or receive the flight control and tasks data.
2. **UAV-to-UAV (U2U)**: this connection is established by linking UAVs far from the ground station. Then, the task data is chained from a UAV to another UAV.
3. **UAV-to-Infrastructure (U2I)**: this connection is made between UAVs and cellular networks.
4. **UAV-to-Sensors (U2S)**: this connection links between UAVs and sensors on the ground for data transmission.

Thus, Multi-UAVs architecture can effectively extend the communication range and transmit data across different network nodes. Usually, the network is based on ad-hoc architecture to overcome transmission bandwidth limitations. An important characteristic that differentiates UAV networks is the High mobility like flying ad hoc networks (FANETs), mobile ad hoc networks (MANETs), and vehicular ad hoc networks (VANETs). These networks have dynamically configured topologies such as star topology, multiple star topology, mesh, and hierarchical mesh. [73] proposed a significant design for Multi-UAVs wireless networks with an efficient and systematic trajectory. Compared to the usability of mono-UAV, this study proved the potential of using Multi-UAVs. The following standpoints are some of the advantages:

- **Coverage & Cost**: able to cover wider areas and perform tasks at a lower cost.
- **Time & Power**: accomplish the mission by doing many assignments in parallel with a mini system prototype that is power-constrained.
- **Scalability & Suitability**: the system is scalable and can easily scale operations to monitor large areas.
- **communication**: a particular UAV could communicate with the ground station and broadcast the message to the rest of the network nodes.

Multi-UAVs can be grouped based on the mission goals like cooperative multi-UAVs. The task starts with the first hovering UAV and the last UAV landing. When a group of UAVs is identified as a team or swarm, they move together without being constrained by collective behaviour. A swarm or fleet of UAVs operates collectively to accomplish tasks with a fully autonomous or semi-autonomous system. Each UAV in a swarm has an assigned data collection and query optimization resource. They are responsible for computing and accomplishing the task in real-time. The communication between a swarm is direct through broadcast and/or direct messages or sensing other UAVs in the environment via their movements and interactions. Swarm robotics has the intention as a noteworthy part of academic and industrial applications. They show three preferable characteristics in multi-UAVs: scalability, flexibility, and efficiency. However, all dynamic Multi-UAVs have constraints. For instance, some areas are physically unreachable, and the vehicle could not fly through them.

**4.2. UAVs Charging Architectures**

UAVs need to have a good charging architecture to accomplish their task to get a long-duration flight. There are two distinct solutions to prolong the flight time. The first solution is to increase the battery’s capacity, but it could be too massive to let the vehicle fly. Also, the substance of the battery could be expensive to be deployed, and this solution is not feasible. The alternative suggestion is to charge the battery from an external energy source continuously. This second solution is based on a wireless network system.
The Wireless feature gives the UAV sufficient flexibility. Consequently, by generating electricity via usable power sources, it is possible to use the same battery and increase the drone's lifespan. Wireless Power Transfer (WPT) is a potential substitute system to satisfy UAVs battery power requirements. WPT enables UAVs to fly for extended lapses and promotes autonomous flights with Highly-efficient powered batteries. Meanwhile, UAVs should be configured to charge themselves dynamically at scheduled times.

### 4.2.1. Wireless Charging System

The Wireless charging system comprises three modules: the battery, the alternator, and the voltage regulator. The alternator is an electrical generator responsible for converting mechanical energy to electrical energy. Two sides of the transmission control the wireless power system: the transmitter and receiver. Also, a few rounded wires are perfectly stabilized. While the UAVs rotate and fly over a specific distance and at a particular location. An aerial electromagnetic field will be created near the station. The UAV landing has no concern about the alignment of the transmitting and the receiving coils. Hence, the aerial vehicle is free to land on the station where the coils will calibrate automatically to transmit power. Also, the drone is equipped with a WPT that receives electronic circular twists (Rx). The WPT transmits circular twists (Tx) located on the ground station and is directly linked to the electric energy that feeds the system. Hence, the charging scenario requires efficient contact across UAVs and the charging source.

**Figure 8:** UAVs Different Power Sources

There are plenty of power-lines energy providers in urban and rural areas. These power lines represent a source of energy and charging suppliers for the flying UAVs during their mission. A brief study [74] introduces UAVs power supplying methods and power lines. The authors presented the photovoltaic cell installation operation. This method extends the drone’s flight time by setting up photovoltaic cells over the vehicle. These cells are connected directly to the battery storage system. Furthermore, there are various sources of power to charge UAVs (see Figure 8) such as:

- **WPT:** have many aspects of recharging the battery on-board successfully. First, the UAV battery should be supplied with adequate energy. Also, the WPT system itself should have good liberalism to coil misalignment. This requirement is to handle the landing phase. There are two methods used for WPT systems which are:
  1. Inductive Power Transfer (IPT).
2. Resonance Coupled Wireless Power Transfer (RC WPT).

- **Batteries**: have three main layers as depicted in Figure 9 the batteries have three layers which are the application layer, the battery management system (BMS), and the physical layer. The BMS controls the parameters like Dc supplier, voltage, temperature, state of charge, and physical condition. The battery cell is designed as a shifting voltage power called the variable-voltage power supply. This open-circuit voltage (VOC) is in series with an inner battery resistance (BR) that ends with battery voltage. The recent terminal voltage depends on the battery power (P) and battery parameters. However, batteries are chosen based on a specific size to fit the UAV. Based on the physical dimensions in the bottom-left of the vehicle. Sometimes, UAVs fall into insufficient battery capacity and need to reach a given charging station. Hence, their overall battery capacity and speed determine the optimum estimation to hit the charging station in question. UAVs battery capacity is also considered to ensure the endurance of UAVs. The commonly used market capacities have capabilities that balance between 5000 mAH and 16000 mAH. For normal UAVs batteries, the power is shrunk to 1000 mAH. The most rechargeable battery type used in UAVs is Lithium Polymer (LiPo). This type has a powerful energy density which delivers better power. Lithium-polymer batteries are provided with a capacity of 1500 mAh, which is a powerful characteristic, and a voltage of 11.1 V. There are other batteries like Nickel–Cadmium (Ni-Cd) Nickel-Metal Hybrid (NiMH) batteries. Each has its criteria, such as energy and power densities, discharging characteristics, temperature effects, efficiency, and endurance. Furthermore, battery voltage is a prime characteristic because it is not specified based on unified regulations.

- **Solar power**: is an off-grid energy system that consists of solar cells, a DC-DC transformer, a power storage system which is the UAV battery, and a load. To attain lifting durability, autonomous charging systems use solar power technology. [75] illustrates the scheme of the solar charging system as shown in Figure 10. The transmitter and the receiver in the wireless solar charging system consist of: (i) Direct current to current direct converters (DC-to-CD); (ii) Resonant capacitors; (iii) Resonant indicators; (iv) Receiving coil.

- **Tethered power**: is an operation made through a connection of tether between the UAV and the power station.

- **Laser beaming**: is used to transfer electrical energy to UAVs batteries from a mobile power source using a laser transmitter. UAVs are provided with a photovoltaic (PV) that charges the battery from the converted laser energy. At a particular moment during the mission, the UAVs battery needs to be recharged from a mobile charging station equipped with a wireless power transmitter to complete the task. Therefore, the laser beam will be redirected to the flying UAVs in a condensed circular loop.

- **Dynamic storing**: is an operation implemented based on the natural winds to charge the UAVs battery, and it is known with albatrosses described by the balanced fixed wings. This operation gets the velocity from energy sources surrounding the environment without discharging the battery.

- **Combustion engine**: is often used as a power supply for military and industrial UAVs [76].

In [77], the author presents a study on wireless techniques and their efficiency to charge UAVs using power lines aiming to create an effective battery charging technique for long-range applications.

A prototype of wireless charging for UAVs is proposed in [75]. The technique relies on a custom-designed charging point mounted on a transmission line. The authors worked on solving the problem of the
impaired starting ability. Using an autonomous PV-powered battery charger, the technique is proved based on RC WPT theories.

In addition, [78] proposed an advanced charging system for UAVs and applied it on a quadcopter. The system is controlled by the energy transmitter and receiver, and the voltage control unit. This proposed system is composed of:

1. Multi-transmitting coils that can have four degrees of freedom and could move in four-way directions in positive and negative directions of x-axis and y-axis.
2. Motors along the two sides that supply the transmitting coils to adapt with the wireless communication system.
3. Battery charging station formed using a board on the two-axis to shift the transmitting coils. Accordingly, the centroid of the transmitting coil is lined up with the centroid of the receiving coil of the UAV.

Eventually, [79] proposed a new system for UAVs wireless power transfer with different amplifications over the configuration. The designed approach deploys magnetic resonance to transmit energy from the initial power source. It loads energy without triggering a direct electrical connection. Thus, this improved power transfer system gets a high-quality coil and solves the low coefficient coupling variation with coil misalignment.

These improved WPT systems raised the charging process’s efficiency and performance.

4.2.2. Wireless Charging Process

UAVs charging process is standardized to establish a completely autonomous system. Whenever a UAV battery reaches a low level and parks, a manual interaction changes the battery or connects the charging settings. Therefore, designing a charging area for UAVs dynamic landing is a reasonable solution to the conflict. The charging procedure leans on converting power-line high voltage energy to UAVs battery needs with low voltage. This power-line perching approaches supply power based on links transmission.

Solar cells generate power, then hold it in battery storage and send it to UAVs on demand. A loading portion is provided by linking the adapter to a wireless battery charging board. [75] Described the autonomous solar charging pipeline as follows:
1. Turning solar energy into electrical energy and storing it in a battery.
2. The reverse alternating current (AC) field transforms the DC power.
3. The transmitting coil generates an alternating electromagnetic current.
4. The receiving coils are connected to the transmitted alternating electromagnetic field.
5. The wireless system battery will be charged through the transformer unit.

The energy demand for UAVs is often not a predictable approximation. Therefore, the needs vary depending on many influences. The authors in [80] studied swarm UAVs energy swapping based on a fixed optimal algorithm that illustrates the best scenario (see Figure 11). The model is composed of:

- An UAV marked as a buyer.
- Charging station marked as a seller energy node.

The drone exchanges information with the station and forms tangles through the running phase. This forms a direct contact between the UAVs and the charging station without any middleware.

The charging process will be launched based on the UAV demands to have IOTA tokens for energy. IOTA is a distributed ledger of the basic blockchain built for IoT and used to record and execute transactions. The charging stations and UAVs are connected as nodes inside the IOTA network. IOTA has reliable security to store transactions of the tangled information issued by the UAVs and the charging stations based on an optimized algorithm.

The station identifies the UAV or the requested node with an ID that holds public and private keys with access to various charging wallet addresses. Then, the power will be exchanged between the two nodes with prior knowledge of the UAVs address and the needs.

This transaction is secured with hashed signatures that correlate with previous transactions. In [81], a novel charging system model for Multi-UAVs is proposed. The authors studied the storage of the charging station and UAVs. The flying distance is taken into consideration to schedule the optimal charging process. We conclude that a good charging system improves the simplicity and flexibility of the entire UAV propulsion system.
5. UAVs Security Issues

Awarded by the current technological advances, UAVs perform vital, complex, and sophisticated tasks. For this reason, they face many security issues, which makes them exposed to devastating attacks. Other attacks are launched to control the UAV or disable it. The consequences are relational to the type of attack. Few tools could be used as a hacking tool [36]. Researchers started to enhance the security of UAVs as part of the IoT environment. Generally, it requires an effective establishment of diverse methods related to different IoT areas of connectivity and deployment. In this section, we highlight UAVs security and privacy issues and UAVs attacks. This section introduces UAVs-based system attacks and UAVs charging system attacks. We also highlight the motivations behind this study for UAVs battery depletion attacks. The preceding mentioned research studies for the following subsections identify various concerns and issues in UAVs. These research works assessed different attack types, as well as multiple consequences. Table 6 attempts to compare these scientific studies based on the studied points (security concerns, attacks against UAVs systems, charging system attacks, and battery depletion attacks).

5.1. UAVs Security Concerns

While coping with any digital system, security is the most concern. It is mandatory to ensure the security of the UAV system. UAV systems are sensitive to cyber-attacks and function degradation, which directly affect the central contributor. Thus, attacks or faults in the system lead to severe issues. Different security issues are highlighted in [23]. The attacker in such cases, interferes with the integrity, availability, and confidentiality of the drone. The leakage of confidential data makes it relatively easy for an attacker to determine the UAV confidential data [82]. In addition, the authors in [7] proved the sensitivity of UAVs networks against attacks and sensor vulnerabilities. The attackers could access the UAV communication links to connect and control the UAV. In this context, [24] criticized several types of attacks and classified them into two main sectors based on UAVs targeted components and the attack vector. Vector attacks are separated into physical attacks or remote attacks. Based on that, there are various consequences of security issues, e.g., a swarm of UAVs were disabled during attacks mounted toward Russia’s Hmeimim airbase in 2019 [83]. 13 offensive fixed-wing UAVs targeted the airbase itself. It has been spread over a wide range of locations like Latakia Governorate, near Latakia in Hmeimim, and Syria with a range of 250 km. Nevertheless, the existing vulnerabilities give the potential to attackers to become more sophisticated and active.

5.2. Attacks on UAVs-based Systems

UAVs systems are similar to other existing IoT systems. They rely on a centralized server, data storage, and wireless communication connectivity. If the system is assaulted, the UAV mission will be interrupted, a security weakness. The prime objective of UAV-based system attacks is to manipulate stored data or to crash the system. There are many cyber-attacks on UAVs based systems, such as:

---

### Table 6

| Studied Points                  | [7] | [23] | [24] | [25] | [26] | [27] | [28] | [29] | [30] | [40] | [41] | [42] | [43] | [44] | [45] | [48] | This Paper |
|-------------------------------|-----|------|------|------|------|------|------|------|------|------|------|------|------|------|------|------|
| Security Concerns             | ✓   | ✓    | ✓    | ✓    | ✓    | ✓    | ✓    | ✓    | ✓    | ✓    | ✓    | ✓    | ✓    | ✓    | ✓    | ✓    |
| Attacks against UAVs          | ✓   | ✓    | ✓    | ✓    | ✓    | ✓    | ✓    | ✓    | ✓    | ✓    | ✓    | ✓    | ✓    | ✓    | ✓    | ✓    |
| Charging Systems              | ✓   | ✓    | ✓    | ✓    | ✓    | ✓    | ✓    | ✓    |
| Battery Depletion Attacks     | ✓   | ✓    | ✓    | ✓    | ✓    | ✓    | ✓    | ✓    | ✓    | ✓    |

---
• **Jamming attack**: [25] [26] [41] [27] [36] [24] [84] are the second most common attack with three related identified types of jamming: GPS Jamming, Control Stream Jamming, and Data Stream Jamming. The attackers hunt and deliver signals that conflict with Radio Frequency (RF) signals in the same frequency band as the targeted drone. The attack is established via nodes based on a wireless channel model for range-based localization. The jammer is equipped with an omnidirectional antenna. This antenna will transmit RF signals radiated equally in azimuthal directions. In [85], a study shows that using specific transmitters to intercept remote control signals is not always secure, even though the jammer is much closer to the UAV than the operator with the remote controller. There is a declared GPS Jamming attack on the 10th of May 2012 in South Korea done by an unknown person during testing [24]. The attack crashed a rotor based on an Austrian UAV “Schiebel Camcopter S-100” with the ground control station and wounded two remote pilots.

• **Spoofing attack**: [37] [86] [87] is comparable to jamming attack but more refined. Rather than interfering with signals, the attacker will produce erroneous signals randomly controlled that counterfeit and falsify the GPS location. Therefore, these fake signals will change the drone behavior by guiding to another location that differs from the main scheduled path. It ends with binding the victim with fake latitude and longitude data. The operation is transparently achieved without interrupting the actual GPS operation. In [88], a study of a spoofing attack was demonstrated using a customized spoofing device that transmits a generated perfect replica of GPS signals to the victim. Hence the GPS receiver will be confused choosing the real and the fake signals. The authors in [89] conducted launching a spoofing attack on a DJI Matrice 100 quadcopter [8] and spoofing data have been successfully ended and collected spoofing data.

• **Data Interception attack**: [34] Intercept Data attacks are a violation of confidentiality that can result in extensive consequences to the drone. The attack enables unauthorized attackers to access data under an illegal file viewer during the interactions, during flight, or at rest. In [24], data interception attack was identified by the American military defense in Iraq who found the stolen data under video form on the apprehended laptop of an activist. Based on that information, the video has been taken by the unsecured communication links between the flying UAVs using SkyGrabber. Hence, data interception attacks will be executed when using an over-accessible non-secure wireless transmission. This type of attack is hard to detect.

• **KeyLogging attack**: [90] [87] is a type of monitoring software modeled to capture keystrokes and steal data. KeyLogging malicious software has emerged as tracking spyware that shares the resources with the legitimate software. In [6], a keylogging attack against US Predator was identified at Creech Air Force Base in Nevada. After linking Predator and Reaper ground control stations to a removable hard drive, it was launched. Thus, confidential information will be captured and transmitted.

• **MSG Injection attack**: [25] [34] is known as an integrity attack which could be carried by remote access. Injecting a malicious payload is the procedure of inoculating legitimate pseudo messages. The messages are supported by an identical structure of the legitimate message. They deflect both the UAV and the GS system with another fake UAV. Based on this, message deletion and message modification are using the same injection process. Hence, injecting malware such as viruses, worms, and Trojans will alter sensitive information. UAVs are defended by specific system tools such as StackGuard and StackOFFence [91]. The First tool is an automatic adaptive detection and prevention technique and the second one is a technique to mitigate such attacks.

• **Eavesdropping attack**: [59] [27] [25] [90] is a passive attack on the UAV confidentiality that acts silently. It is interpreted as an unauthorized real-time interception through the communication chan-
nels. A malicious vehicle listens to the communications between the UAV entities without affecting the network transmission. This attack captures confidential data without disrupting the valid receiver’s signal quality. Hence, eavesdropping violates network privacy. According to [6], eavesdropping is considered a type of man-in-the-middle attack. Differently, the attacker establishes an independent network connected with the victim and relays messages as if they are communicating with a legitimate person.

- **Distributed denial of service (DDoS) attack**: [59] [91] [44] [90] [25] is a common direct attack on the availability of the UAV during the mission by sending excessive requests. The attacker can transmit erroneous data in continuous requests through data links. Thus, the increased network traffic will overflow the communication channel, which will block the connection.

- **Sybil attack**: [92] occurs whenever an attacker generates multiple dissimilar nodes in the network using two types, stolen and fabricated identities. This action will augment the opportunity to enable a malicious intercepting routing message and control the Peer to Peer (P2P) overlay network. The attacker can attain an excessive level of authority and influence data integrity, energy consumption, and entire system performance via threats.

- **Blackhole attack**: [93] [29] is defined as a denial of service attack and classified as lethal attacks. A Malicious node attracts all data packets via falsely reporting to obtain a sustainable path to the destination node. The source node delivers data packets to the black hole rather than to the ending node. The routing protocol will be quite disturbed by deceiving the nodes about routing data. Hence, while transferring data through the black hole, the attacker will access these packets. The attacker promotes many falsified pathways trying to attract data traffic. This particular attack is used to introduce a directed pull attack and completely change routing data.

- **Grey hole attack**: [28] could shift from an authentic to sinkhole attitude. A similar concept for the grey hole is launched where the malicious nodes interrupt network data transfer by broadcasting false routing information. For that, it is an extension of the black hole attack. However, the node could operate in two states, as malicious or as a normal node.

- **Fake information dissemination (FID) attack**: [25] happens whenever the intruder transmits a fake GPS signal to shift the direction of the UAV and get data by imitating. FID attack is carried by an intruder that produces falsified authentication messages obtained as lawful routing packets from malware devices. The routing table of nodes will be destroyed by the false injection of the malicious node. In consequence, the nodes will lose the packets through a routing error. In addition, the packet delivery rate will be decreased.

- **Replay attack**: [34] [59] is a DoS-like attack that intercepts valid data transmission or slows it down to resend an altered data instead without decrypting the captured message.

These aforementioned attacks are pinpointed based on the studied works in Tables 7 and 8. Some attacks such as eavesdropping, keylogging, and especially Sybil attacks can potentially destroy data availability across the entire system.

### 5.3. Attacks on the UAVs-charging Systems

UAVs charging system [30] [94] is a related embedded mechanism of power. The UAV charging system is vulnerable to attacks that could end the life of the entire UAV. These types of issues can stop the UAV functionality. Recently, researchers have been aiming to empower the UAV charging system security. Author in, [40] designed a model with an assessment of energy demands. The model will accurately predict the
drone demands based on the legitimate task energy usage. Accordingly, this model will be aware of attacks, limiting the charging system vulnerability.

Many features significantly impact the charging system performance, like temperature and actual discharge rate. That will affect the resistance of the battery and the power supply. Moreover, different attack scenarios pose a risk in this typical system. In addition, voltage regulation faults [43] may cause many issues to UAVs charging systems. This vulnerability leads to overcharging or undercharging. Also, it causes a decrease in battery life and damages the contributing unit. In [41], the UAV was a target for an attack where the attacker generated falsified requests which damaged the charging system. It caused an issue of excessive energy and excessive drop of voltage. This could be accomplished by meddling with the charger control unit or manipulating data sources. For instance, [41] identified different charging system prospect issues such as the improper operation of the WPT. Also, in [42], the authors analyses the attacks that manipulate the charging process. When the UAV connects to a fast-charging station, the malicious software overwrites the charger software. The attack will turn the UAVs into fast chargers till damaging the charging system. This bad power attack is silent and fast without any reaction or alert. It can shift the configuration and add extra effort till causing damage to the entire system. Consequently, any UAV mounted or connected to the charging station will generate a menace.

5.4. Attacks related Depleting UAVs Battery

Depletion of Battery (DoB) [35] is a specific attack that could target the UAVs and cause extra usage of power at various levels. Hence, it makes failure difficult to predict but when it occurs, the damage could not be recovered because it is complicated. According to the original communication, If an unexpected decrease in remaining battery capacity was detected between follow-up visits, accelerated depletion could be detected. As a result, these kinds of attacks are the most common causes of mission failures and may potentially cause loss of the connection and possibly a crash. Some sensors will crash during the attack in addition to some functionalities which will degrade until shutting down. DoB exhibits a higher likelihood of an electrical component failure causing a fast battery depletion.

UAVs are especially vulnerable to DoB attacks because they exploit their autonomy, physical movements in the environment, wire and wireless communication channels, or all of them simultaneously. Through DoB, the attacker can expose the target UAV’s software/hardware computational modules, the physical construction and data. DoB attacks are analogous to energy deprivation [45] and DoS attacks. DoS attacks accelerate battery depletion up to 18.5% [45]. In addition, Denial of Sleep (DoS) [44] is a similar attack that shares the same goal. It is based on minimizing the UAV sleep mode to maximize the power consumption till depleting the battery. Moreover, the attacker uses cross-layer attacks [44] indirectly to deplete the UAV battery by changing the charging parameter. However, there are two forms of battery depletion attacks:

- **Attacks without physical contact:** this first form includes attacks that do not require physical interaction with the device. They are wireless channel attacks. These recent attacks are composed of two-channel categories of energy crisis control systems. They are the GPS data transfer channel and the control data transfer channel. GPS data transfer is used to determine where the UAV is located geographically. Therefore, the attacker targets the GPS channel and interferes using an Omni antenna. The attack aims to block out the signals of the receiving side or deliver them with false coordinates. Also, making incoherent movements when the UAV receives various instructions makes the battery more consuming. The second channel synchronizes instructions with the UAV, such as GPS data, network parameters, and UAV global status.

- **Attacks with physical contact:** This type is launched while the UAV is in standby mode. Based on this, the attack is started from many entries like physical constituent, USB interface, and microcircuit.
Also, by connecting a physically excessive weight to imbalance the UAV, the intruder will force the UAV main rotors to run at maximum strength and use more charge. [47] made an experimental study to evaluate the weight factor on UAVs power consumption. The first of two UAVs used in the experimental setup with 30 Kg of total weight and 8 Motors, and the second is with additional payloads to get up to 35 Kg of weight with the same number of motors. The movement sets of lifting, hovering, and landing power usage for each test were noted. The power consumption is based on the Rotation Speed (RPM). This study shows that the values increased for each movement in the second test.

In addition, based on [56], UAV DoS attacks can happen in two ways:

- By delivering fake communication packets, the attacker sends requests constantly. As a result, the UAV will use a portion of extra energy for the authentication process to analyze each request, draining the battery.

- By Generating Electromagnetic (EM) noise to cause high error rates at the UAV. That will increase the energy consumption due to the increased number of re-transmissions. The UAV may be forced to raise transmission power due to the increased noise, which affects battery life.

There are various threats to deplete UAVs battery such as overcharging to boil the battery, draining, leaking, illegal configuration, and exhausting the energy. Also, many factors cause energy depletion. For instance, works in [40] [48] evaluate the effects of these factors like payload, movement, hovering, communication, and speed in energy exhaustion.

Finally, unless the vehicle’s battery is completely depleted during the flight, it may not have sufficient time to return to the base and complete its task effectively. Thus, the infrastructure’s logistic operations may be significantly disrupted.

6. Attacks Assessments of UAVs-based Systems

In this section, a taxonomy of UAV-based systems attacks is proposed. These attacks are classified in Table 9 based on four categories:

1. Attacks on the base software
2. Attacks on the sensors
3. Attacks on the communication channels
4. Attacks on the GPS channel.

6.1. Proposed Taxonomy

Most UAVs attack types are classified based on the attacker type, the offences, and the goals of the attack. Accordingly, an attack chain is modeled in Figure 12. The modeled chain illustrates the sequence of UAVs-based System attacks. The attack process is composed of four main parts. An attacker with a relative purpose, attack vector to specify the attack entry. Then, it reaches a predefined attack depth. Finally, the impact or the damages carried by the attack. This sequence supports the proposed taxonomy (see Figure 13). The taxonomy summaries all the attack forms on the UAVs-based system. Each strike has a set of behavior parameters realized to attack one or more layers. Particularly, the attacker could exploit one or more vectors to perform more attacks.
### Table 7
Summarize of Some Works with Their Different Attack Studies on the UAVs-Based System

<table>
<thead>
<tr>
<th>Ref</th>
<th>Attack Type</th>
<th>Attack Nature</th>
<th>Target</th>
<th>Main Concept</th>
<th>Influence</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Privacy</td>
<td>Confidentiality</td>
<td>Integrity</td>
</tr>
<tr>
<td>[37] [86] [87] [88]</td>
<td>Spoofing</td>
<td>Authentication</td>
<td>X</td>
<td>X</td>
<td>✓</td>
</tr>
<tr>
<td>[24] [25] [26] [27]</td>
<td>Jamming</td>
<td>Authentication</td>
<td>X</td>
<td>X</td>
<td>✓</td>
</tr>
<tr>
<td>[7] [24] [25]</td>
<td>Deauthentication</td>
<td>Authentication</td>
<td>X</td>
<td>X</td>
<td>✓</td>
</tr>
<tr>
<td>[23] [24] [25]</td>
<td>Man in the Middle</td>
<td>Authentication</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>[34] [25]</td>
<td>Fabrication</td>
<td>Exploitation and Authentication</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
</tr>
<tr>
<td>[24] [25] [26] [34]</td>
<td>Data Interception</td>
<td>Interception</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
</tr>
<tr>
<td>[6] [14]</td>
<td>Data Manipulation</td>
<td>Exploitation</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
</tr>
<tr>
<td>[9] [37]</td>
<td>KeyLogging Attack</td>
<td>Interception</td>
<td>X</td>
<td>✓</td>
<td>X</td>
</tr>
<tr>
<td>Ref</td>
<td>Attack Type</td>
<td>Attack Target</td>
<td>Main Concept</td>
<td>Influence</td>
<td></td>
</tr>
<tr>
<td>-----</td>
<td>-------------</td>
<td>---------------</td>
<td>--------------</td>
<td>-----------</td>
<td></td>
</tr>
<tr>
<td></td>
<td>MSG (Code) Injection</td>
<td>Exploitation</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
</tr>
<tr>
<td>[23][14]</td>
<td>Eavesdropping</td>
<td>Interception</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
</tr>
<tr>
<td>[27][39][25][6]</td>
<td>Denial of Services Authentication</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>✓</td>
</tr>
<tr>
<td>[14][59]</td>
<td>Replay</td>
<td>Exploitation</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>[28][92][39]</td>
<td>Sybil</td>
<td>Authentication</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>[28][93][38]</td>
<td>Wormhole Infection</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>[28][90][99]</td>
<td>Authentication</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>✓</td>
</tr>
<tr>
<td>[28][91]</td>
<td>Gray hole Infection</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>✓</td>
</tr>
<tr>
<td>[28]</td>
<td>Fake information dissemination Infection</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>[24][67]</td>
<td>Zero-Day</td>
<td>Authentication</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
Table 9
Related Papers Studied Categories of Vulnerabilities in Attacks

<table>
<thead>
<tr>
<th>Targeted Entity</th>
<th>[28]</th>
<th>[14]</th>
<th>[37]</th>
<th>[86]</th>
<th>[87]</th>
<th>[88]</th>
<th>[89]</th>
<th>[25]</th>
<th>[26]</th>
<th>[41]</th>
<th>[27]</th>
<th>[36]</th>
<th>[24]</th>
<th>[84]</th>
<th>[85]</th>
<th>[90]</th>
<th>[9]</th>
<th>[6]</th>
<th>[44]</th>
<th>[100]</th>
<th>[101]</th>
<th>[87]</th>
<th>[102]</th>
<th>[96]</th>
<th>Our Taxonomy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base Software</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Sensors</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Communication</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Channels</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>GPS Channel</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

Figure 12: UAVs Based-System Attack Chain of the Proposed Taxonomy

These attacks are grouped based on the previous chain and reply to the following purpose questions:

- **Attacker**: Who is the attacker?
- **Attack Vector**: How is it triggered? On which surface it has logged in? What is the threat? Is it a direct attack or with a remote auxiliary? What are the attacked entities of the UAV?
- **Attack Depth**: What is the nature of the attack? Are there any specialized attacks?
- **Attack Offences**: What are the vulnerabilities that were attacked? What are the consequences of the attack?

More formally, every taxonomy dimension is defined as follows:

- **Attacker**: an attack is made by different individuals or groups such as terrorists, spies, thieves, and hacktivists for other goals in different areas of attacks and positions. In [34], researchers studied various attacker cases for UAVs for terrorist airstrikes, hijackers, and spying. Also, the paper revealed UAV thieves as the recent attack of theft of a US RQ-170 Sentinel by Iranian forces [103]. As an intelligent attack, a SkyGrabber [37] software system was used for hacking UAVs. Various UAVs hijacking software such as SkyJack engineered to hack and manipulate the UAV wirelessly using an autonomous middleware. Moreover, the term "Terror by Joystick" [104] into the path of the airliner reveals the malicious attacks on UAVs by terrorists. Hence, thieves are a threat worth trying to use UAVs to wreak havoc.

- **Attack Vector**: attacks are launched through different vectors like being a direct attack or a remote using medium entries. Remote attacks intercept with an auxiliary to be affected by suspicious methods through external tools. These auxiliaries are the control software, the sensors, the communication channels, and the GPS channel. These four are the main used targets for attackers. The attacked
entities are the surface, or the element targeted by an attack. This element resides in the based system of the physical vehicle. UAVs interact with the physical environment. As a result, it could be either an integral component or a cyber or physical environment.

- **Attack Depth:** these threats are measured by their nature, which could be one of four specialized attacks. The adversary is targeting the UAV for intelligence purposes: malware infection, exploitation for gathering information or anything familiar, interception for cracking, and authentication. Cybersecurity threats might exploit data to achieve the attack goals without operator knowledge. Various
attacks could be grouped by exploitation nature like injection, and modification [6]. As well, one of the standard listed authentication attacks is fabrication [34]. This last attack is prey for the UAV authenticity that permits the attacker to obtain privileged access to the components to supply them by fabricating false information. For specialized attacks, there are distinct types to change the content or influence the decision-making of the UAV.

- **Attack Offences**: Consequently, their data will be stolen, modified, and corrupted. Other offences are obtained from these attacks as Data Theft, an authentication offence for cracking and stealing, and fuzzing where attackers use fuzzing to find zero-day exploits. Hence, they could cause system fuzzing by disturbing the process, the communication, and the functionalities.

Therefore, UAVs-based system attacks could sneak through various means using a planned entry and fixed damage to leave.

### 6.2. Software-based Attacks

UAVs-based software is the processing of data for a decision-making system [6]. It is responsible for connecting the components and controlling the sensors, navigation, and communications protocols. Essentially, the base software is responsible for setting the flight parameters [105]. These elements are vulnerable to attacks. Hence, there are no strict security measures in the drone base software that prevent malicious programs from modifying the data. There are many software’s used for attacks, such as the buffer overflow [106]. It is software for UAVs operating system attacks. The attacker locates memory blocks to fill them with additional data to waste the allocated space for data. This will force the system to run random codes allowing the control and monitoring of these systems. Also, other advanced attacks on the base software could extract sensitive data. For instance, Structured Query Language Injection or SQL injection attack for data-driven.

Furthermore, some attackers choose to launch the attack on the embedded Software Defined Radio (SDR) [107] boards due to their easy access and low security.

Eventually, base Software security issues are continually maintained due to micro-controller system failures with appropriate authentication and authorization review.

### 6.3. Attacks on the Sensors

There are different sensors [108] in the drone that carries data and provide measurements. For this reason, sensors are considered as a target for attackers. They are using them as the surface of attack to intercept from them. These attacks are altering the transmitted data to these sensors.

In [109], the intruders crafted an attack through sensors and called it a "sensor input spoofing attack.” This demonstrated the effectiveness of attacks against UAVs through the sensors. Also, Nichols et al. [100] described in a way the attacker transmits false data through an onboard sensor to confuse the drone. In addition, in [44] the attacker physically tampers with the UAV sensors to disable the availability and then launches a DDOS attack. However, there are no reported attacks on sensors directly as a linked camera to UAV [24]. But Studies like [6] [101] secured the sensor to secure the transmission of data in the network.

### 6.4. Attacks the Communication Protocols

Generally, UAVs and GCS communicate via different communication protocols [97]. The major communication protocols are Micro Air Vehicle Link (MAVLink) protocol [110] [111], UranusLink [102], and UAVCAN [112]. These protocols have several vulnerabilities with many failures as followings:

- **MAVLink**: a marshaling library designed to establish lightweight message serialization protocol. It is the most popular among its peers. There is a remarkable lack of this protocol with structured references apart from the basic concepts. Although there exist some threats, it has no mechanism to
guarantee the reliability of the delivered messages. In addition, the messages dissemination security is weak. Therefore, it needs security enhancement over the end-to-end communication between GCS and UAVs.

- **UranusLink**: is a packet-oriented protocol that yields unreliable and reliable services. This protocol is dissimilar to the existing protocols that interact with UAVs. It includes the checksum to check the transmission of the original message and if it was received. But it could not check whether the message was modified or not. As a result, A simple checksum does not guarantee data confidentiality or integrity. However, there is a deficiency of sufficient experimental evidence for UranusLink.

- **UAVCAN**: is an open-source protocol based on CAN bus for controller area network. It is meant to ensure secure communication over robust vehicle networks. It is not recommended for sensitive missions or the system since the protocol provides no shielding.

### 6.5. Attacks on the GPS Channel

Wireless attacks are executed through GPS channels such as GPS Jamming and Spoofing. These two recent attacks are computer emulators [95]. There are ranges of jammers [96]. First, the simple constant jammer transmits a continuous jamming signal with standard power. Also, another simple regular jammer but with high power transmission sent out with packets. The constant transmission could be deceptive with normal and high capacity. In the second place, the random jammer only transmits intermittently. Both valuations of high power and normal power are misleading. Besides, the reactive jammer is described by the complex jammer the signal will be sent when the transmission target is defined and sensed. Also, the intelligent jammer with the pre-knowledge of the used leverage protocols and modulation. In conclusion, GPS channels security is essential for the UAVs to accomplish the mission.

### 7. Attacks Assessments against UAVs Charging Systems

Currently, only a few studies are heading towards UAVs charging systems security. A study in [35] highlights three attacks on the charging system. The first is done by sending empty requests to the UAV. These requests are regularly rejected. The sent packet could have no core data or a fake authorization request. The second might be performed by transmitting a request to execute worthless operations. Finally, the third attack consists of running a query to adjust the UAV software/hardware settings. In this section, UAVs charging system vulnerabilities and attacks are analysed based on the UAVs’ different sets. In accordance with the attacks on the UAVs charging system, a taxonomy is suggested and discussed below.

#### 7.1. Proposed Taxonomy

Imposing requirements on UAVs charging system security is essential. In Figure 14, we illustrate several types of attacks on the UAVs charging systems that could occur on the separate phases of the UAV status. These phases are classified as follows:

- **On Movement phases**: the attacker could launch the attack during the main three phases of UAV movements of lifting, hovering, and landing. There is a suspected vulnerability while hovering where attackers could replace batteries at the power supply. In another situation, the attacker can replace the UAV battery or tamper with the charging system before discharging it.

- **The Technical phases**: the attacker could perform the attack while the UAV is on standing before performing its tasks. Also, when it starts, the movement phases or when it is completely off in the base. Recently, the attacker could infect the charging system before the UAV launches its mission.
• **The Charging status**: the attacker has two possibilities, either to launch the attack through the charging system connection while charging or when it is off charge. In the last case, we talk about a long-term attack.

These phases allow the attackers to perform malicious actions on the UAV charging system. Hence, UAVs’ charging system is exposed to kinetic and non-kinetic attacks. We propose a taxonomy on these attacks in Figure 15 with an abstract illustration in Figure 16 which are defined as follows:

- **Attack Layer**: typically, most attacks start with a target layer. The attacker finds the perfect surface to intercept with available vulnerabilities. Then, when the layer is chosen, he implements a tool or software to launch the attack. The main attack vectors of the charging systems are the physical layer, the BMS layer, and the application layer. The possible attacks surfaces for the last two layers are software and hardware. In addition, attacks on the application layer come from the network channels or sensors. But for the physical layer, the attack could be performed either by swapping or tampering. As long as these layers are cascaded and inter-connected, the attacker can attain more compound attacks than simple ones.

- **Attack Features**: like generic security attacks, a charging system attack requires several pre-conditions to be launched successfully. Attacks generate intentional offenses on the charging system, which are discharged by deep or draining discharge. Also, another feature is the over/undersupplying of the charging system.

- **Attack Offences**: The two main results are intentional and unintentional. The first takes the primary goal to damage the charging system or discharge the drone. Additionally, the unintentional attack offence aims to disturb the process. This is done using many techniques like blocking the communication channel, the loss of communication, and control. Hence, the application layer is susceptible to security attacks on the all-inclusive system. Table 10 address each layer with the target challenges and the used techniques of attacks with the results.
- **Attack Impact Duration**: the deployment of charging attacks requires changes to the existing system infrastructure, which takes a long time to achieve the main goal. Some attacks like Code Injection, data modification, and manipulation are long-term attacks [113]. Hence, attacks affect the overall charging system or one of its layers in a short duration.

### Figure 15: UAVs Charging System Attacks Taxonomy

#### 7.2. Attacks on the System Application Layer

Attacks via the application layer are broadly classified into three classes based on the CIA triad of confidentiality, integrity, and availability of the critical operation within the system. The CIA triad on the application layer are as follows:

- **Application Layer Confidentiality Attacks**: are the assaults on the charging system that aims to transmit illegal data over all the charging system.

- **Application Layer Integrity Attacks**: conscious actions to corrupt or interrupt UAVs battery performance or information exchanged by data networks, BMS, and the system.

- **Application Layer Availability Attacks**: are DoS attacks on the charging system that aim to interrupt the service availability of the charging system.
Table 10
Overview of Charging System attacks on Charging Layers and Challenges

<table>
<thead>
<tr>
<th>Layer</th>
<th>Target</th>
<th>Technique of Attack</th>
<th>Offences</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Application Layer</td>
<td>✓ ✓ ✓ ✓</td>
<td>- Software authority is a common technique to control the charging system.</td>
<td>Gain access to the system and leverage negatively the logic process.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Direct and indirect attacks with a medium.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Simple attacks on sensors.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Complex attacks based on multi-entries such as software and hardware.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Potential to fatigue, jam, and damage the overall system by the power of control.</td>
<td></td>
</tr>
<tr>
<td>Battery Management System Layer</td>
<td>X ✓ ✓ ✓</td>
<td>- Direct and indirect control attacks on BMS.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Simple attacks on sensors.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Complex attacks based on multi-entries such as software and hardware.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Breaking down security regulations and requirements.</td>
<td></td>
</tr>
<tr>
<td>Physical Layer</td>
<td>X ✓ ✓ ✓</td>
<td>- Counterfeiting attacks.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Swapping and Tampering attacks</td>
<td></td>
</tr>
</tbody>
</table>

Attacks on integrity and confidentiality typically occur in applications, sensors, and communication channels. The main objective of these attacks is to access and modify vital information illegally by leveraging the charging system. The security of the application layer ought to integrate various features to mitigate static and dynamic attacks. In [44], there are two categories of attacks on the application layer, which are:

1. **Static attacks**: consist of the authentication attacks that aim to damage the charging system parameters and applications by executing malicious code or installing operations.
2. **Dynamic attacks**: they set out code injection or malware execution. Therefore, the system security must detect this instant unplanned behavior in operations’ logic process, such as power consumption and communication patterns.

Alternatively, such scenarios with highly gradual loss will put the battery in a dangerous state.
7.3. Attacks on the Battery Management System Layer

The BMS manages the charging system, and it is sensitive to attacks. Some attacks can shorten their lifetime. Hence, the security in this layer will ensure the availability and safety of the charging system. This structural hardware and software safety layer could influence the physical system layer, system parameters, safety control, charging process control, battery equalization by the balancing module, and data. Accordingly, malicious hardware trojans could manipulate the circuitry to influence the behavior of the BMS logic. For availability attacks, the malicious software and code injection will cascade even control the behavior of the charging system. Also, the Attacker could have the authority for influencing the BMS functionalities to command more wise attacks. Another type is the tampering attack on the BMS software [114]. This could occur during the system integration so the attacker can log in and take access to the BMS firmware. DoS attacks are more ferocious and more complex at a higher level of vulnerability. They aim to surreptitiously fabricate or obtain information exchanged between the UAV and the BMS.

7.4. Attacks on the Physical Layer

The attacks at this level are threatening the charging systems. The effects of attacks such as supplying, counterfeit, or others could affect the system’s availability, integrity, and authenticity. This is attributable to a deficiency of security technology in the physical layer, as well as the hardware and the processing methods used to interface the forgery [44]. Also, tampering attacks could occur at this level to cause the overall charging system failures. The authorization is ensured at the physical layer, and then the power charge is delivered to the rest [46]. The attackers launch authentication attacks on the external and internal charging systems. These attacks could be performed together or individually. Also, the attacker may physically tamper with the microcontroller or sensors to disrupt the battery module’s availability and reliability. Furthermore, the attacker could drain the battery and perform a DoS attack once the communication between the sensors and the microcontroller is affected. Hence, the performance and security of the charging system will be threatened in most scenarios.

8. Mitigation and Countermeasures against UAVs Charging System Attacks & Battery Depletion Attacks

After analyzing UAVs security attacks and their damage, this section provides guidelines for mitigating actions and countermeasures against UAVs charging systems and battery depletion attacks.

8.1. Mitigation and Countermeasures against UAVs Battery Depletion Attacks

Researchers proposed some solutions for the problems posed by the UAV battery depletion attacks like:

- **Power Prediction and Analysis:** [54] to avoid the depletion of power resources, the authors proposed a system for energy consumption prediction and analysis. The system considers all the scheduled tasks and the needed energy to perform an efficient mission. The developed model called “a mission-based black box” aimed to predict energy consumption. The experimental results show that it is 98.773% accurate with the tasks beginning from the takeoff until the launch command returns. In [55], the authors focus on reducing the impact of the limited flight caused by battery vulnerabilities. They proposed a battery optimization model deploying an enhanced energy consumption scheme based on empirical studies of battery performance.

- **Dynamic Control Power:** [115] is an energy-aware method used to shift the majority amount of energy into less constrained operators. This dynamic method will set and control the transmission of power nodes.
• **Battery Counterfeit Countermeasure**: the solution has been proposed in [35]. The author’s solution is to strengthen the protocol’s security and enforce specific network security policies. Also, they proposed to use encryption methods to protect the integrity and authenticity.

Owing to the novelty of this attack, there are not many flexible security solutions. The majority of mitigations are limited. But, since UAVs are an emerging form of flying IoT devices [116], various solutions proposed for IoT battery depletion attacks will be compatible and convenient on UAVs. There appear to be limited studies on UAV battery depletion attacks in the literature. Still, there are solutions for battery depletion that have been approved in IoT and electric vehicles in [117] [118] [119]. Accordingly, [118] proposed a model based on a detection algorithm called the cumulative sums method (CUSUM). The model will evaluate the energy consumption while the battery is under attack to analyse the excessive transmission of power. The method assumes that the battery depletion attack will result in unexpected changes in the process compared to the power consumption in the normal case.

### 8.2. Mitigations and Countermeasures against UAVs Charging Systems Attacks

The attacks against UAVs charging systems extend the need for countermeasures to prevent them. [52] proposed a probabilistic model checking scheme for attack modeling. This model helps to study attacks such as DDoS attacks and malware. Also, the model provides the probability of success. To enhance data security, the authors suggested the deployment of digital signatures. The authors aim to extend the study to other several types of attacks. In addition, they proposed using an electromagnetic sensor in a designed model to enhance the regulation abuse. A group of engineers at Southwest Research Institute (SwRI) [49] [50] proceeded three manipulations upon the charging system to enhance the system against the attacks. They recommended a study on limiting the charging rate, blocking battery charging, and blocking the overcharging. Besides that, Pazos-Revilla et al. [46] reviewed the security and privacy scheme against the attacks considered in the charging system and, more precisely, in the physical layer. They used a feature for privacy that amends the powerful effects of jamming and/or eavesdropping attacks-based authorization schemes. For the recent attacks presented in section 7, there is a various logical countermeasure to apply, such:

- **Attack on the controller module countermeasures**: to detect these attacks, the controller should analyze the network from malware and also check the power consumption statistics.

- **Bereave energy resources via USB countermeasures**: the prevention method is visually controlled and applies techniques for the physical security of the hardware interfaces and entries. The same solution has been proposed for oversupplying attacks.

- **Unauthorized weighing and movements attacks countermeasures**: the proposed solution for this problem is to check the control channels and interfere with the immunity of the UAV navigation.

Therefore, securing UAV nodes from various attacks requires rapid, timely techniques, counter-mechanisms, and easily updatable methodologies to counterfeit deleterious offenses. In [60], researchers proposed a novel computation offloading scheme. The existing schemes of UAVs data transmission do not consider real-time limitations. This scheme considers the real-time qualifications and decreases UAVs power consumption in large areas’ monitoring. Also, researchers in [58] designed an energy-saving algorithm proposed for solar-powered wireless sensor networks. The authors aim to avoid charging conflicts and improve drone security against depletion attacks. Hence, the simulation of the designed algorithm shows a significant reduction in power consumption. Authors in [61] developed a flexible energy-designed model for a quadcopter. The model attributes the life-cycle and energy influence with payloads on systems. The study concluded that UAVs consume less energy for each packet and presented other charging systems solutions and future directions to counter-UAVs.
9. Open Issues and Future Directions

In this section, we analyze future directions on UAVs vulnerabilities. Future research is frontally directed across the amplification of wireless charging system security against threats and attacks such as jamming attacks, spoofing attacks, safety attacks, and software attacks [53]. In this context, Attorney General William Barr of the U.S emitted orientations to Justice Department agencies on defensive UAVs countermeasures. These orientations comprise the devastation of all sources of threats to national security [57]. Different open issues need to be addressed before achieving the UAVs paradigm’s successful functionality. These available issues pave the way for future researchers to further investigate UAVs security.

A - Effective UAVs Attack Detection Techniques

For UAV security deployment, efficient intrusion and attack detection strategies are essential. Novel models of attack measures are deployed to UAV security. Consequently, researchers should take advantage of this potential. The latter establish more intelligent and powerful faults, attack detection, and mitigation methods, to solve this crucial problem.

C - Artificial Intelligence Based Security Techniques

Many novel design attacks against UAVs have been performed. As a solution, Artificial Intelligence based on mitigating techniques is demanded. The adoption of artificial neural networks, deep learning, and machine learning techniques improves the security and privacy of UAV-based systems and UAVs charging systems. However, integrating artificial intelligence-based techniques in UAVs poses significant complications. Therefore, further research into selecting the suitable deep learning or machine learning method for specific UAVs security requirements is also essential.

E - Lack of Dynamic Power Load Balancing

There is an overhead in the charging system performance, and they lead to many issues such as power exhaustion, battery degradation, and performance degradation. As a result, the demand for efficient charging systems becomes a primary challenge.

F - Survivability and Battery Life

UAVs battery capacity and lifetime operation are limited. Therefore, fitting the power should be improved to ensure survivability and starvation conditions. It is a critical issue that needs improvement to extend the UAV lifetime.

10. CONCLUSION

Their increased usage has compounded the considerable gap in security concerns for UAVs. This work presented various vulnerabilities and attacks that threaten the UAV-based system and UAV charging systems. Moreover, battery depletion attacks are covered. Based on this, we propose two nomenclature and taxonomies on UAVs attacks assessments on their based systems and charging systems. Furthermore, mitigations and countermeasures against UAVs charging systems and battery depletion attacks are suggested. Finally, the paper highlights UAVs open issues and their future challenges.

References


[42] Catalin Cimpanu. Badpower attack corrupts fast chargers to melt or set your device on fire. 2020.


[49] Southwest Research Institute. Southwest research institute, advanced science of applied technology published by the official southwest research institute in https://www.swri.org/.

[50] Cate Lawrence and Florian Richert. What’s holding back electric vehicle charging security?, cate lawrence and florian richert published in 2021, 2021.


TASS. Russia’s hmeymim airbase in syria strikes over 100 terrorists’ drones over past two years, published by tass in 27-08-2019, 2019.


[108] MilSource. 4 military sensor technologies drones transporting commercial market published by milsource.


[116] Lori Cameron. Drones as the new “flying iot”: They’ll track people and deliver goods using a new low-power architecture to juice the apps while staying aloft, published by lori cameron in 2020, 2020.

