frontiers | Frontiers in Communications and Networks

TYPE Review
PUBLISHED 28 February 2025
DOI 10.3389/frcmn.2025.1443592

OPEN ACCESS

EDITED BY
Kuo-Hui Yeh,
National Yang Ming Chiao Tung University, Taiwan

REVIEWED BY
Dharminder Chaudhary,
Amrita School of Engineering, India
Ella Pereira,
Edge Hill University, United Kingdom

*CORRESPONDENCE
Sara Sumaidaa,
sara.awadh@tii.ae
Kyusuk Han,
kyusuk.han@tii.ae

RECEIVED 04 June 2024
ACCEPTED 06 February 2025
PUBLISHED 28 February 2025

CITATION
Sumaidaa S, AlMenhali H, Alazzani M and Han K (2025) Enhancing security of mobile crowd sensing in unmanned aerial vehicle ecosystems. *Front. Commun. Netw.* 6:1443592. doi: 10.3389/frcmn.2025.1443592

Enhancing security of mobile crowd sensing in unmanned aerial vehicle ecosystems

Sara Sumaidaa*, Hamda AlMenhali, Mohammed Alazzani and Kyusuk Han*

Secure System Research Center, Technology Innovation Institute, Abu Dhabi, United Arab Emirates

The rapid expansion of mobile devices with enhanced sensing and computing capabilities has driven the growth of mobile crowd sensing (MCS), enabling applications that collect large datasets from sources like smartphones and smartwatches. However, this data aggregation raises substantial security and privacy concerns, especially when MCS integrates with unmanned aerial vehicles (UAVs), where potential risks are further amplified. This study identifies and analyzes specific security and privacy threats in UAV-based MCS through the framework of the confidentiality, integrity, and availability (CIA) triad. We categorize potential vulnerabilities and propose comprehensive countermeasures targeting hardware, software, and communication models. Our findings outline strategic and actionable countermeasures to mitigate identified risks, thus ensuring data integrity and reliable functionality within MCS systems. Additionally, we present a security scenario involving mitigation suggested for data integrity and recovery. This work underscores the critical need for robust security frameworks in UAV-enhanced MCS applications, offering a holistic approach to mitigate emerging security threats.

KEYWORDS

crowd sensing, mobile crowd sensing, UAV, drone, security, threat analysis

1 Introduction

The sensing and computing capabilities of mobile devices have grown rapidly with the spontaneous advancement in information technology. Mobile devices such as smart phones, smart tags, body sensors, and in-vehicle sensing devices collect sensor data and share it to measure and monitor some phenomena of common interest. These capabilities in mobile devices are evolving the Internet of Things (IoT) as they provide sensing data to the Internet on a large scale. These devices are equipped with more diverse sensors and wireless connections that enable them to generate, collect, and share data across the Internet, which is called *mobile crowd sensing* (MCS), as addressed by Capponi et al. (2019).

The rapid developments in communication technology have also resulted in substantial breakthroughs in utilizing *unmanned aerial vehicles* (UAVs) for diverse applications within the MCS framework. As flying objects, UAVs are not limited to terrain. Any place can use them for any purpose, including civil applications in urban areas or military activities over battlefields. Researchers are particularly interested in the fundamental attributes of UAVs, such as their adaptability, mobility, and energy efficiency, which make them highly suitable for wireless networks. It is worth noting that combining MCS applications with UAVs significantly enhances the capabilities of MCS.

However, MCS could give rise to noteworthy privacy and security concerns because the data collected by MCS applications may contain sensitive personal information of participants. Sharing such sensor measurements with the larger community to measure or study events could potentially breach privacy if improperly used. Many researchers, including Abualigah et al. (2021), Owoh and Singh (2022), and Gharibi et al. (2016), reported that the main concerns in this context include authentication risks and the risk of identity, location, and flight route information being leaked. Moreover, MCS with UAVs could amplify noteworthy privacy and security concerns due to the lack of terrain restrictions and the constraints from the battery-powered environment of UAVs, in addition to the security and privacy issues in MCS.

Although many researchers have endeavored to identify threats in MCS applications and proposed the mitigation against privacy and security issues, as far as we know, there has yet to be a holistic approach to mitigate the overall system with a comprehensive analysis of potentially possible threats encompassing multiple perspectives, including software, hardware, and communication channels specific to MCS with UAV environments.

This paper seeks to tackle these pressing challenges by thoroughly examining the security issues present in UAV environments when implementing MCS applications. Our main objective is to identify potential threats and develop strategies to mitigate their impact. To accomplish this, we perform a comprehensive threat analysis, categorizing threats within the framework of confidentiality, integrity, and availability (CIA). Furthermore, we present a scenario centered on the retrieval of lost drones, highlighting the essential role of secure communication in facilitating effective recovery and rebuilding trust among UAVs.

1.1 Objective and contribution

This paper aims to validate a comprehensive threat modeling framework that addresses vulnerabilities associated with hardware, software, and secure communication within UAV ecosystems. By examining a practical scenario involving lost UAVs, we aim to highlight the critical need for targeted countermeasures that facilitate secure communication and restore trust among UAVs.

This paper presents a validated threat modeling framework that identifies significant vulnerabilities related to hardware, software, and secure communication in the context of MCS and UAV operations. It introduces a practical scenario in which UAVs conducting crowd-sensing missions face temporary communication loss, illustrating the consequences of the threat model and underscoring the necessity of the proposed countermeasures.

Additionally, it outlines specific measures for establishing secure communication with lost UAVs, including authentication processes, the utilization of device lists for trust assessment, and strategies for re-establishing communication based on reputation models. Our findings demonstrate effective methods for rebuilding trust between UAVs following disconnection events, detailing the essential steps for assessing the status of lost UAVs and evaluating their trustworthiness. Ultimately, this study lays the groundwork for future research into advanced security measures and protocols tailored to specific UAV applications, particularly in situations involving data recovery and operational integrity.

The outline of this paper is as follows: Section 2 provides an overview of mobile crowd sensing and UAV applications. Section 3 presents a literature review of the security issues in crowd-sensing-based platforms and UAVs. Section 4 highlights the threat modeling process aimed at enhancing drone security through the lens of confidentiality, integrity, and availability. Section 5 provides a summary of the primary countermeasures required as holistic approaches: system hardening, adopting hardware security, securing communication, lifecycle management, and adopting a cybersecurity framework. Section 6 examines practical scenarios concerning the management of trust in UAVs and their communication dynamics. Finally, Section 7 concludes the paper and discusses future directions.

2 Mobile crowd sensing-based platform overview

In this section, we provide an overview of MCS platforms and UAV ecosystems.

2.1 Mobile crowd-sensing environments

Smart devices such as smartphones, smart watches, smart tags, and body sensors are commonly used in our daily lives. For example, 14.4% of the world's population already uses a smart wristband device, and the market is predicted to grow at a compound annual growth rate (CAGR) of 15.6% between 2024 and 2032[1]. These devices consist of sensing capabilities to detect and collect data and communication capabilities to connect with other network-enabled devices.

As a result, a unique sensing paradigm known as *mobile crowd sensing* (MCS) has been sparked by the extensive capabilities of such mobile devices and networking technology. Capponi et al. (2019) are credited with pioneering the concept of MCS, and Guo et al. (2015) defined the concept as a platform enabling common individuals to gather and contribute sensed data that is subsequently aggregated and fused in the cloud to extract useful insights.

Yang et al. (2015) defined the system architecture as four entities: *service provider*, *end users*, *sensing crowd*, and *computing crowd*. The service provider's role is to accept the request from the end user, process this task within the sensing and computing crowd, and return the final result to the end user. The end users are the customers who send the requests and receive the results. Crowd sensing is diverse among users who participate in sensing tasks, which are collecting data from the end users and sending it to the server that stores that data or sends it back to the users as a result. Computing sensing has diverse users who participate in the

1 Rohit Shewale, Smartwatch Statistics 2024: Worldwide Market Data, 24 March 2024, demandsage, https://www.demandsage.com/smartwatch-statistics/

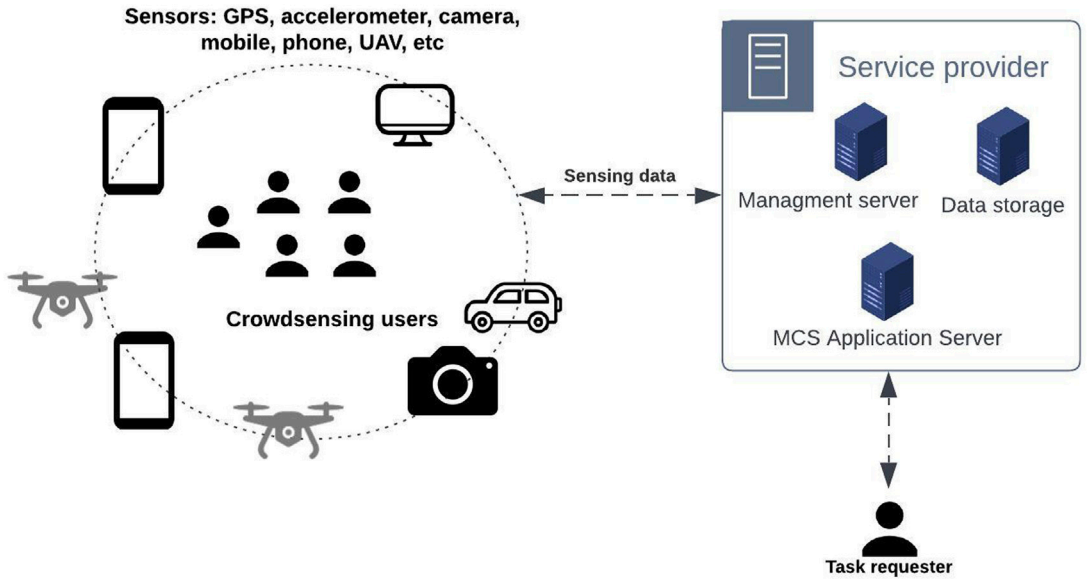

FIGURE 1
Model MCS system.

computing task, which is a task of collecting data from multiple sources and considering different computing device data as input.

Figure 1 illustrates the network of the MCS application. A typical MCS system consists of a *service provider*, a *task requester*, and a group of *mobile users* working together to make data gathering, aggregation, and analysis easier. The *task requester*, driven by specific data requirements and MCS system objectives, initiates and defines sensing tasks to be completed by mobile users. To maintain system functionality and meet the needs of task requesters, the *service provider* acts as an intermediary, overseeing and organizing communications between task requesters and mobile users. As data contributors, *mobile users* are essential because they use their smartphones or other devices with multiple sensors to gather and send data to the system.

The overall architecture of an MCS system includes user interaction, cloud or server processing, data analysis, sensing tasks, data gathering, communication infrastructure, data aggregation, and collaboration among mobile users. Each component is crucial for facilitating the collection and processing of large-scale data and generating insightful results for various applications, such as early warning systems, traffic anomaly detection, noise pollution monitoring, and air pollution monitoring. For example, the popular commercial application Waze gathers real-time traffic data through crowd sensing and serves as a traffic monitoring and route assistance system. A key component of MCS is encouraging mobile users to participate in sensing and providing the system with high-quality data. Thus, Suhag and Jha (2023) suggested models that allow users of mobile devices to donate data voluntarily or in exchange for rewards.

Fascista (2022) highlighted two large categories of transmission paradigms in MCS: *infrastructure-based transmission* and *opportunistic transmission*. Infrastructure-based transmission considers users accessing sensory data across a network, such as a 3G/4G connectivity. Opportunistic transmission, on the other hand, enables users to share and receive data through intermittent connections, such as radio wave and Bluetooth short-range communications.

2.2 Mobile crowd sensing with unmanned aerial vehicles

The increasing availability of UAVs has encouraged their widespread use for a variety of applications, including tracking, mapping, surveillance, and search and rescue missions, as reported by Pandey et al. (2022). UAV capabilities are advancing with new technologies, including software-defined networks (SDNs) and fog computing, which are essential for MCS applications for a variety of purposes. SDN is an approach that uses software-based controllers or APIs to direct network traffic and interact with the underlying hardware. Several researchers, including Boite et al. (2017) and McCoy and Rawat (2019), suggest that SDN could be essential for UAV environments due to its ability to provide centralized control and dynamic network management, which are crucial for adapting to rapidly changing conditions and large-scale deployments. SDN enhances scalability, allowing efficient handling of numerous UAVs, and optimizes resource utilization to ensure critical data receives the necessary bandwidth. It also bolsters security through centralized policy enforcement, ensures high quality of service (QoS) by prioritizing important traffic, and supports rapid deployment and reconfiguration in dynamic scenarios. Additionally, SDN improves cost efficiency by centralizing management and resource use, facilitates interoperability between diverse UAV systems, and enhances network resilience and reliability by enabling real-time monitoring and quick recovery from failures.

However, SDN faces several security risks. One issue is the reliance on a central controller, which creates a single point of failure from which attackers could control the entire network. Additionally,

vulnerabilities in the APIs between the controller and network devices can be exploited by attackers to inject harmful commands, intercept data, or disrupt communications. Furthermore, the lack of encryption in communications between the controller and devices allows attackers to intercept and manipulate data (Boite et al., 2017). Configuration errors can also happen because SDN's dynamic setup can lead to mistakes or weak security policies, creating vulnerabilities. Lastly, SDN controllers can be targeted by distributed denial-of-service (DDoS) attacks, which can overload the controller and cause network outages (Yassine et al., 2022).

3 Literature review

In this section, we review the literature on security and privacy issues and mitigation in MCS in Section 3.1 and in UAVs in Section 3.2.

3.1 Security and privacy challenges in mobile crowd sensing

Yang et al. (2015) addressed three main threats against the *privacy*, *reliability*, and *availability* of mobile crowd sensing.

The *privacy* threat is the leakage of privacy information such as the location, health monitoring data, and personal identities of the participants or the output result of the tasks. Hiding the participant identities or keeping participants anonymous are suggested to protect MCS against privacy threats.

The *reliability* threat can occur in two directions. First, the data sent to the end user could originate from a malicious participant to provide false information or impersonate the service provider. Ensuring that the data are from the true source requires identifying the sender. Second, someone could intercept the packets and alter the data during transmission. In MCS applications, encryption and authentication could be used to protect the integrity and confidentiality of outgoing data during transit.

Several types of attacks could lead to *availability* threats, including a denial-of-service (DoS) attack, where intruders participate in a task but do not send any data or results, thereby disrupting the service. Countermeasures could include authenticating participants before they join the task and implementing a system of rewards to encourage their loyalty. Additionally, continuous monitoring of the network for suspicious behavior and removing any suspicious entities was suggested to further protect against these threats.

Capponi et al. (2019) studied different types of MCS applications, classifying sensing applications into *personal* and *community* categories based on the phenomena measured. *Personal sensing applications* measure individual factors, such as movement patterns (*e.g.*, walking, exercising), while *community sensing applications* measure large-scale phenomena through numerous participants. Community sensing encompasses two primary models: participatory sensing, where users actively participate in data collection, and opportunistic sensing, which automatically gathers data based on location and application requirements without user involvement. Both models present unique challenges regarding data ownership and control. They addressed the fact that efficient scheduling and predicting energy and bandwidth needs under constraints are critical to protecting availability due to the varying capabilities of devices in MCS. They also suggested mitigation to protect the security and privacy of MCS needs while considering the resource constraints of devices. For example, they argued that cryptographic methods could use more energy than adding noise to the data.

Brahem et al. (2022) explored the privacy concerns associated with monitoring individual sensing instruments, tracking daily activities, recording habits, and assessing wellbeing. Privacy and trust mechanisms in MCS require a holistic approach that combines technical solutions with user behavior due to their complex environments. To address privacy concerns, the *personal data store* (PDS) is proposed as a secure repository for aggregating, storing, processing, and sharing individual data, as a unified data-sharing infrastructure supports seamless data exchange through mobile devices. A PDS could implement local data processing, filtering, and privacy-preserving techniques. Incentives may be necessary to encourage users to engage with a PDS and share their data.

Li et al. (2017) focused on security and privacy challenges in handling multimedia data in MCS, highlighting three main challenges: *data reliability*, *participant privacy*, and *inadvertent data*. *Data reliability* refers to the accuracy of the sensor data provided by the volunteer, where the participant might be exposed to some *malicious code* that could infect the whole sensing system. *Participant privacy* issues could occur because participants have no control over the application that is responsible for performing the sensing tasks where it collects, stores, and uploads data, and the volunteers are not fully aware of the data being collected from their devices. This issue would cause another issue called *inadvertent data*. As the participant has no explicit knowledge of who controls the application, some sensitive personal information might be disclosed inadvertently. For example, a pedestrian's face could be shown in an image that has been sensed by the application.

Thus, we could summarize that privacy, integrity, and availability are important issues in MCS, and addressing these issues must also consider resource constraints and complex environments.

3.2 Threats in unmanned aerial vehicles

As UAVs fly over public environments, communication over the wireless channel could be targeted by attackers to access, alter, or inject harmful data into communication streams. Bera et al. (2021) reported that the security challenges in UAVs are more difficult due to the resource constraint conditions. Because battery-powered UAVs may have lower processing power and storage capacity, deploying strong security countermeasures into UAVs is more difficult than in other environments.

He et al. (2018) analyzed the communication threats in UAV systems in terms of *confidentiality*, *integrity*, and *availability* perspectives. Unauthorized access to sensitive information in UAVs, ground stations, and communication links poses a major

threat to confidentiality. Security breaches can occur through attacks such as viruses, malware, trojans, and keyloggers, particularly targeting ground stations and compromising data integrity. Additionally, communication links face risks from password cracking, identity spoofing, cross-layer attacks, and multi-protocol attacks. Implementing strong encryption, strict access control measures, and regular security audits is suggested to address these threats and prevent unauthorized access and data breaches.

Threats to data integrity involve disrupting the accuracy and consistency of information through alterations or the creation of false data. Attackers may insert, delete, or modify critical information, undermining the integrity of UAV operations. Maintaining data integrity is vital for the reliability of UAV systems. To mitigate these threats, employing data integrity checks, digital signatures, and secure communication protocols is essential to ensure the authenticity and reliability of data transmitted and stored by UAVs.

Denial-of-service (DoS) attacks significantly threaten the availability of UAV systems by overwhelming them with false requests, causing network congestion and service disruption. Further risks include flooding attacks, buffer overflows, and smurfing attacks, which can disrupt UAV services. To mitigate these threats, robust network monitoring tools, intrusion detection systems, and firewalls should be utilized to detect and counteract DoS attacks. Additionally, implementing load-balancing techniques can help distribute traffic efficiently and maintain service availability.

GPS spoofing involves transmitting false GPS data to UAV receivers, leading to incorrect navigation and control. UAVs that rely on GPS signals are especially at risk from deception and interference, which can threaten flight safety. To counter GPS spoofing, strategies include using information fusion techniques that combine monocular sensors and inertial measurement units (IMUs) to detect spoofing. Additionally, using error reduction methods based on feature detection and matching can help UAVs return safely, reducing the impact of GPS spoofing attacks and ensuring safe operation.

Many researchers reported that ensuring robust encryption is critical for maintaining network integrity and confidentiality, and protecting controllers from such attacks is also essential for maintaining network availability. Various countermeasure approaches are being studied by researchers.

Boite et al. (2017) and McCoy and Rawat (2019) suggested that adopting a software-defined network (SDN) into the UAV ecosystem could enhance more optimal management and utilization; however, SDNs also encounter several vulnerabilities that cause serious damage to the operation of UAVs and their applications. For example, an SDN relies on centralized control, which could cause a single point of failure. Furthermore, configuration errors, such as the dynamic configuration capabilities of the SDN, can lead to misconfigurations or inadequate security policies, which in turn create exploitable vulnerabilities. API vulnerabilities could pose an additional serious threat. SDN controllers could also be targeted by distributed denial-of-service (DDoS) attacks, which can overwhelm the controller and lead to network outages. Furthermore, unsecured communications between the controller and devices can result in data being intercepted and manipulated by attackers.

Mohamed et al. (2020) explored the integration of unmanned aerial vehicles (UAVs) within smart cities, emphasizing their diverse applications, including environmental monitoring, traffic management, and public safety. Their article outlines the advantages of utilizing UAVs to improve resource efficiency, streamline city operations, and enhance citizen engagement. Furthermore, the paper tackles the challenges linked to this integration, such as safety, privacy, and regulatory concerns, while advocating for the establishment of strong regulatory frameworks and further research to support the effective deployment and incorporation of UAV technologies in urban settings.

4 Threats of mobile crowd sensing in UAV ecosystems

In this section, we show the comprehensive threat analysis in the context of MCS and UAVs. First, we demonstrate the environment with scenarios by presenting a proposed data flow diagram (DFD) in Section 4.1. Then, we discuss the identified threats in Section 4.2, providing a systematic evaluation of possible dangers and weaknesses that are inherent in MCS and UAV operations.

This sequential methodology enables a comprehensive and systematic study of security concerns within the context of MCS and UAV deployments. It promotes a holistic awareness of the system architecture and guides the subsequent identification and analysis of risks. In order to assess the comprehensive threat scenarios in UAV ecosystems, we performed the threat analysis from the perspectives of *confidentiality*, *integrity*, and *availability*.

4.1 Modeling data flow of MCS in UAV ecosystems

The UAV consists of internal hardware components and software to be the flight controller with sensing modules and wireless communication modules to use for the MCS application. The *ground control station* (GCS) consists of infrastructures to communicate with UAVs, to control UAVs, and to exchange data with UAVs. They are interconnected through different communication channels, including WiFi direct, Bluetooth, cellular, WiFi, or even a wired connection. Section 4.2 shows the threat analysis with the DFD of this scenario depicted in Figure 2.

The DFD includes two main entities: the UAV (E1) and the GCS (E2). The communications channels are defined below.

- Direct wireless communication between GCS and UAV, represented as the dashed line. (L1)
- Wireless communication through a third-party entity, that is, cellular or satellite communication, represented as the dashed line. (L2 & L3)
- Wired connection, represented as the continuous line. (L4, used for maintenance)
- Wireless through Bluetooth, represented as the dashed line. (L5)

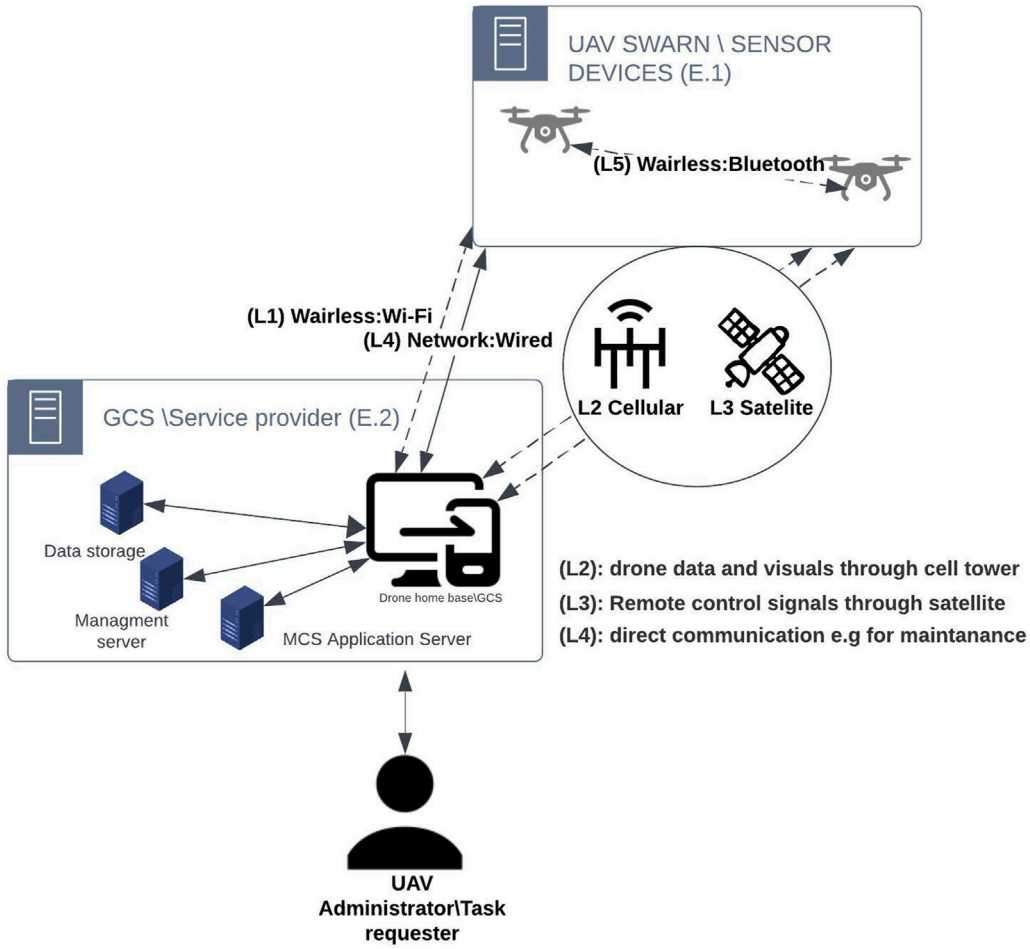

FIGURE 2
Data flow diagram (DFD) of the UAV ecosystem for mobile crowd sensing.

4.2 Threat analysis

This section is divided into three main subsections and examines the risks in the context of MCS and UAVs. This text outlines a variety of possible impacts that are naturally associated with these areas, specifically highlighting how they might compromise the integrity of a system, the confidentiality of data, and the availability of services. Based on the DFD, this analysis focuses on identifying potential dangers that may emerge during interfaces, interactions, and communication processes. Referring to Spyros (2022), we show comprehensive lists of threats in software, hardware, and communication fields below.

4.2.1 Hardware-related threats

Table 1 summarizes the hardware-related threats, indicated by threat ID T.H. Each threat is explained below, detailing the hardware vulnerabilities that cause security threats, how adversaries launch attacks, and the impacts and risks of these threats.

4.2.1.1 Tampering attack on physically captured UAVs

As UAVs operate in an unmanned state, a UAV can be physically captured by an adversary. Captured UAVs risk exposing sensitive data like secret keys, coordinates, a mission plan, and security measures to adversaries. This intersects with mobile crowd sensing (MCS), potentially compromising sensed data integrity (Pundir et al., 2019).

Physical tampering also includes the act of making alterations to the electrical hardware, such as modifying the hardware circuit or changing the logic gate (Vosatka, 2018). Specifically, the act of physically tampering with the flight controller exposes the UAV system to several forms of attack. The tampering is intentionally inserted by an untrusted third party in the semiconductor supply chain of the flight controller (Rahman et al., 2020). The opponent exploits these alterations to undermine the capabilities and security attributes of the flight controller's integrated circuit (IC) (for example, reducing the propellers' rotation speed or divulging the cryptographic keys of the flight controller). An instance of such manipulation was discovered in the Actel ProASIC chip of the Boeing 787 aircraft (Yuvaraj and Velliangiri, 2023). The presence of a backdoor enabled the intruder to observe and manipulate the avionics system, thereby compromising the safety of the flight mission (Mekdad et al., 2021).

Additionally, an adversary may have the ability to impair cables to attempt to sabotage connections (Constantin et al., 2019).

TABLE 1 Threats and mitigation on hardware.

Threat ID	Threat	C	I	A	Suggested mitigation	Interaction
T.H.01	Physical capturing of UAV/tampering attack (§4.2.1.1)	o	o	o	• *Hardware-based security* • *Authenticated encryption* • *Device locking* • *Following standards*	E1, L4
T.H.02	Physical collisions (§4.2.1.2			o	• *Hardware-based security* • *Two-stage reinforcement learning* • *Collision avoidance systems*	E1, E2
T.H.03	Technical failure (§4.2.1.3)			o	• *Power prediction systems* • *Battery optimization* • *Dynamic control power*	E1
T.H.04	Human error (§4.2.1.4)	o			• *Hardware-based security* • *Reconfigurable flight control system* • *HFACS*	E1, E2
T.H.05	Airborne and land threats (§4.2.1.5)			o	• *Hardware-based security* • *Two-step GA-XGBoos* • *Hijacking detection*	E1
T.H.06	Supply chain attack (§4.2.1.6)			o	• *Securing communication* • *Anti-temper solutions* • *Blockchain, ML, and PUF* • *Controls at different levels*	E1

4.2.1.2 Physical collisions

UAVs operate within tangible environments where natural obstacles like trees can complicate or obstruct their tasks. The hurdles encountered by UAVs can impact the precision and reliability of information gathered via MCS endeavors (Koubâa et al., 2019).

During a flight mission that necessitates the cooperation and collaboration of numerous UAVs, there is a possibility of physical collisions occurring, which could lead to the drones crashing. In order to avoid such accidents in the public airspace, UAVs primarily depend on collision avoidance systems (CAS) (Yasin et al., 2020). However, these systems lack inherent security measures and are unable to effectively address the collision avoidance risk posed by malevolent individuals (Hannah et al., 2020).

4.2.1.3 Technical failure

UAVs are equipped with rechargeable lithium-ion batteries supported by a battery management system (BMS) to ensure a reliable energy supply to various UAV components. These UAVs are vulnerable to attacks during different operational phases, including hovering, moving, takeoff/landing, charging, and standby mode. Such attacks can quickly drain the battery, causing premature returns to base or even crashes before mission completion (Mohsan et al., 2022).

Malicious entities can deplete the battery's energy through hypothetical battery depletion attacks, compromising the availability, integrity, and confidentiality of the batteries (Lopez et al., 2017). Attackers can disrupt UAV batteries by physically tampering with them or replacing them with defective ones, leading to system failure. Another form of attack involves intentionally causing rapid battery depletion by compromising other UAV elements, such as falsifying sensors or introducing malicious software, resulting in the depletion of the UAV batteries (Mekdad et al., 2021). This undermines battery reliability by altering genuine battery data transmitted to the operator via UAV-2-GCS communication. Additionally, the privacy of UAV batteries can be jeopardized by disclosing sensitive information, such as the state-of-charge (SoC), which indicates the proportion of available charge compared to the battery's capacity.

Another hardware vulnerability arises when UAVs are exposed to high-power microwave (HPM) radiation. Such exposure can cause the UAV to lose control and sustain damage, potentially resulting in it dropping to the ground (Zhao et al., 2022).

4.2.1.4 Human error

The human factor could influence the proficiency in flying skills, including the ability to remotely control the speed, altitude, and orientation of the UAV, is necessary. In such situations, the operator's deficiency in these technical abilities could result in the drone crashing and leading to operational failure. As a result, the UAVs are susceptible to physical theft. The human errors that occurred could be significant, as investigation reveals 58% of fatal accidents are attributed to these errors[2]. Injecting malicious USBs could be performed with legitimate human users through either the UAV or the GCS. Malicious software often spreads through infected USB sticks. These infected USBs may be plugged into MCS devices either intentionally by a hostile actor or unintentionally by an unsuspecting legitimate user (Mohsan et al., 2022). To reduce the impact of human error, the autopilot system can be enhanced by including advanced decision-making capabilities, such as obstacle recognition, collision avoidance, and course planning. This will increase the autonomy of the system (Yasin et al., 2020).

2 Accident Statistics. spanning from January 1960 to December 2015. Accessed: Sep. 13, 2019. [Online]. Available: http://www.planecrashinfo.com/cause.htm

TABLE 2 Threats and mitigation on software.

Threat ID	Threat	C	I	A	Suggested mitigation	Interaction
T.S.01	Malware attack (§4.2.2.1)	o	o		• *System hardening* • *Malware detection (static/dynamic)* • *Intrusion detection systems*	E2
T.S.02	Database attack (§4.2.2.2)		o		• *Secure storage and anti-tampering*	E2
T.S.03	Snoopy attack (§4.2.2.3)	o	o		• *Secure storage and anti-tampering* • *Blockchain-based access control*	E1 L1
T.S.04	Skyjet attack (§4.2.2.4)	o		o	• *Fog computing in UAV env* • *Permission-based access control and attestation*	E1
T.S.05	Mal-drone attack (§4.2.2.5)	o	o	o	• *Malware detection (static/dynamic)* • *Intrusion detection systems* • *Secure communication*	L1,L2,L3
T.S.06	Malicious firmware update (§4.2.2.6)	o	o	o	• *Lifecycle management* • *Secure storage and anti-tampering* • *Permission-based access control and attestation*	E1
T.S.07	Vulnerabilities in drone OS (§4.2.2.7)	o	o	o	• *System hardening* • *Intrusion detection systems* • *Secure communication*	E1
T.S.08	PX4 and Ardupilot software bugs (§4.2.2.8)		o		• *Permission-based access control and attestation* • *System hardening* • *Secure communication*	E1
T.S.09	SQL & NoSQL Injection (§4.2.2.9)	o	o	o	• *Secure storage and anti-tampering* • *Intrusion detection systems* • *ML-based detection*	E2
T.S.10	Phishing (§4.2.2.10)	o			• *Permission-based access control and attestation* • *Intrusion detection systems*	E2
T.S.11	System failures (§4.2.2.11)		o		• *Fog computing in UAV env* • *System hardening*	E1, E2 L1,L2,L3
T.S.12	Backdoor attacks (§4.2.2.12)	o			• *System hardening* • *Malware detection (static, dynamic)*	L1,L2,L3
T.S.13	Zero-day exploit (§4.2.2.13)	o			• *Hardware-based security* • *ML-based detection*	E1, E1

4.2.1.5 Airborne and land threats

UAVs are susceptible to attacks from other armed UAVs, which can inflict damage on vital telecommunication infrastructure (Constantin et al., 2019).

Additionally, UAV swarms are being employed for military offensives as a result of their technological advancements. Currently, there is a deficiency in strategies to counteract such attacks. However, GPS spoofing could be utilized as a countermeasure to trick the position-sensing mechanism of armed UAVs. Using the open-source tools ROS and Gazebo, a simulation environment was constructed for the position perception of an armed swarm of UAVs (He et al., 2020).

Moreover, UAVs are vulnerable to hijacking due to their visibility at low heights. Opponents can gain control by directly taking over operations or using malicious software. Anti-drone guns, used by law enforcement to disable unauthorized UAVs, can also be exploited by attackers to hijack drones[3].

3 K. Hodgkins, Anti-drone shoulder rifle lets police take control of UAVs with radio pulses. (2015), (Online; Accessed 2 April 2022) (2015). https://www.digitaltrends.com/cool-tech/battle-innovations-anti-drone-gun/.

4.2.1.6 Supply chain attacks

Supply chain attacks on UAVs are increasing as the drone industry expands. Adversaries exploit weaknesses in the supply chain, targeting sensitive components like propellers, airframes, and actuators. Belikovetsky et al. (2017) demonstrated a feasible attack by remotely manipulating the design files of 3D-printed propellers, reducing their fatigue life and causing delayed damage during flight. This highlights the complexity of identifying sabotage in additive manufacturing systems.

4.2.2 Software-related threats

Threats targeted to UAV software are identified as below. Table 2 shows the threats related to software. Threat ID T.S. indicates a threat related to software.

4.2.2.1 Malware attacks

Malware, a type of malicious software, is designed to disrupt the regular operations of computers, servers, networks, or other system elements. When malicious actors introduce malware into the system, they carry out unauthorized activities, constituting a malware attack (Pundir et al., 2019).

Within the context of MCS, viruses and Trojans are commonly identified as threats to service providers and GCS systems. A malware attack on cyber-physical systems such as GCS is more critical, as Xu et al. (2023) addressed.

4.2.2.2 Database attacks

Within MCS, database infrastructures hosted in the cloud become vulnerable to targeted attacks, potentially leading to unauthorized data exposure. These threats are not confined to wireless sensor networks (WSNs) or IoT communication environments but extend to any cloud-based database systems. Such attacks may result in the unauthorized disclosure of information, with notable examples including cross-site scripting (XSS) and cross-site request forgery (CSRF), as addressed by Malik and Patel (2016) and Pundir et al. (2019).

4.2.2.3 Snoopy attacks

Utilizing a WiFi-enabled smartphone, the attacker gains the capability to track and manipulate the navigation control of the compromised UAV, thereby connecting the security breach to MCS and the manipulation of sensed data.

4.2.2.4 Skyjet attacks

In Skyjet attacks, UAV navigation controllers are targeted. He et al. (2017) reported that attackers install specialized software to disrupt the connection, leading to the hijacking of the UAV during flight. This malware enables the attacker to identify nearby wireless networks. As a result, the pilot loses control as the compromised UAV connects to the attacker's network, facilitating device theft (Yahuza et al., 2021). This scenario highlights the intersection of UAV security vulnerabilities with the potential exploitation of sensed data in MCS.

4.2.2.5 Maldrone attacks

Maldrone is a versatile software that acts as a backdoor, using TCP ports to serve as a mediator between the flight controller and sensor communication of the target UAV. Once a TCP connection is established, the attacker gains access to tamper with the sensors, ultimately enabling UAV theft. By awaiting a reverse TCP connection, Maldrone empowers the attacker to control the target UAV upon connection (Arteaga et al., 2019).

4.2.2.6 Malicious firmware updates

The attacker manipulates users into installing fake firmware updates on UAVs, granting them control upon activation. These vulnerabilities intersect with MCS, raising concerns about compromised sensed data (Sidharthan et al., 2021).

4.2.2.7 Vulnerabilities in drone OSs

Despite UAVs' widespread use, their operating systems lack essential cybersecurity measures, with software vulnerabilities posing risks of disruptions or significant consequences like theft or crashes (Constantin et al., 2019).

4.2.2.8 PX4 and Ardupilot software bugs

PX4 and *Ardupilot*, widely used in UAVs and other unmanned vehicles, have been found to contain numerous vulnerabilities that endanger UAVs. An extensive analysis revealed 569 bugs (Wang et al., 2021), including UAV-specific vulnerabilities, within these autopilot software systems. This highlights the significant intersection with MCS and the potential compromise of sensed data.

4.2.2.9 SQL & NoSQL injections

SQL injection involves exploiting SQL databases by executing malicious queries, aiming to breach security and potentially access, alter, or execute commands remotely. UAVs storing data on the cloud, like surveillance footage, are vulnerable to such attacks. NoSQL injections targeting databases such as MongoDB follow a similar pattern (Gupta et al., 2020). These vulnerabilities underscore the significant link with MCS and the risk of compromising sensed data.

4.2.2.10 Phishing

Successful phishing attacks can lead to the theft of sensitive information or the installation of malware on systems like GCS, enabling further malicious actions. These risks intersect with MCS and the potential compromise of sensed data (Mohsan et al., 2022).

4.2.2.11 System failures

System failure, including software failure, can cause network disruption and affect operations (Constantin et al., 2019).

4.2.2.12 Backdoor attacks

Backdoor attacks involve attackers circumventing all existing cybersecurity measures to gain unauthorized access to the target system or application (Constantin et al., 2019).

4.2.2.13 Zero-day exploits

Attackers capitalize on vulnerabilities that are not yet known to vendors or developers, known as zero-days, exploiting them before any remedial actions, like patches, can be implemented (Constantin et al., 2019).

4.2.3 Communication-related threats

Table 3 shows the communication-related threats. Threat ID T.C. indicates the threat is related to the communication.

4.2.3.1 Communication interception attacks

This includes attacks like eavesdropping, traffic analysis, signal capturing, and port scanning. All of them refer to the act of intercepting and accessing information transferred between two parties through unprotected network channels. An instance of such communication that could be focused on in an MCS architecture is the transmission of messages between the GCS and the UAV (Pundir et al., 2019). The attackers could examine traded communications to extract valuable information, such as the communication frequency and the packet sizes. Additionally, the attackers engage in unauthorized post-scanning activities within the target network to find ports that may be running potentially susceptible services.

Bera et al. (2021) reported that ephemeral secrets used in communication sessions are the target of ESL attacks. Attackers may be able to take over sessions and access the UAVs without authorization if these transient secrets are exposed.

In 2009, insurgents in Iraq used SkyGrabber software to intercept live video streams from U.S. UAVs. The tool, priced at

TABLE 3 Threats and mitigation on communication.

Threat ID	Threat	C	I	A	Suggested mitigation	Interaction
T.C.01	Communication interception attacks (§4.2.3.1)	o			• *Encryption* • *Transmitting artificial noise* • *Filter the flight paths*	E1, E2 L1,L2,L3
T.C.02	Denial-of-service attack (DoS) Jamming, flooding (§4.2.3.2			o	• *Monitoring packet flows to detect DDoS* • *Mobility model for multi-UAV WSNs* • *Network management protocol* • *Direct sequence spread spectrum (DSSS)* • *Frequency-hopping spread spectrum (FHSS)*	E1, E2 L1,L2,L3
T.C.03	Data manipulation (§4.2.3.3)		o		• *Encryption* • *Blockchain technology*	E.1 L2 (cellular),L3 (satellite), and L5
T.C.4	Autopilot attack (§4.2.3.4)		o		• *Real-time autopilot*	E1
T.C.5	Acoustic attack (§4.2.3.5)			o	• *Physical isolation* • *Software analysis* • *Signal processing techniques, Acoustic shielding*	E1 L1, L2, L3, and L5
T.C.6	Byzantine attack (§4.2.3.6)			o	• *redundancy and diversity* • *Byzantine fault tolerance* • *Monitoring and logging*	L1, Lnor2, and L3
T.C.7	DNS cache poisoning attack (§4.2.3.7)			o	• *Domain name system security extensions*	E2
T.C.8	Wormhole attack (§4.2.3.8)		o		• *Position-based routing protocols* • *Local monitoring*	L1, L2, and L3

TABLE 4 Overview of hardware mitigations.

Mitigation strategy	References	Pros	Cons	Threat
Hardware-based security	Jin (2015); Kaushal et al. (2022); Plooij et al. (2015); Mekdad et al. (2021); SAE International (2020); GlobalPlatform (2022); Trusted Computing Group (2024)	• Leverages physical components like crypto-accelerators to enhance security, providing protection against remote attacks while improving system performance	• Expensive and less adaptable than software-based approaches	T.H.01
Physical collision mitigation	Wang et al. (2020); Yasin et al. (2020); Pan et al. (2022)	• Uses reinforcement learning and decentralized algorithms to handle dynamic environments, improving obstacle avoidance and flight navigation	• May lead to instability or oscillations in rapidly changing scenarios	T.H.02
Technical failure management	Prasetia et al. (2019); Abeywickrama et al. (2018); Bentz and Panagou (2017); Shakhov and Koo (2018); Shaikh et al. (2021); Tlili et al. (2022); Seerangan et al. (2024)	• Implements predictive analytics, energy optimization, and dynamic controls to manage power limitations, avoid technical failures, and improve overall efficiency	• Dependent on IoT data integration and may require coordination with external energy systems	T.H.03
Human error reduction	Kopyt and Żugaj (2020); Grindley et al. (2024)	• Enhances operator performance through reconfigurable systems and human factor assessments, reducing the likelihood of control mistakes	• Changes UAV control mechanics, necessitating additional training and algorithmic refinements	T.H.04
Hijack detection and prevention	Feng et al. (2020); Jares and Valasek (2021)	• Uses machine learning and flight path monitoring to detect and mitigate GPS spoofing or hijacking attempts in real time with high accuracy	• Struggles with novel attack patterns outside of known data	T.H.05
Supply chain protection	Gurtu and Johny (2021); Mekdad et al. (2021); Hassija et al. (2020); Rao et al. (2021)	• Protects UAV components through tamper-resistant methods, blockchain, and machine learning, ensuring strong authentication and improving transparency	• Requires extensive adoption, with blockchain usage still limited and PUFs challenging to deploy in complex systems	T.H.06

only $26, enabled the attackers to capture satellite signals without complex technology, exploiting the UAVs' lack of encryption. This encryption was intentionally omitted to prevent delays in real-time transmission (Oruc, 2022).

4.2.3.2 Denial-of-service attacks, jamming, and flooding

The attacker performs a flooding attack by sending an extensive number of requests, leading to the exhaustion of the target system's resources. Typical methods involve reducing the

TABLE 5 Overview of software mitigations.

Mitigation strategy	References	Pros	Cons	Threat
System hardening	Barker et al. (2015); Pendleton et al. (2016)	• Reduces vulnerabilities by disabling unnecessary services • Strengthens security with proper system configurations	• Challenging to enforce consistently across diverse systems • Needs frequent updates and active monitoring	T.S.01, T.S.07, T.S.08, T.S.11, T.S.12
Secure storage and anti-tampering	Wu et al. (2023); Lee (2020)	• Safeguards sensitive information like credentials • Prevents unauthorized software changes	• Anti-tampering adds operational complexity • Secure storage may strain resources	T.S.02, T.S.03, T.S.06, T.S.09
Containerization and virtualization	Chandramouli (2019)	• Restricts attack impact through system isolation • Promotes security using microservices	• Can reduce performance • Integration with legacy systems can be tricky	T.S.08
Fog computing in UAV environments	Habibi et al. (2020); Al-Khafajiy et al. (2020)	• Cuts latency and saves bandwidth by local data processing • Protects sensitive data by localizing it • Enhances resilience during network failures	• Demands additional infrastructure and management effort • Dependent on available hardware and networks	T.S.04, T.S.11
Blockchain-based access control	Bera et al. (2021)	• Detects and blocks unauthorized UAVs • Ensures data legitimacy with transparent records	• Expensive and complex to implement • Requires specialized infrastructure	T.S.03
Machine learning-based detection (e.g., SVM)	Shafique et al. (2021); Selvarajan et al. (2024)	• Efficient in identifying spoofing and threats automatically • Adapts to evolving attack patterns	• Relies on extensive training datasets • Computationally intensive and prone to false positives	T.S.09, T.S.13
Intrusion detection systems (IDS)	Sedjelmaci et al. (2016)	• Monitors real-time activities to spot threats • Can be tailored to UAV networks	• Communication delays may occur • Struggles to scale with many UAVs	T.S.01 T.S.05 T.S.09 T.S.10
Permission-based access control and attestation	Iqbal et al. (2020); Dushku et al. (2020)	• Verifies software integrity to block malicious code • Scales well for large IoT systems with remote attestation	• Needs continuous updates and oversight • Vulnerable to bypass if poorly implemented	T.S.04 T.S.06 T.S.08 T.S.10
Malware detection (static & dynamic)	Ahsan et al. (2022); Niyonsaba et al. (2023)	• Recognizes known and unknown malware using diverse methods • Offers a layered approach to detection	• Static detection misses novel threats • Dynamic detection requires high resources and special setups	T.S.01 T.S.05 T.S.12
Privacy-preserving techniques	Li et al. (2017); Brahem et al. (2022); Mun et al. (2024)	• Protection for sensitive data • Allows secure data aggregation and analysis, ensuring data remain useful without exposing sensitive details	• Require significant computational power • Integration can be complex	T.S.03 T.S.09 T.S.12

processing of GCS and the battery power of UAVs (Pundir et al., 2019).

Bera et al. (2021) reported that denial of service (DoS) attacks try to overload UAV communication systems and make them unusable, and attackers can prevent UAVs from operating normally by overloading the network with requests or jamming communication signals.

In MCS applications and specifically within the UAV's network, this could happen in many forms, such as GPS, GCS, and global navigation satellite system (GNSS) jamming. They all primarily refer to the act of obstructing signals intended for the designated UAV (Yahuza et al., 2021). This might lead to a loss of control over the UAVs, which would put operational safety and mission success in danger. This attack requires that the adversary transmits discovery messages faster than the remaining nodes within the infrastructure.

4.2.3.3 Data manipulation

Data manipulation assaults encompass various types of attacks, including *GPS spoofing*, *data injection*, *enlargement attacks*, *reduction attacks*, *route injections*, and *blackhole attacks*.

GPS spoofing is widely recognized as a prevalent form of assault targeting UAVs. The assailant produces counterfeit GPS signals and feeds them to the targeted UAV, so altering its course. The attacker first disrupts communication between the UAV and the GCS through different types of communication and then sends false signals (Yahuza et al., 2021).

Bera et al. (2021) reported that sensitive information breaches, data manipulation, and unauthorized control are all possible outcomes of these attacks. Sending fake data packets to UAVs to trick or control their behavior is known as packet spoofing.

He et al. (2018) reported that GPS spoofing involves transmitting false GPS data to UAV receivers, leading to incorrect navigation and

TABLE 6 Summary of secure communication strategies.

Mitigation strategy act	Reference	Pros	Cons	Threat
Secure communication channels (e.g., TLS, MAVLink) and policy measures	Han et al. (2024); GlobalPlatform (2022)	• Protects confidentiality, integrity, and authenticity	• High cryptographic overhead and challenges in key management	T.C.01
Physical-layer security with artificial noise and altering UAV flight paths	Liu et al. (2017); Zhang et al. (2017)	• Strengthens resilience against interception	• Requires additional resources and complex implementation	T.C.01
Packet flow monitoring, GPS-based algorithms, and SDN security measures	Tan et al. (2020); McCoy and Rawat (2019); Ashraf and Latif (2014)	• Enhances system reliability and reduces disruptions	• Resource-intensive for constrained devices	T.C.02
Spread spectrum techniques (DSSS and FHSS)	Kong (2021)	• Effective against jamming attacks	• High energy usage and increased system complexity	T.C.02
Encrypting navigation and control messages	Rodday et al. (2016)	• Prevents unauthorized command tampering	• Expensive and limited in civilian applications	T.C.03
Blockchain technology for message integrity	Ghribi et al. (2020)	• Guarantees data authenticity and integrity	• Computationally demanding and lacks confidentiality	T.C.03
Intrusion detection systems (IDS) and embedded markers	Stracquodaine et al. (2016)	• Detects anomalies and ensures operational integrity	• Susceptible to false alarms, requiring constant monitoring	T.C.04
Physical shielding and filtering techniques	Gao et al. (2022); Kong (2021)	• Minimizes interference and enhances accuracy	• Adds weight and struggles in dynamic conditions	T.C.05
Byzantine fault tolerance (BFT) and redundant routing	Taggu and Marchang (2019)	• Ensures network functionality despite faults	• Increases overhead and routing delays	T.C.06
DNSSEC (domain name system security extensions)	Anagnostis et al. (2024)	• Cryptographically secures DNS responses	• Infrastructure requirements limit widespread adoption	T.C.07
Position-based routing with digital signatures	Anagnostis et al. (2024); Selvarajan (2024)	• Maintains data integrity and mitigates routing anomalies	• Cryptographic reliance can create inefficiencies	T.C.08

control. UAVs heavily reliant on GPS signals are particularly vulnerable to such deception and interference, which can jeopardize flight safety. Mitigation strategies for GPS spoofing include using information fusion techniques that integrate monocular sensors and inertial measurement units (IMUs) to detect spoofing effectively. Additionally, employing error reduction methods based on feature detection and matching can support autonomous return functions, reducing the impact of GPS spoofing attacks and ensuring safe UAV operations.

Data injection attacks are a malicious technique where an attacker inserts or manipulates data in a system or flight control computer in order to exploit vulnerabilities and gain unauthorized access or control over the system. This type of attack can be classified into two main categories: false/fake data injection attack and generic false data injection attack. The first category pertains to situations in which the attacker manipulates the estimation of the UAV's direction state by tampering with the corresponding measurement in a way that avoids detection by a bad measurement detector. In the context of the generic false data injection attack category, the attacker alters the position estimation value of the UAV within a specific range (Khan et al., 2022).

A *blackhole attack* intercepts incoming data packets but refrains from forwarding them to their intended destination. Alternatively, the black hole discreetly discards the packets, so establishing a "black hole" in the network where data vanishes without reaching its intended destination (Chaari et al., 2020).

Lastly, the reduction attack refers to the assailant manipulating the data of the UAV's distance measurement to make it seem smaller than its actual value and sending this altered data to the UAV. In contrast, an enlargement attack manipulates the measured distance to appear larger than the actual value and then sends the data to the UAV (Yahuza et al., 2021). Singh et al. (2019) showed an enlargement attack on *ultra-wideband* and proposed a detection mechanism against the attack.

4.2.3.4 Autopilot attacks

An autopilot attack entails exploiting weaknesses in autopilot software to manipulate the intended trajectory of the UAV (Yahuza et al., 2021).

4.2.3.5 Acoustic attacks

An acoustic attack refers to the deliberate employment of a hostile UAV that is equipped with specific equipment to generate sounds that purposefully deviate from the resonance frequency of the targeted UAV's gyroscope. By manipulating the targeted UAV, the acoustic position control algorithm is disturbed, which compromises the integrity of its navigation (Yahuza et al., 2021).

4.2.3.6 Byzantine attacks

A Byzantine attack involves a multifaceted assault where attackers engage in various tactics simultaneously. These tactics include creating routing loops, deliberately directing packets along suboptimal paths, and selectively dropping packets to disrupt network availability. The consequences of these actions are significant, leading to both the destabilization and deterioration of routing services (Chaari et al., 2020).

4.2.3.7 Domain name server (DNS) cache poisoning attacks

This attack seeks to capitalize on weaknesses in DNS servers in order to redirect traffic to a malicious server rather than the intended legitimate server (Gupta et al., 2020).

4.2.3.8 Wormhole attacks

The attacker is responsible for recording the packets and forwarding them to the second attack, as reported by Zhang (2023).

This could be similar to the replay attack, where valid communication data are intercepted and then retransmitted to generate reactions or actions that are not authorized. Furthermore, it is similar to MITM attacks, where an adversary eavesdrops on and potentially modifies the communications between UAVs and their control centers, as reported by Bera et al. (2021).

5 Holistic strategies for mitigating MCS threats in UAVs

Existing mitigation techniques, as outlined in Section 3, are often scenario-specific and insufficient to address the diverse threats UAVs face discussed in Section 4. To address this gap, we propose a comprehensive strategy that integrates multiple countermeasures.

We begin by examining *hardware-assisted security*, which enhances resilience against physical and remote attacks. Next, we focus on *system hardening*, emphasizing software-based protections to secure UAV operations. Finally, we address *communication countermeasures*, targeting confidentiality, integrity, and availability, especially against physical-layer attacks.

Each strategy is accompanied by an assessment of its advantages and limitations, ensuring a balanced evaluation. These measures are applied throughout the UAV *lifecycle*, from pre-deployment to post-operation, and we discuss the adoption of a *cybersecurity framework*. Relevant mitigation areas are summarized in Tables 4–6, correlating specific threats to corresponding solutions.

5.1 Adopting hardware-assisted security environments

5.1.1 Relevant threats

Physical capturing of UAV/tampering attack (T.H.01), Physical collisions (T.H.02), Technical failure (T.H.03), Human error (T.H.04), Airborne and land threats (T.H.05), and Supply chain attack (T.H.06).

5.1.2 Mitigation

Hardware is traditionally considered a reliable component that supports the entire computer system. Because modifying the hardware requires physical contact, hardware-related methods are utilized to mitigate cyberattacks, which are usually performed remotely. Hardware components designed for a dedicated purpose show higher performance than software-only methods, such as hardware-based crypto-accelerators. Consequently, hardware-based security research typically focuses on the practical use of cryptographic techniques and the protection of system integrity.

5.1.2.1 Physical capturing

As Jin (2015) reported, hardware-based security is used in various ways to enhance the authenticity of the devices. Several researchers, including Kaushal et al. (2022) and Plooij et al. (2015), studied *device-locking* techniques to prevent unauthorized access when a device is stolen. To avoid unauthorized access and hijacking of the flying UAV, it is crucial to employ authenticated encryption to secure both the GCS and the UAVs. Additionally, ensuring that they are free from malware will greatly reduce the risk of bad actors seizing control. By utilizing flight paths, it is possible to hinder the adversary's ability to discern the flying pattern, hence increasing the level of difficulty for physical theft of the target (Mekdad et al., 2021). As software-only protection cannot guarantee strong security against physical attack, several standards, such as SAE International (2020), GlobalPlatform (2022), and Trusted Computing Group (2024), recommend deploying hardware-assisted security environments as the trust anchor.

5.1.2.2 Physical collisions

Wang et al. (2020) introduce a decentralized collision avoidance strategy for multi-UAV systems utilizing reinforcement learning (RL) without depending on flawless sensing. The method proposes a two-stage training approach to improve resilience and accelerate the rate of convergence. The initial phase entails supervised training to direct the agent toward achieving optimal collision avoidance, while the subsequent phase uses traditional reinforcement learning to enhance the policy. Although this strategy exhibits substantial enhancements in success rate, trajectory length, and time cost compared to existing policies, the current limitation of this method, such as possible oscillations caused by sudden scenario changes, requires investigating the use of recurrent neural network architectures. Additionally, Yasin et al. (2020) classified collision avoidance of autonomous systems in different approaches into two categories: *perception* and *action*. Perception, specifically obstacle detection, entails the utilization of sensors to identify impediments. Active sensors emit signals, whereas passive sensors depend on external sources such as sunlight. The actions for avoiding collisions can be classified into four categories: *geometric methods*, *manipulation of force fields*, *optimizations based on known obstacle parameters*, and *real-time judgments* made through sensing and avoiding. However, these systems lack inherent security measures and are unable to effectively address the collision avoidance risks posed by malevolent individuals (Pan et al., 2022).

5.1.2.3 Technical failure

A number of strategies have been suggested for UAV battery depletion attack mitigations, such as power prediction and analysis (Prasetia et al., 2019), battery optimization (Abeywickrama et al., 2018), and dynamic control power (Bentz and Panagou, 2017). However, these approaches have limitations and frequently depend on solutions derived from IoT and attacks on electric vehicle battery depletion[4]. Several methods, such as the cumulative sums method (Shakhov and Koo, 2018) and a probabilistic model checking scheme (Shaikh et al., 2021), can detect aberrant energy use

4 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.

during attacks. Additional safeguards involve performing malware analysis on the network, managing physical hardware interfaces, and monitoring control channels for illegal activities (Tlili et al., 2022). Seerangan et al. (2024) employed adaptive deep reinforcement learning with a novel loss function to enhance energy efficiency.

5.1.2.4 Human error

Kopyt and Żugaj (2020) propose a reconfigurable flight control system for UAVs that compensates for control surface failures by utilizing other control surfaces and the engine. The system's effectiveness was validated through experiments with human operators using a UAV flight simulator, testing various failure configurations. The reconfigurable system, while effective in critical failure scenarios, significantly altered UAV dynamics in single failure cases, sometimes making it harder for operators to control the UAV. This issue could be mitigated with improved algorithms and additional operator training to adapt to the system. Moreover, Grindley et al. (2024) employ human factors analysis and classification system (HFACS) to methodically identify and analyze the underlying causes of UAV mishaps. HFACS classifies these factors as risky actions, preconditions, supervisory deficiencies, and organizational impacts, offering a thorough structure to evaluate the human and environmental aspects that contribute to UAV accidents. The study examined 77 instances of UAV accidents from accident investigation reports spanning a period of 12 years. The study specifically investigated the role of human factors in 42 of these incidents. The main constraint identified in the study is the relatively limited sample size of 42 occurrences related to human factors, which may not encompass the complete spectrum of UAV accident scenarios.

5.1.2.5 Hijack

Feng et al. (2020) present a method for identifying GPS spoofing attacks on drones, which is called the two-step GA-XGBoost method. The approach begins by training the model externally using flight data. The training parameters are optimized using a Genetic Algorithm (GA) to improve the performance of the XGBoost model. After the model is trained, it is sent to the drone, and additional training is performed using real-time sensor data to ensure accurate predictions. Subsequently, the model transitions to prediction mode, facilitating the immediate identification of GPS spoofing assaults. However, the suggested approach is dependent on learning-based detection; hence, it can only identify attacks that exhibit behaviors comparable to those observed during the training process. Jares and Valasek (2021) introduced a hijacking detection technique for UAVs based on a statistical analysis of typical flying patterns. They demonstrated its efficiency against 20 potential hijacking cases through simulations tested against 50 baseline flights. However, the method proves ineffective when simulation factors, such as control instability, are altered, indicating a need for further testing and enhancement of simulation data accuracy.

5.1.2.6 Supply chain

To combat supply chain assaults, it is crucial to ensure the security of the supply chain during the manufacturing process in order to prevent the utilization of hacked UAV components (Gurtu and Johny, 2021). In addition, tamper-proof microprocessors and anti-tamper software can effectively prevent any unauthorized alterations, whether physical or logical, that could potentially jeopardize the legitimacy of the vital components of the UAV (Mekdad et al., 2021). Hassija et al. (2020) suggested employing blockchain, machine learning, and *physically unclonable functions* (PUFs) to solve security problems in existing supply chain designs. Blockchain is proposed as a means to increase transparency and security, machine learning to enhance predictive capacities and efficiency, and PUFs for strong authentication. The study highlights the capacity of these technologies to fundamentally transform supply chain processes by enhancing their security and reliability. However, the constraint is in the extensive acceptance and execution of these technologies. Although IoT and AI have been widely adopted, blockchain technology is still not being fully leveraged, and there is currently no established reference model for PUFs in complex supply chains.

Rao et al. (2021) emphasize that in order to address supply chain assaults in IoT, it is essential to apply controls at the device, network, and organizational levels. It is crucial to thoroughly test products for security at the device level before deploying them. Additionally, it is important to use strong authentication mechanisms that use cryptographic keys and to ensure that software updates are secure by using permitted connections. At the network level, it is crucial to divide important networks, follow secure integration standards, install hardware firewalls, and set up warning systems to quickly identify anomalous device behavior. It is crucial for organizations to perform a thorough risk assessment to detect weaknesses, follow industry standards for cybersecurity, and utilize machine learning and artificial intelligence to analyze network traffic for malicious activities. These combined actions greatly enhance overall security and foster confidence in the IoT ecosystem.

5.2 System hardening

5.2.1 Relevant threats

Malware attack (T.S.01), Database attack (T.S.02), Snoopy attack (T.S.03), Skyjet attack (T.S.04), Mal-drone attack (T.S.05), Malicious firmware update (T.S.06), Vulnerabilities in Drone OS (T.S.07), PX4 and Ardupilot software bugs (T.S.08), SQL and NoSQL injection (T.S.09), Phishing (T.S.10), System failures (T.S.11), Backdoor attacks (T.S.12), and Zero-day exploit (T.S.13).

5.2.2 Mitigations

Hardening of the system, or system hardening, is a process intended to eliminate a means of attack by patching vulnerabilities and turning off nonessential services, as defined by Barker et al. (2015). Pendleton et al. (2016) reported that system hardening techniques are methods to reduce security vulnerabilities and threats by configuring different functionalities, including hardware and software in the target system.

5.2.2.1 Database attacks

Multiple security techniques must be adopted for system hardening. For example, deploying secure data storage in UAV clusters emphasizes the adoption of distributed storage methods to enhance data protection. These techniques safeguard data against

unauthorized access while ensuring its integrity and availability across the UAV network (Wu et al., 2023). Also, device anti-tampering applications could be deployed to detect, prevent, or impede unauthorized modification of software (Lee, 2020).

5.2.2.2 PX4 and Ardupilot software

Bug system hardening is not limited to adopting the sole technology but also includes designing the architectures. Deploying isolation techniques such as containerization or virtualization as microservices is recommended as an effective way to limit the impact even when a certain part of the system is compromised, as reported by Chandramouli (2019).

5.2.2.3 Skyjet attacks, system failures, and zero-day exploits

Deploying fog computing architecture into UAV environments could be considered. Habibi et al. (2020) and Al-Khafajiy et al. (2020) identified that fog computing could reduce security risks, not only improving UAV operations by lowering latency and bandwidth issues but also enabling faster data processing and decision-making. Because fog computing also allows local data processing when network bandwidth is limited, resiliency during network disruptions could be improved. Additionally, fog computing enhances data privacy and security by processing sensitive information locally, thus mitigating some risks associated with transmitting data over external networks.

5.2.2.4 Vulnerabilities in drone OSs

Regular updates to the operating system are essential for preventing the compromise of UAVs and their payloads. By implementing firewalls on the GCS, it is possible to prevent harmful traffic from accessing the UAVs. Software solutions such as antivirus programs and intrusion detection systems (IDSs) can oversee network traffic in order to safeguard UAVs from malevolent actions (Mekdad et al., 2021).

5.2.2.5 SQL and NoSQL injections and phishing

In their study, Sedjelmaci et al. (2016) developed an IDS specifically designed for UAV networks. The system demonstrated an impressive detection accuracy of over 93% in simulations while maintaining a false positive rate of under 3%. However, the act of augmenting the quantity of UAVs has a substantial impact on both the rate of incorrect negative outcomes and the amount of energy consumed, hence influencing the scalability of the network. Rabie et al. (2024) presented an advanced IDS for IoT networks by integrating the Decisive Red Fox (DRF) algorithm for feature selection with a descriptive back-propagated radial basis function (DBRF) classifier. Machine learning- (ML) based methods are also considered as security countermeasures. Shafique et al. (2021) proposed a spoofing detection mechanism based on the support vector machine (SVM) and voting techniques. Other researchers, including Li et al. (2017), Brahem et al. (2022), and Mun et al. (2024), have proposed privacy-preserving mechanisms for the data in MCS.

5.2.2.6 Snoopy attacks and backdoor attacks

Implementing permission measures for UAV system resources can effectively prevent the execution of malicious code. Software-based attestation methods, which guarantee the integrity of the software operating on the flight stack, provide protection against software-based attacks (Iqbal et al., 2020). Remote attestation solutions are cost-effective and can efficiently verify the authenticity of the software stack.

5.2.2.7 Mal-drone attacks and malicious firmware updates

Dushku et al. (2020) presented a secure asynchronous remote attestation (SARA) protocol specifically for the purpose of verifying a substantial amount of IoT devices. Based on their accurate simulations, it was shown that SARA has a small storage need of 3.03 KB, a runtime of 19 s for 250 services, and a very low energy usage of 0.196 mJ. Selvarajan et al. (2024) explored generative AI techniques to enhance automated content creation, particularly in identifying and filtering fraudulent or duplicated content. Emerging technologies are also being adopted. Several researchers are proposing blockchain-based methods as mitigation. For example, Bera et al. (2021) proposed a blockchain-based access control scheme to detect unauthorized UAVs, only allowing the genuine data from a UAV to the GCS and storing the suspicious data for detection of unauthorized UAVs in a private blockchain.

5.2.2.8 Malware

The categorization of virus detection technologies, as outlined in Ahsan et al. (2022), is based on static and dynamic detection methods. Static detection examines the code of files to identify virus signatures, whereas dynamic detection executes files in a virtual environment to monitor their behavior for any dangerous activities. Virus detection methods encompass signature-based, heuristic-based, behavior-based, and emulation-based detection (Niyonsaba et al., 2023).

- *Signature-based detection involves the comparison of known viral signatures with files or email attachments.*
- *Heuristic-based detection involves analyzing the behavior or attributes of a program in order to find previously unknown malware or virus variants.*
- *Behavior-based detection involves monitoring the execution of files and programs in order to identify any harmful actions.*
- *Emulation-based detection involves simulating the execution of a file in a controlled environment to monitor and document its behavior to identify any potential harmful intentions.*

5.3 Securing communication

5.3.1 Relevant threats

Communication interception attacks (T.C.01), Denial-of-service attack (DoS), Jamming, flooding (T.C.02), Data manipulation attacks (T.C.03), Autopilot attack (T.C.04), Acoustic attack (T.C.05), Byzantine attack (T.C.06), DNS cache poisoning attack (T.C.07), and Wormhole attack (T.C.08).

5.3.2 Mitigations

To ensure secure communication, deploying authenticated and encrypted channels with techniques such as *transport layer security* (TLS) is essential. Han (2023) discusses various securing techniques employed in UAV communication, including *intra-drone secure*

messaging and *drone external communication*, as well as technologies like MAVLink.

However, as discussed in Section 4.2, communication threats extend beyond cryptographic vulnerabilities and include physical interference aimed at disrupting communication availability. Efforts to address these threats include SDN-based security measures that counter physical attacks, including *denial-of-service* (DoS), *jamming*, and *spoofing* attacks.

5.3.2.1 Jamming

Several studies, such as Tan et al. (2020) and Ashraf and Latif (2014), have developed methods for monitoring packet flows to detect *DDoS* attacks. In addition, McCoy and Rawat (2019) introduced network management protocols within a monitoring architecture that improves resilience and reduces outages caused by jamming attacks alongside GPS-based algorithms for countering spoofing attacks. Kumar et al. (2019) proposed a mobility model for multi-UAV wireless sensor networks to detect DoS attacks. Li et al. (2019) introduced a Dyna-Q-based reinforcement learning algorithm for attack detection and response. Selecting sensors that remain effective under environmental noise and equipping onboard components with anti-tampering features is crucial. Communication security can be further enhanced using direct sequence spread spectrum (DSSS) and frequency hopping spread spectrum (FHSS) techniques, which counter jamming attempts by frequently shifting transmission frequencies (Kong, 2021). Access control can be reinforced by restricting connections to approved devices based on MAC addresses, hiding the UAV's access point, and encrypting authentication messages to prevent unauthorized access and defend against Wi-Fi de-authentication attacks (He et al., 2016). Additionally, Selvarajan (2024) reported that *evolutionary* and *swarm* intelligence-based optimizers are particularly effective for complex applications, offering faster convergence and superior performance than physics-based and nature-inspired ones.

5.3.2.2 Interception

Cryptography plays an essential role in safeguarding UAV communications, with symmetric encryption often being the preferred choice for resource-limited systems. However, securely distributing the keys used in symmetric encryption remains a significant challenge. Rugo et al. (2022) proposed mitigation strategies encompass both technological and policy measures. These include evaluating current defenses against space communication security (SCS) vulnerabilities and advocating for global collaboration to create robust and comprehensive space security policies. Furthermore, Podhradsky et al. (2017) proposed a scheme using Galois Embedded Crypto, adapted for Arduino-based systems, which enables secure key distribution over radio control channels on standard radio modules without the need for hardware modifications.

5.3.2.3 Eavesdropping

Both physical-layer security and cryptographic techniques are used to protect against eavesdropping. One approach involves transmitting artificial noise alongside the information signal, with optimal power distribution to minimize interception risks (Liu et al., 2017). Additionally, UAVs can alter their altitude and flight paths to further secure communication. Despite these measures, challenges remain when eavesdroppers are positioned near the transmission source (Zhang et al., 2017).

5.3.2.4 Spoofing

Encrypting control messages prevents attackers from altering or injecting malicious commands, such as those used in man-in-the-middle attacks (Rodday et al., 2016). Cryptographic methods protect navigation messages, although they are primarily used in military contexts due to cost constraints. Encrypted GPS signals, such as the Precise (P)-Code, are available to military users, while civilian GPS signals (C/A-Code) are not encrypted (Rodday et al., 2016).

5.3.2.5 Message injections

Encryption not only ensures the integrity of messages but also helps defend against message injection attacks by authenticating the sender's identity and confirming that the message has not been tampered with (Rodday et al., 2016). Blockchain technology enhances communication security by providing a verifiable record of past interactions. Although it does not safeguard the confidentiality of current messages, it ensures message integrity through consensus among UAVs. In this system, messages are encrypted and validated before delivery, ensuring secure exchanges. Blockchain is also used for the distributed storage of machine learning data, supporting collaborative decision-making among UAVs (Ghribi et al., 2020).

5.3.2.6 Autopilot attacks

Stracquodaine et al. (2016) proposed a solution that embeds markers within the UAVs to continuously monitor and record their control flow. This recorded data, reflecting typical software behavior, establishes a baseline profile. During flight, the IDS analyzes live event data against this profile, identifying any irregularities. When anomalies are detected, the system initiates various responses, including sending alerts, switching to backup controls, or, in critical situations, securely disabling sensitive components.

5.3.2.7 Acoustic attacks

Physical shielding and shock absorption protect against acoustic and external disturbances (Gao et al., 2022). Signal processing techniques, like filtering, enhance data accuracy by isolating noise from valid measurements. Redundant sensors and external reference systems help detect and reject erroneous data from acoustic interference. Acoustic shielding, using enclosures and sound-absorbing materials, further limits sound exposure to the sensors (Kong, 2021).

5.3.2.8 Byzantine attacks

Introducing redundancy and diversity in routing paths and network protocols helps reduce the impact of malicious or faulty nodes. Byzantine fault tolerance (BFT) algorithms enable the system to remain operational, even if parts are compromised. Additionally, monitoring and logging mechanisms can detect abnormal activities, ensuring the identification of network disruptions or malicious behavior (Taggu and Marchang, 2019).

5.3.2.9 DNS cache poisoning attacks

To protect against DNS cache poisoning, one effective countermeasure is the use of domain name system security

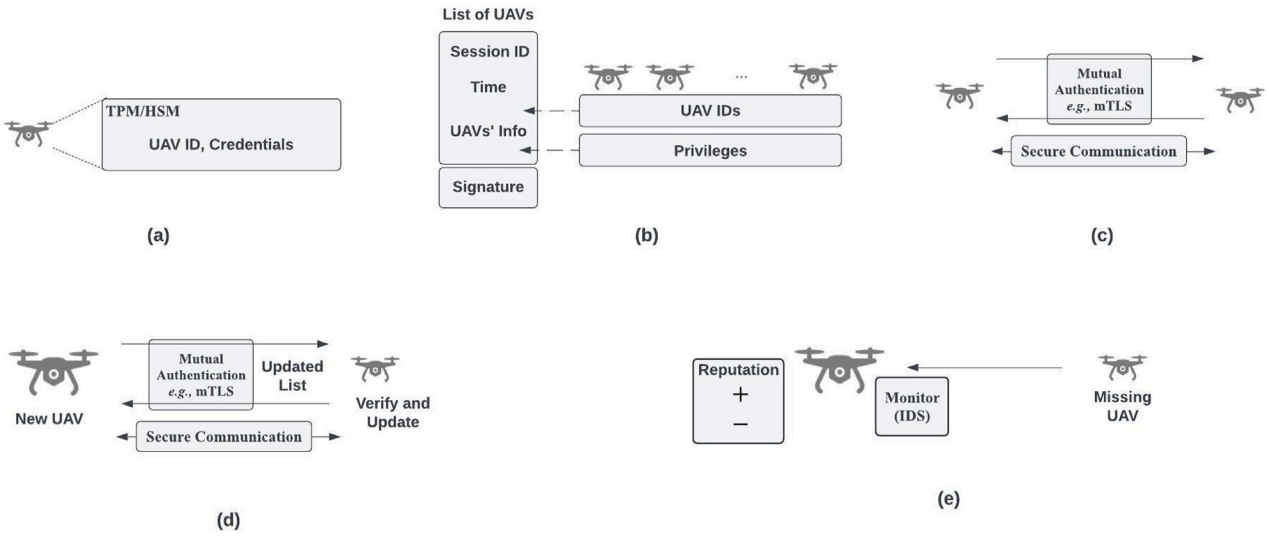

FIGURE 3
(A) A UAV stores credentials in hardware-protected security environments; **(B)** An operator assembles a group of UAVs for a specific mission; **(C)** UAVs establish a secure channel; **(D)** A new UAV joins the mission; **(E)** A suspicious UAV is monitored, and its reputation level is adjusted.

extensions (DNSSECs). This security mechanism employs cryptographic techniques to sign DNS responses to ensure their authenticity and prevent unauthorized alterations (Anagnostis et al., 2024).

5.3.2.10 Wormhole attacks

To counter wormhole attacks, it is crucial to authenticate UAV communications and verify the integrity of routing information. Approaches such as position-based routing and local network monitoring assist in detecting anomalies in the network topology. Additionally, the use of cryptographic methods like digital signatures ensures message integrity, preventing attackers from tampering with data exchanged between distant UAVs (Anagnostis et al., 2024).

5.4 Secure lifecycle management

Effective security management must encompass the entire lifecycle of a UAV—not only during operations but also before and after.

In the initial stage, UAVs may lack the capabilities for authentication or encryption. To address this, *provisioning* of secrets or software is conducted during the manufacturing phase in a physically protected environment. By installing secrets in hardware-based security environments, a more hardened system is achieved. For instance, system integrity can be protected through secure boot mechanisms that verify software using the provisioned secret.

During deployment, devices must undergo a *registration process*, which includes associating symmetric or asymmetric keys. Once registered, devices can be managed and controlled by central management entities. Researchers such as Han et al. (2024) have detailed key provisioning scenarios for UAVs. For fleet operations, registered devices can retrieve fleet mission details from the ground control station (GCS), a process known as *fleet provisioning*.

During operation, it is crucial to address incidents and ensure systems remain up to date. Researchers such as Al Blooshi and Han (2022) have demonstrated secure methods for software updates in UAV environments.

At the conclusion of operations, systems may reach *end-of-life (EOL)*. In such cases, *decommissioning* is necessary. This includes scenarios such as completing or aborting fleet missions, key revocation or expiration, or the physical end of a device's lifecycle. The operational data of fleet missions must be securely erased. Certificate revocation or key updates are required for key EOL. Device EOL disposal processes should include sanitization or zeroization of data.

Adopting a recognized cybersecurity framework, such as the *NIST Cybersecurity Framework (CSF)*, is critical to managing and reducing cybersecurity risks. The CSF, applicable across industries regardless of technical sophistication, is also suitable for UAV environments. Version 1.1 of the CSF defines five core functions: *identify*, *protect*, *detect*, *respond*, and *recover*. CSF 2.0 expands on these principles, emphasizing governance and supply chain security.

To effectively secure mobile crowd sensing in UAV environments, it is essential to consider not only specific technical measures but also the broader ecosystem, including governance and supply chain management.

6 Case study on secure UAV design

In this section, we present a case study of a specific scenario involving MCS with UAVs, utilizing the model defined in Section 5.

6.1 General operations

An operator assigns a group of UAVs to an MCS mission for a specific time period.

As shown in Figure 3A, UAVs maintain unique identifiers and credentials, such as public key pairs and certificates, within hardware-assisted security environments (*e.g.*, TPM and HSM), as discussed in Section 5.1.

Figure 3B illustrates the operator configuring a group of UAVs for a specific mission. Information about the session, including session ID, time period, UAV privileges, and UAV IDs, is collected and signed by the operator. This signed information is stored in each UAV, as described in Section 5.1.

Figure 3C depicts two UAVs establishing a secure channel. Methods such as mTLS are already suggested, as outlined in Section 5.3.

After mutual authentication, the UAVs perform MCS within the mission field over secure communication channels.

6.2 Maintaining MCS operability with missing UAVs

During the mission, UAVs may experience a temporary or permanent loss of connection due to environmental conditions. Losing UAVs can impact MCS performance. To maintain operability, the operator may assign new UAVs as replacements. When new UAVs are introduced, they might also locate the missing UAVs. In such cases, securely integrating new UAVs into the group and reconnecting with "found" UAVs are the primary security objectives.

6.2.1 Establishing secure connection with new UAVs

Figure 3D illustrates a new UAV joining an existing group by presenting verifiable information. For example, the operator may sign updated session information, including details about the new UAV, similar to the process depicted in Figure 3B. Upon verification, the new UAV can integrate into the group.

6.2.2 Restoring secure connections with missing UAVs

As shown in Figure 3E, a previously missing (lost) UAV may be exposed to threats, as discussed in Section 4.2.1. Although the credentials of the found UAV may remain valid due to protections outlined in Section 5.1, it is prudent to treat it as suspicious.

If the credentials of the "found" UAV are intact, a secure connection can be reestablished. However, its status as potentially compromised necessitates monitoring its sensing data. Intrusion detection systems or machine learning-based detection methods, as described in Section 5.2, may be employed.

Based on observed behavior, the UAV's reputation level may increase or decrease. A high reputation level would render its collected data more trustworthy for MCS operations.

6.3 Case study summary

This section presented a case study utilizing the threat analysis and mitigation strategies described in Sections 4.2, 5. The focus was on establishing secure communication among authenticated UAVs and handling suspicious UAVs. Efficient monitoring to detect intrusions is crucial for MCS in UAV environments. The detailed design and analysis of methods for effectively and securely handling missing UAVs in MCS will be addressed in future work.

7 Conclusion

The increasing use of unmanned aerial vehicles (UAVs) in mobile crowd sensing (MCS) brings forth significant challenges in ensuring data security and reliability. As UAVs are equipped with increasing numbers of sensors, the potential risks to data privacy and security are amplified. Although extensive research has been conducted on the security and privacy issues of MCS, this paper specifically focuses on the integration of MCS applications within UAV ecosystems. We presented a comprehensive review of the security and privacy challenges both within MCS and UAV contexts, followed by an in-depth threat analysis of MCS applications in UAV environments. Our analysis covered a range of attacks targeting software, hardware, and communication systems, underscoring the multifaceted nature of security threats.

Our findings indicate that relying on a single countermeasure is insufficient to address these security and privacy challenges. To effectively mitigate risks, a holistic approach is necessary—one that includes system hardening, the integration of hardware-based security solutions, secure communication protocols ensuring confidentiality, integrity, and availability, the implementation of a robust cybersecurity framework, and thorough lifecycle management practices. Additionally, our case study demonstrates how the proposed framework can enhance the security of UAV systems, particularly in scenarios where UAVs go missing, a situation that occurs periodically in UAV operations. A practical implementation of this case study is an avenue for future work, which will further explore its real-world applicability and effectiveness in mitigating UAV security issues.

Author contributions

SS: writing–original draft and writing–review and editing. HA: investigation and writing–original draft. MA: investigation and writing–original draft. KH: supervision, writing–original draft, and writing–review and editing.

Funding

The author(s) declare that no financial support was received for the research, authorship, and/or publication of this article.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

References

Abeywickrama, H. V., Jayawickrama, B. A., He, Y., and Dutkiewicz, E. (2018). Comprehensive energy consumption model for unmanned aerial vehicles, based on empirical studies of battery performance. *IEEE access* 6, 58383–58394. doi:10.1109/access.2018.2875040

Abualigah, L., Diabat, A., Sumari, P., and Gandomi, A. H. (2021). Applications, deployments, and integration of internet of drones (iod): a review. *IEEE Sensors J.* 21, 25532–25546. doi:10.1109/jsen.2021.3114266

Ahsan, M., Nygard, K. E., Gomes, R., Chowdhury, M. M., Rifat, N., and Connolly, J. F. (2022). Cybersecurity threats and their mitigation approaches using machine learning—a review. *J. Cybersecurity Priv.* 2, 527–555. doi:10.3390/jcp2030027

Al Blooshi, S., and Han, K. (2022). "A study on employing UPTANE for secure software update OTA in drone environments," in 2022 IEEE International Conference on Omni-layer Intelligent Systems (COINS) (IEEE), 1–6.

Al-Khafajiy, M., Baker, T., Hussien, A., and Cotgrave, A. (2020). Uav and fog computing for ioe-based systems: a case study on environment disasters prediction and recovery plans. *Unmanned Aer. Veh. Smart Cities*, 133–152. doi:10.1007/978-3-030-38712-9_8

Anagnostis, I., Kotzanikolaou, P., and Douligeris, C. (2024). Understanding and securing unmanned aerial vehicle (uav) services: a comprehensive tutorial. *Authorea Prepr.* doi:10.36227/techrxiv.170975064.43115762/v1

Arteaga, S. P., Hernández, L. A. M., Pérez, G. S., Orozco, A. L. S., and Villalba, L. J. G. (2019). Analysis of the gps spoofing vulnerability in the drone 3dr solo. *IEEE Access* 7, 51782–51789. doi:10.1109/access.2019.2911526

Ashraf, J., and Latif, S. (2014). "Handling intrusion and ddos attacks in software defined networks using machine learning techniques," in *2014 Nat. Soft. Eng. Conf.*, 55–60. doi:10.1109/NSEC.2014.6998241

Barker, E. B., Smid, M., and Branstad, D. (2015). *A profile for U. S. federal cryptographic key management systems*. Gaithersburg, Maryland: National Institute of Standards and Technology, 800–152.

Belikovetsky, S., Yampolskiy, M., Toh, J., Gatlin, J., and Elovici, Y. (2017). "dr0wned–{Cyber-Physical} attack with additive manufacturing," in *11th USENIX workshop on offensive technologies (WOOT 17)*.

Bentz, W., and Panagou, D. (2017). "3d dynamic coverage and avoidance control in power-constrained uav surveillance networks," in 2017 International Conference on Unmanned Aircraft Systems (ICUAS) (IEEE), 1–10.

Bera, B., Das, A. K., and Sutrala, A. K. (2021). Private blockchain-based access control mechanism for unauthorized uav detection and mitigation in internet of drones environment. *Comput. Commun.* 166, 91–109. doi:10.1016/j.comcom.2020.12.005

Boite, J., Nardin, P.-A., Rebecchi, F., Bouet, M., and Conan, V. (2017). "Statesec: stateful monitoring for ddos protection in software defined networks," in *2017 IEEE Conf. Net. Soft. (NetSoft)*, 1–9. doi:10.1109/NETSOFT.2017.8004113

Brahem, M., Scerri, G., Anciaux, N., and Issarny, V. (2022). Consent-driven data reuse in multi-tasking crowdsensing systems: a privacy-by-design solution. *Pervasive Mob. Comput.* 83, 101614. doi:10.1016/j.pmcj.2022.101614

Capponi, A., Fiandrino, C., Kantarci, B., Foschini, L., Kliazovich, D., and Bouvry, P. (2019). A survey on mobile crowdsensing systems: challenges, solutions, and opportunities. *IEEE Commun. Surv. & tutorials* 21, 2419–2465. doi:10.1109/comst.2019.2914030

Chaari, L., Chahbani, S., and Rezgui, J. (2020). "Vulnerabilities assessment for unmanned aerial vehicles communication systems," in 2020 International Symposium on Networks, Computers and Communications (ISNCC) (IEEE), 1–6.

Chandramouli, R. (2019). "Security strategies for microservices-based application systems," in *Tech. Rep. NIST special publication (SP)*. Gaithersburg, MD: National Institute of Standards and Technology, 800–204.

Constantin, I., Patachia, C., Patrascu, C., Avadanei, A., and Nitescu, L. (2019). "Threat classification in current communication infrastructures," in 2019 11th International Conference on Electronics, Computers and Artificial Intelligence (ECAI) (IEEE), 1–6.

GlobalPlatform (2022). GlobalPlatform technology: TEE system architecture v1.3. Available at: https://www.bing.com/search?q=GlobalPlatform+(2022).+GlobalPlatform+technology%3A+TEE+system+architecture+v1.3&cvid=69e44bcdf8ff4ee8a691522bd8129e59&gs_lcrp=EgZjaHJvbWUyBggAEEUYOdIBBzUzMmowajGoAgCwAgA&FORM=ANNTA1&PC=U531.

Dushku, E., Rabbani, M. M., Conti, M., Mancini, L. V., and Ranise, S. (2020). Sara: secure asynchronous remote attestation for iot systems. *IEEE Trans. Inf. Forensics Secur.* 15, 3123–3136. doi:10.1109/tifs.2020.2983282

Fascista, A. (2022). Toward integrated large-scale environmental monitoring using wsn/uav/crowdsensing: a review of applications, signal processing, and future perspectives. *Sensors* 22, 1824. doi:10.3390/s22051824

Feng, Z., Guan, N., Lv, M., Liu, W., Deng, Q., Liu, X., et al. (2020). Efficient drone hijacking detection using two-step ga-xgboost. *J. Syst. Archit.* 103, 101694. doi:10.1016/j.sysarc.2019.101694

Gao, M., Zhang, L., Shen, L., Zou, X., Han, J., Lin, F., et al. (2022). "Kite: exploring the practical threat from acoustic transduction attacks on inertial sensors," in *Proceedings of the 20th ACM conference on embedded networked sensor systems*, 696–709.

Gharibi, M., Boutaba, R., and Waslander, S. L. (2016). Internet of drones. *IEEE Access* 4, 1148–1162. doi:10.1109/access.2016.2537208

Ghribi, E., Khoei, T. T., Gorji, H. T., Ranganathan, P., and Kaabouch, N. (2020). "A secure blockchain-based communication approach for uav networks," in 2020 IEEE International Conference on Electro Information Technology (EIT) (IEEE), 411–415.

Grindley, B., Phillips, K., Parnell, K. J., Cherrett, T., Scanlan, J., and Plant, K. L. (2024). Over a decade of uav incidents: a human factors analysis of causal factors. *Appl. Ergon.* 121, 104355. doi:10.1016/j.apergo.2024.104355

Guo, B., Wang, Z., Yu, Z., Wang, Y., Yen, N. Y., Huang, R., et al. (2015). Mobile crowd sensing and computing: the review of an emerging human-powered sensing paradigm. *ACM Comput. Surv. (CSUR)* 48, 1–31. doi:10.1145/2794400

Gupta, R., Tanwar, S., Tyagi, S., and Kumar, N. (2020). Machine learning models for secure data analytics: a taxonomy and threat model. *Comput. Commun.* 153, 406–440. doi:10.1016/j.comcom.2020.02.008

Gurtu, A., and Johny, J. (2021). Supply chain risk management: literature review. *Risks* 9, 16. doi:10.3390/risks9010016

Habibi, P., Farhoudi, M., Kazemian, S., Khorsandi, S., and Leon-Garcia, A. (2020). Fog computing: a comprehensive architectural survey. *IEEE Access* 8, 69105–69133. doi:10.1109/ACCESS.2020.2983253

Han, K. (2023). Employing automotive security to improve the security of unmanned aerial vehicles. *Front. Commun. Netw.* 4. doi:10.3389/frcmn.2023.1122231

Han, K. H. K., Al Nuaimi Kyusuk Han, E., Al Nuaimi, S. A. B. E., Al Blooshi, R. P. S., and Psiakis, C. Y. Y. (2024). Scalable authenticated communication in drone swarm environment. *J. Internet Technol.* 25, 255–265. doi:10.53106/160792642024032502008

Hannah, J., Mills, R., and Dill, R. (2020). "Traffic collision avoidance system: threat actor model and attack taxonomy," in *2020 new trends in civil aviation (NTCA)* (IEEE), 17–26.

Hassija, V., Chamola, V., Gupta, V., Jain, S., and Guizani, N. (2020). A survey on supply chain security: application areas, security threats, and solution architectures. *IEEE Internet Things J.* 8, 6222–6246. doi:10.1109/jiot.2020.3025775

He, D., Chan, S., and Guizani, M. (2016). Communication security of unmanned aerial vehicles. *IEEE Wirel. Commun.* 24, 134–139. doi:10.1109/mwc.2016.1600073wc

He, D., Chan, S., and Guizani, M. (2017). Drone-assisted public safety networks: the security aspect. *IEEE Commun. Mag.* 55, 218–223. doi:10.1109/MCOM.2017.1600799CM

He, D., Qiao, Y., Chan, S., and Guizani, N. (2018). Flight security and safety of drones in airborne fog computing systems. *IEEE Commun. Mag.* 56, 66–71. doi:10.1109/MCOM.2018.1700916

He, D., Yang, G., Li, H., Chan, S., Cheng, Y., and Guizani, N. (2020). An effective countermeasure against uav swarm attack. *IEEE Netw.* 35, 380–385. doi:10.1109/mnet.011.2000380

Iqbal, W., Abbas, H., Daneshmand, M., Rauf, B., and Bangash, Y. A. (2020). An in-depth analysis of iot security requirements, challenges, and their countermeasures via software-defined security. *IEEE Internet Things J.* 7, 10250–10276. doi:10.1109/jiot.2020.2997651

Jares, G., and Valasek, J. (2021). "Investigating malware-in-the-loop autopilot attack using falsification of sensor data," in 2021 International Conference on Unmanned Aircraft Systems (ICUAS) (IEEE), 1268–1276.

Jin, Y. (2015). Introduction to hardware security. *Electronics* 4, 763–784. doi:10.3390/electronics4040763

Kaushal, R. K., Kumar, N., Singhal, S., Singh, S., and Singh, H. (2022). Locking device for physical protection of electronic devices. *ECS Trans.* 107, 1769–1779. doi:10.1149/10701.1769ecst

Khan, N. A., Jhanjhi, N., Brohi, S. N., Almazroi, A. A., and Almazroi, A. A. (2022). A secure communication protocol for unmanned aerial vehicles. *CMC-COMPUTERS Mater. & CONTINUA* 70, 601–618. doi:10.32604/cmc.2022.019419

Kong, P.-Y. (2021). A survey of cyberattack countermeasures for unmanned aerial vehicles. *IEEE Access* 9, 148244–148263. doi:10.1109/access.2021.3124996

Kopyt, A., and Żugaj, M. (2020). Analysis of pilot interaction with the control adapting system for uav. *J. Aerosp. Eng.* 33, 04020025. doi:10.1061/(asce)as.1943-5525.0001109

Koubâa, A., Qureshi, B., Sriti, M.-F., Allouch, A., Javed, Y., Alajlan, M., et al. (2019). Dronemap planner: a service-oriented cloud-based management system for the internet-of-drones. *Ad Hoc Netw.* 86, 46–62. doi:10.1016/j.adhoc.2018.09.013

Kumar, R., Sayeed, M. A., Sharma, V., and You, I. (2019). "An sdn-based secure mobility model for uav-ground communications," in *Mobile internet security*. Editors I. You, H.-C. Chen, V. Sharma, and I. Kotenko (Singapore: Springer Singapore), 169–179.

Lee, M. W. (2020). Applying cybersecurity and anti-tamper methods for secure operating of unmanned weapon systems. *J. Korean Soc. Syst. Eng.* 16, 36–42. doi:10.14248/JKOSSE.2020.16.1.036

Li, Y., Jeong, Y.-S., Shin, B.-S., and Park, J. H. (2017). Crowdsensing multimedia data: security and privacy issues. *IEEE Multimed.* 24, 58–66. doi:10.1109/mmul.2017.4031306

Li, Z., Lu, Y., Shi, Y., Wang, Z., Qiao, W., and Liu, Y. (2019). A dyna-q-based solution for uav networks against smart jamming attacks. *Symmetry* 11, 617. doi:10.3390/sym11050617

Liu, C., Quek, T. Q., and Lee, J. (2017). "Secure uav communication in the presence of active eavesdropper," in 2017 9th International Conference on Wireless Communications and Signal Processing (WCSP) (IEEE), 1–6.

Lopez, A. B., Vatanparvar, K., Deb Nath, A. P., Yang, S., Bhunia, S., and Al Faruque, M. A. (2017). A security perspective on battery systems of the internet of things. *J. Hardw. Syst. Secur.* 1, 188–199. doi:10.1007/s41635-017-0007-0

Malik, M., and Patel, T. (2016). Database security-attacks and control methods. *Int. J. Inf.* 6, 175–183. doi:10.5121/ijist.2016.6218

McCoy, J., and Rawat, D. B. (2019). Software-defined networking for unmanned aerial vehicular networking and security: a survey. *Electronics* 8, 1468. doi:10.3390/electronics8121468

Mekdad, Y., Aris, A., Babun, L., Fergougui, A., Conti, M., Lazzeretti, R., et al. (2021). A survey on security and privacy issues of uavs. arxiv 2021. *arXiv Prepr. arXiv:2109*. doi:10.48550/arXiv.2109.14442

Mohamed, N., Al-Jaroodi, J., Jawhar, I., Idries, A., and Mohammed, F. (2020). Unmanned aerial vehicles applications in future smart cities. *Technol. Forecast. Soc. change* 153, 119293. doi:10.1016/j.techfore.2018.05.004

Mohsan, S. A. H., Khan, M. A., Noor, F., Ullah, I., and Alsharif, M. H. (2022). Towards the unmanned aerial vehicles (uavs): a comprehensive review. *Drones* 6, 147. doi:10.3390/drones6060147

Mun, H., Han, K., Damiani, E., Kim, T.-Y., Yeun, H. K., Puthal, D., et al. (2024). Privacy enhanced data aggregation based on federated learning in internet of vehicles (IoV). *Comput. Commun.* 223, 15–25. doi:10.1016/j.comcom.2024.05.009

Niyonsaba, S., Konate, K., and Soidridine, M. M. (2023). A survey on cybersecurity in unmanned aerial vehicles: cyberattacks, defense techniques and future research directions. *Int. J. Comput. Netw. Appl.* 10, 688–701. doi:10.22247/ijcna/2023/223417

Oruc, A. (2022). Potential cyber threats, vulnerabilities, and protections of unmanned vehicles. *Drone Syst. Appl.* 10, 51–58. doi:10.1139/juvs-2021-0022

Owoh, N. P., and Singh, M. M. (2022). Security analysis of mobile crowd sensing applications. *Appl. Comput. Inf.* 18, 2–21. doi:10.1016/j.aci.2018.10.002

Pan, W. J., Xu, Y. X., and Wang, J. K. (2022). "Research on tcas warning factors between transportation and training flights using monte-carlo simulation," in 2022 2nd International Conference on Big Data Engineering and Education (BDEE) (IEEE), 115–119.

Pandey, G. K., Gurjar, D. S., Nguyen, H. H., and Yadav, S. (2022). Security threats and mitigation techniques in uav communications: a comprehensive survey. *IEEE Access* 10, 112858–112897. doi:10.1109/access.2022.3215975

Pendleton, M., Garcia-Lebron, R., Cho, J.-H., and Xu, S. (2016). A survey on systems security metrics. *ACM Comput. Surv. (CSUR)* 49, 1–35. doi:10.1145/3005714

Plooij, M., Mathijssen, G., Cherelle, P., Lefeber, D., and Vanderborght, B. (2015). Lock your robot: a review of locking devices in robotics. *IEEE Robotics & Automation Mag.* 22, 106–117. doi:10.1109/MRA.2014.2381368

Podhradsky, M., Coopmans, C., and Hoffer, N. (2017). "Improving communication security of open source uavs: encrypting radio control link," in 2017 International Conference on Unmanned Aircraft Systems (ICUAS) (IEEE), 1153–1159.

Prasetia, A. S., Wai, R.-J., Wen, Y.-L., and Wang, Y.-K. (2019). Mission-based energy consumption prediction of multirotor uav. *IEEE Access* 7, 33055–33063. doi:10.1109/access.2019.2903644

Pundir, S., Wazid, M., Singh, D. P., Das, A. K., Rodrigues, J. J., and Park, Y. (2019). Intrusion detection protocols in wireless sensor networks integrated to internet of things deployment: survey and future challenges. *IEEE Access* 8, 3343–3363. doi:10.1109/access.2019.2962829

Rabie, O. B. J., Selvarajan, S., Hasanin, T., Alshareef, A. M., Yogesh, C., and Uddin, M. (2024). A novel iot intrusion detection framework using decisive red fox optimization and descriptive back propagated radial basis function models. *Sci. Rep.* 14, 386. doi:10.1038/s41598-024-51154-z

Rahman, M. A., Rahman, M. T., Kisacikoglu, M., and Akkaya, K. (2020). "Intrusion detection systems-enabled power electronics for unmanned aerial vehicles," in *2020 IEEE CyberPELS (CyberPELS)*, 1–5.

Rao, V. V., Marshal, R., and Gobinath, K. (2021). "The iot supply chain attack trends-vulnerabilities and preventive measures," in 2021 4th International Conference on Security and Privacy (ISEA-ISAP) (IEEE), 1–4.

Rodday, N. M., Schmidt, R. d. O., and Pras, A. (2016). "Exploring security vulnerabilities of unmanned aerial vehicles," in *NOMS 2016-2016 IEEE/IFIP Net. Opera. Manag. Sympo. (IEEE)*, 993–994.

Rugo, A., Ardagna, C. A., and Ioini, N. E. (2022). A security review in the uavnet era: threats, countermeasures, and gap analysis. *ACM Comput. Surv. (CSUR)* 55, 1–35. doi:10.1145/3485272

SAE International (2020). SAE-J3101: hardware protected security for ground vehicles. *Tech. Rep*. Available at: https://www.sae.org/standards/content/j3101_202002/

Sedjelmaci, H., Senouci, S. M., and Messous, M.-A. (2016). "How to detect cyber-attacks in unmanned aerial vehicles network?," in 2016 IEEE Global Communications Conference (GLOBECOM) (IEEE), 1–6.

Seerangan, K., Nandagopal, M., Govindaraju, T., Manogaran, N., Balusamy, B., and Selvarajan, S. (2024). A novel energy-efficiency framework for uav-assisted networks using adaptive deep reinforcement learning. *Sci. Rep.* 14, 22188. doi:10.1038/s41598-024-71621-x

Selvarajan, S. (2024). A comprehensive study on modern optimization techniques for engineering applications. *Artif. Intell. Rev.* 57, 194. doi:10.1007/s10462-024-10829-9

Selvarajan, S., Manoharan, H., Khadidos, A. O., Khadidos, A. O., Shankar, A., Maple, C., et al. (2024). Generative artificial intelligence and adversarial network for fraud detections in current evolutional systems. *Expert Syst.* 42, e13740. doi:10.1111/exsy.13740

Shafique, A., Mehmood, A., and Elhadef, M. (2021). Detecting signal spoofing attack in uavs using machine learning models. *IEEE Access* 9, 93803–93815. doi:10.1109/ACCESS.2021.3089847

Shaikh, E., Mohammad, N., and Muhammad, S. (2021). "Model checking based unmanned aerial vehicle (uav) security analysis," in 2020 International Conference on Communications, Signal Processing, and their Applications (ICCSPA) (IEEE), 1–6.

Shakhov, V., and Koo, I. (2018). Depletion-of-battery attack: specificity, modelling and analysis. *Sensors* 18, 1849. doi:10.3390/s18061849

Sidharthan, S., Ashok, A., and Bourgeois, A. (2021). "Internet service via uav: user centric comprehensive attack surface analysis," in *Proceedings of the 12th ACM wireless of the students, by the students, and for the students (S3) workshop*, 1–2.

Singh, M., Leu, P., Abdou, A., and Capkun, S. (2019). "UWB-ED: distance enlargement attack detection in Ultra-Wideband," in *28th USENIX security symposium (USENIX security 19)* (Santa Clara, CA: USENIX Association), 73–88.

Spyros, A. (2022). *A study of cybersecurity threats in UAVs and threat model approaches*. Greece: International Hellenic University. Master's thesis.

Stracquodaine, C., Dolgikh, A., Davis, M., and Skormin, V. (2016). "Unmanned aerial system security using real-time autopilot software analysis," in 2016 International Conference on Unmanned Aircraft Systems (ICUAS) (IEEE), 830–839.

Suhag, D., and Jha, V. (2023). A comprehensive survey on mobile crowdsensing systems. *J. Syst. Archit.* 142, 102952. doi:10.1016/j.sysarc.2023.102952

Taggu, A., and Marchang, N. (2019). "Random-byzantine attack mitigation in cognitive radio networks using a multi-hidden markov model system," in 2019 International Conference on Electrical and Computing Technologies and Applications (ICECTA) (IEEE), 1–5.

Tan, L., Pan, Y., Wu, J., Zhou, J., Jiang, H., and Deng, Y. (2020). A new framework for ddos attack detection and defense in sdn environment. *IEEE access* 8, 161908–161919. doi:10.1109/access.2020.3021435

Tlili, F., Fourati, L. C., Ayed, S., and Ouni, B. (2022). Investigation on vulnerabilities, threats and attacks prohibiting uavs charging and depleting uavs batteries: assessments & countermeasures. *Ad hoc Netw.* 129, 102805. doi:10.1016/j.adhoc.2022.102805

Trusted Computing Group (2024). Trusted platform module library part 1: architecture. Available at: https://trustedcomputinggroup.org/resource/tpm-library-specification/.

Vosatka, J. (2018). Introduction to hardware trojans. *Hardw. Trojan War Attacks, Myths, Defenses*, 15–51. doi:10.1007/978-3-319-68511-3_2

Wang, D., Fan, T., Han, T., and Pan, J. (2020). A two-stage reinforcement learning approach for multi-uav collision avoidance under imperfect sensing. *IEEE Robotics Automation Lett.* 5, 3098–3105. doi:10.1109/lra.2020.2974648

Wang, D., Li, S., Xiao, G., Liu, Y., and Sui, Y. (2021). "An exploratory study of autopilot software bugs in unmanned aerial vehicles," in *Proceedings of the 29th ACM joint meeting on European software engineering conference and symposium on the foundations of software engineering*, 20–31.

Wu, K., Tian, B., and Wang, X. (2023). "Data security storage scheme for uav cluster based on distributed storage," in 2023 International Conference on Networking and Network Applications (NaNA) (IEEE), 13–17.

Xu, S., Tu, H., and Xia, Y. (2023). Resilience enhancement of renewable cyber–physical power system against malware attacks. *Reliab. Eng. & Syst. Saf.* 229, 108830. doi:10.1016/j.ress.2022.108830

Yahuza, M., Idris, M. Y. I., Ahmedy, I. B., Wahab, A. W. A., Nandy, T., Noor, N. M., et al. (2021). Internet of drones security and privacy issues: taxonomy and open challenges. *IEEE Access* 9, 57243–57270. doi:10.1109/access.2021.3072030

Yang, K., Zhang, K., Ren, J., and Shen, X. (2015). Security and privacy in mobile crowdsourcing networks: challenges and opportunities. *IEEE Commun. Mag.* 53, 75–81. doi:10.1109/mcom.2015.7180511

Yasin, J. N., Mohamed, S. A., Haghbayan, M.-H., Heikkonen, J., Tenhunen, H., and Plosila, J. (2020). Unmanned aerial vehicles (uavs): collision avoidance systems and approaches. *IEEE access* 8, 105139–105155. doi:10.1109/access.2020.3000064

Yassine, M., Youssef, Q., EL Gholami, K., Sadqi, Y., and Mounir, S. (2022). A comprehensive survey on sdn security: threats, mitigations, and future directions. *J. Reliab. Intelligent Environ.* 9, 201–239. doi:10.1007/s40860-022-00171-8

Yuvaraj, R., and Velliangiri, S. (2023). "A comprehensive study on unmanned aerial vehicle security issues," in 2023 IEEE 5th International Conference on Cybernetics, Cognition and Machine Learning Applications (ICCCMLA) (IEEE), 544–550.

Zhang, G., Wu, Q., Cui, M., and Zhang, R. (2017). "Securing uav communications via trajectory optimization," in GLOBECOM 2017-2017 IEEE Global Communications Conference (IEEE), 1–6.

Zhang, K. (2023). A wormhole attack detection method for tactical wireless sensor networks. *PeerJ Comput. Sci.* 9, e1449. doi:10.7717/peerj-cs.1449

Zhao, M., Chen, Y., Zhou, X., Zhang, D., and Nie, Y. (2022). Investigation on falling and damage mechanisms of uav illuminated by hpm pulses. *IEEE Trans. Electromagn. Compat.* 64, 1412–1422. doi:10.1109/temc.2022.3187017