

Article

A Survey on Reputation Systems for UAV Networks

Simeon Ogunbunmi ¹, Yu Chen ^{1,*}, Erik Blasch ² and Genshe Chen ³¹ Department of Electrical & Computer Engineering, Binghamton University, Binghamton, NY 13902, USA; sogunbu1@binghamton.edu² Air Force Research Laboratory, Arlington, VA 22203, USA; erik.blasch.1@us.af.mil³ Intelligent Fusion Technology, Inc., Germantown, MD 20874, USA; gchen@intfusiontech.com

* Correspondence: ychen@binghamton.edu

Abstract: The proliferation of unmanned aerial vehicle (UAV) networks is increasing, driven by their capacity to deliver automated services tailored to the varied demands of numerous smart city applications. Trust, security, and privacy remain paramount in the public domain. Traditional centralized network designs fall short of ensuring device authentication, data integrity, and privacy within the highly dynamic and adaptable environments of UAV networks. Decentralized reputation systems have emerged as a promising solution for enhancing the reliability and trustworthiness of data and communications within these networks while safeguarding UAV security. This paper presents an exhaustive survey of trust and reputation systems, exploring existing frameworks and proposed innovations alongside their inherent challenges. The crucial role of reputation systems is to strengthen trust, security, and privacy throughout these networks, and various strategies can be incorporated to mitigate existing vulnerabilities. As a useful resource for researchers and practitioners seeking to advance the state of the art in UAV network security, we hope this survey will spark further community discussion and stimulate innovative ideas in this burgeoning field.

Keywords: reputation system; unmanned aerial vehicle (UAV); trust; security; feedback system



Citation: Ogunbunmi, S.; Chen, Y.; Blasch, E.; Chen, G. A Survey on Reputation Systems for UAV Networks. *Drones* **2024**, *8*, 253. <https://doi.org/10.3390/drones8060253>

Academic Editor: Petros S. Bithas

Received: 30 April 2024

Revised: 29 May 2024

Accepted: 6 June 2024

Published: 8 June 2024



Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

In the past decades, unmanned aerial vehicles (UAVs), often called drones, have become very popular and useful in various sectors, such as package delivery [1]. UAV technology has changed how society collects information in various applications, ranging from military [2], public safety [3], delivery [4], agriculture [5], healthcare [6], security [7], to disaster response [8]. Moreover, UAV applications extend to smart cities, which have played a vital role in enhancing urban management and public services. Smart cities strive to revolutionize how people move within and across urban spaces to create more efficient, sustainable, and accessible transportation networks, meeting the 2030 sustainable development goals [9]. UAVs equipped with cameras and sensors can monitor traffic patterns in real time to capture data on congestion, road closures, and accidents. UAVs can monitor traffic flow, detect congestion, and optimize routes, which helps reduce travel times and enhance overall transportation efficiency. By 2028, up to 36.5% of drone fleet deployments will be driven by smart city applications [10]. These examples underscore the increasing importance of UAV networks in optimizing urban living and resource management in smart cities. The ability of UAVs to operate autonomously without human intervention can transform traditional operational paradigms, enabling them to efficiently perform complex tasks in diverse and challenging environments.

One crucial thing about UAVs is their ability to work independently without being controlled by humans or pilots. UAV autonomous control is a different challenge versus autonomous ground-based vehicle control, as UAVs conduct challenging tasks in extreme environments like disaster recovery scenarios, where it is necessary to collect on-site

real-time information, transfer the data to the ground controls, and orchestrate resource allocation in different places, from cities to areas affected by disasters [11].

At the core of UAV systems' effectiveness lies the seamless communication infrastructure that facilitates connectivity between UAVs, ground control stations, and, in some special situations, satellites [8], as shown in Figure 1. A data link is essential for timely communication and is pivotal for delay-sensitive tasks. UAVs use wireless technology to communicate, which allows them to send and receive data in places that are either difficult to access or hazardous for human operators [12].

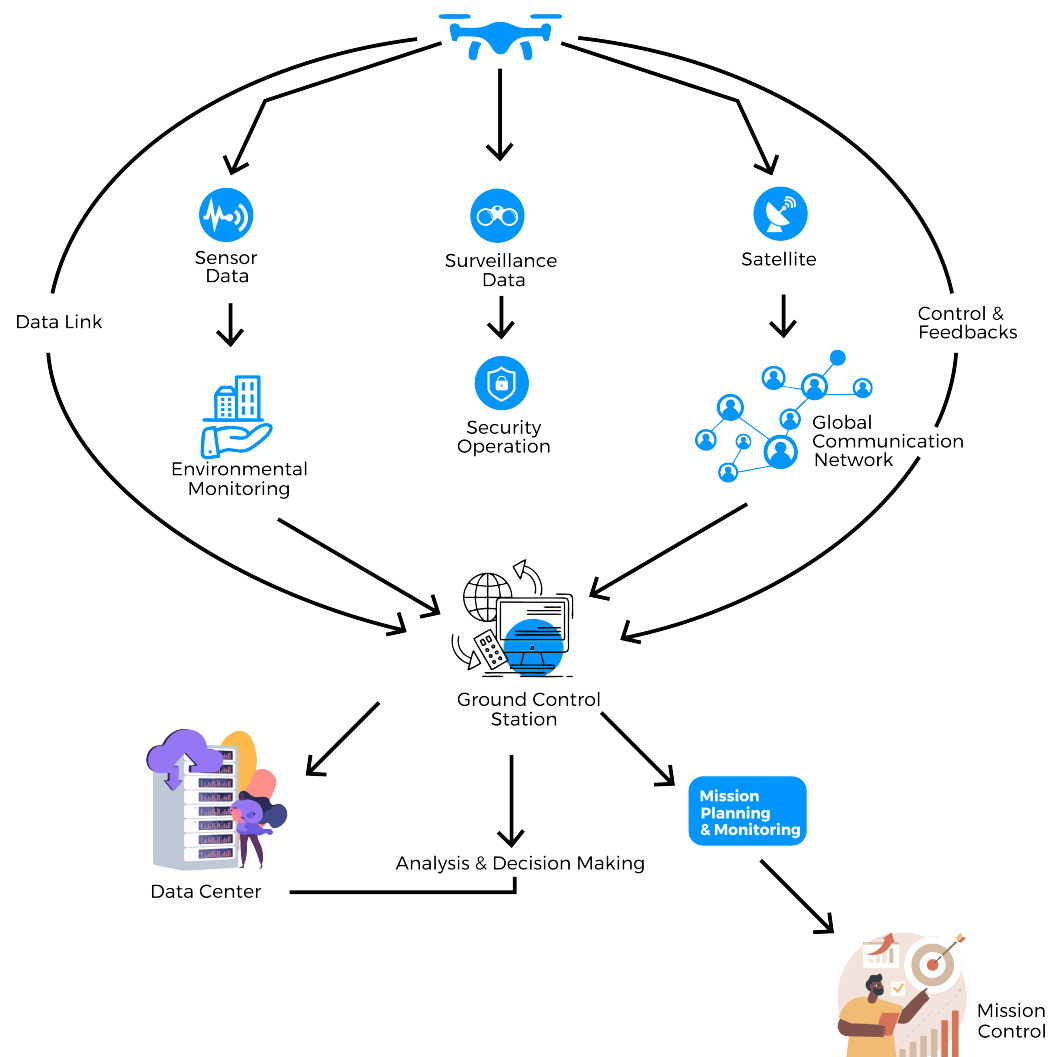


Figure 1. Illustration of UAV communication infrastructure.

While UAVs offer many advantages regarding safety, efficiency, and convenience, they also bring challenges. Security, reliability, trust, and privacy are among the foremost concerns. UAVs can easily be damaged or hacked because of their limited storage and battery power. The chips and sensors in a UAV can be taken advantage of by malicious individuals, potentially leading to unauthorized access and data breaches [13]. Therefore, it is imperative to address the security requirements of UAVs comprehensively, particularly as their applications continue to expand and diversify [14,15]. In many security-critical applications, UAVs fall short of providing robust data protection measures, leading to the potential for significant financial losses or even life-threatening risks [13]. Thus, there is an urgent need to develop robust security protocols and mechanisms to safeguard UAV networks from various threats [16].

Trust, a subjective notion, varies from person to person and from service to service, impacted by personal experiences, cultural background, and individual opinions [4]. It is inextricably linked to risk perception since trust minimizes the perceived hazards of online interactions. A user's past engagements, the quality of their contributions, the legitimacy of their information, and the regularity of their conduct all impact their trust in UAV devices [17]. Devices with a good reputation are viewed as more trustworthy, promoting a feeling of dependability based on their track record.

Trust plays a significant role in guaranteeing the safe and consistent functioning of UAVs [18]. Various algorithms and metrics are utilized to assess the trustworthiness of individuals, aiding users in making informed decisions about whom to trust and engage with by evaluating their actions, comments, and interactions with others [19]. These measurements are essential aids in grasping and effectively utilizing complex UAV systems. Furthermore, online platforms linking UAV service providers with clients utilize rating systems to display the providers' reputation [20], which helps customers choose operators whom they can trust. Users can rate UAV operators and service providers, assessing their service quality, task efficiency, and professionalism. A reputation platform rating has an impact on UAV operators' qualifications.

A high reputation score within a UAV ecosystem has various benefits, including enhanced access rights, motivating individuals to contribute positively, and maintaining their trust level [21]. Consistent rendering and providing of trustworthy service and deliveries enables service requesters to have more transactions performed by service providers, thereby increasing the trustworthiness and reputation of the providers [22]. Meanwhile, delivering poor quality work or a low task completion rate will ruin one's reputation score [23]. However, by making worthwhile contributions to the system and providing non-malicious service, reputation scores can be restored [24].

Feedback plays a significant role in maintaining the safety and compliance of UAVs and other Internet of Things (IoT) devices, emphasizing its importance. Notifying regulatory agencies and organizations about safety incidents and violations increases the chances of preemptively mitigating risks. Feedback helps improve the accuracy and reliability of the data collected by UAVs [25]. By consistently offering quality data, users can cultivate a positive image and gain recognition within the UAV community. Collaboratively, the communities of UAV pilots and enthusiasts work together to exchange valuable information. Reputation systems acknowledge experienced members and incentivize them to mentor and impart their knowledge to others [26].

Paper Selection and Review Process

Our extensive analysis elucidates the challenges, solutions, and future directions that will shape UAV technology's reliable and secure integration across various applications while maintaining their trustworthiness. This paper aims to provide valuable insights into the evolving dynamics of UAV systems in an era where they are poised to revolutionize industries. As illustrated in Figure 2, we present an overview of the multifaceted landscape of UAV systems, focusing on security, reputation, and trust, by addressing these critical issues through the following research questions:

- *What are the primary vulnerabilities affecting current UAV reputation systems?*
- *How do various reputation management approaches mitigate these vulnerabilities?*
- *Which future research directions are suggested by current findings in UAV reputation systems?*

To provide an overview of reputation systems in the context of UAV networks, 96 papers were selected, as shown in Table 1, published from 2006 to April 2024. Figures 3 and 4 present the distribution of these papers in terms of publication time and category.

The rest of this paper is structured and organized as follows: Section 2 presents the different classes and types of available UAV devices. Section 3 gives a glimpse of the various trust and reputation management methods that have been proposed. Section 4 describes background knowledge on UAVs and reputation systems, and a survey on reputation and trust systems is introduced. Section 5 presents a taxonomy for both trust

and reputation systems, and the solutions are discussed in Section 6. Finally, Section 7 provides the conclusions and future directions.

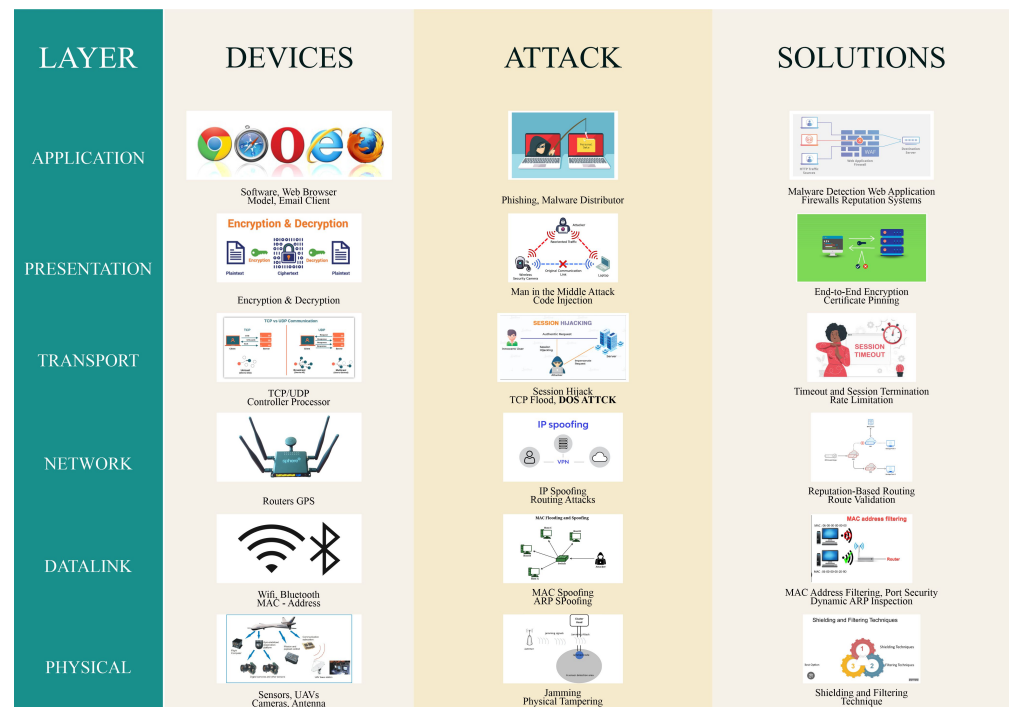


Figure 2. Multifaceted landscape of trust, reputation, and security.

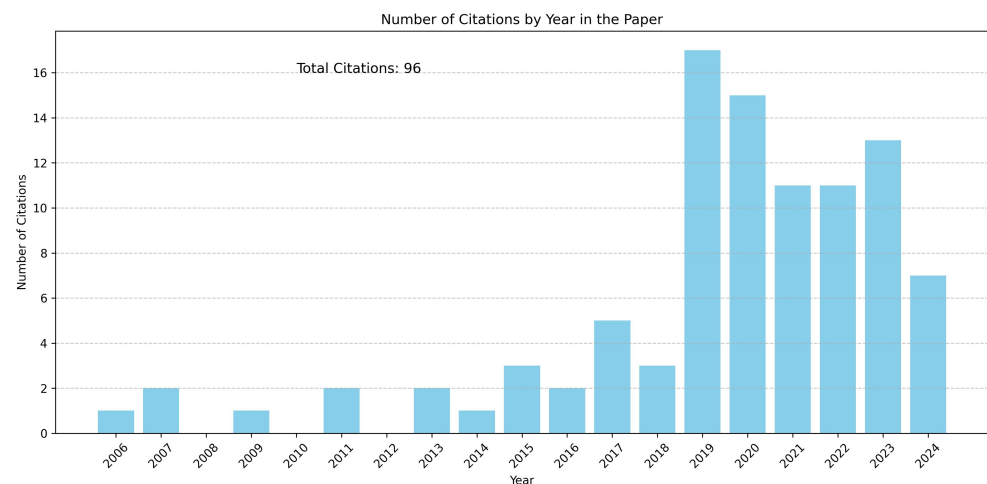


Figure 3. Distribution of selected papers by publishing time.

Table 1. Categories of papers.

Category	Papers
Security	[2,3,7–12,14,15,22,24,27–53].
Trust	[1,4–6,13,17,18,20,25,29,35,36,40,46,49,54–67].
Reputation	[4,13,16,17,19–24,26,31,33,49,53–56,63–65,68–77].
General	[78–83]

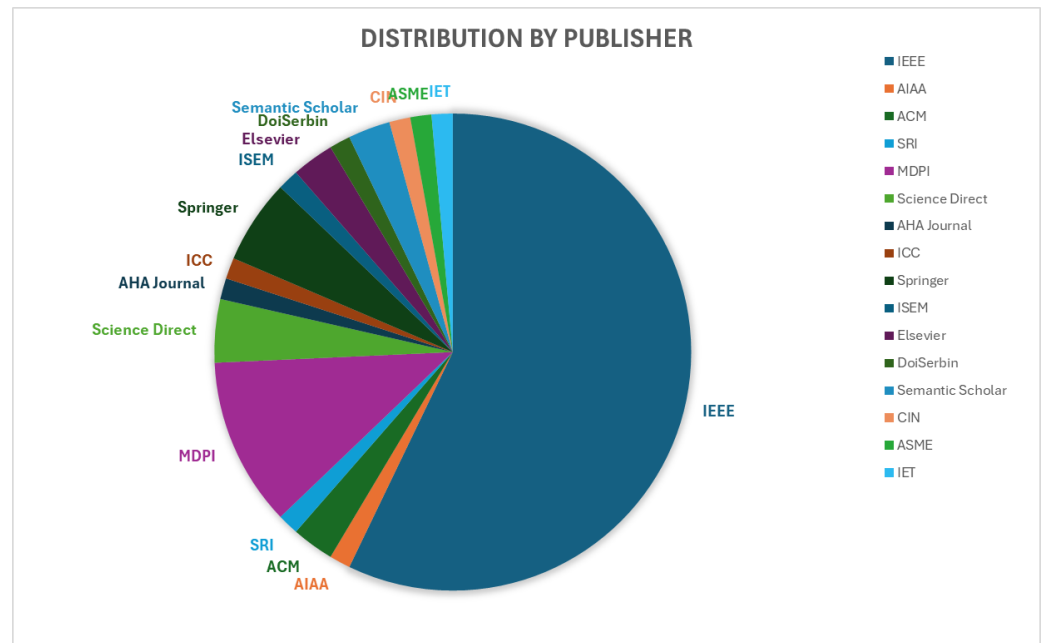


Figure 4. Distribution of selected papers by publishers.

2. Classes/Types of UAV Devices

There are various types and classes of UAVs or UAV systems based on their unique design, flight types, capacities, and applications. They can be organized into three classes: single-rotor UAVs, multi-rotor UAVs, and fixed-wing UAVs.

2.1. Single-Rotor UAVs

Single-rotor UAVs only have one rotor. One of the primary characteristics that distinguishes single-rotor UAVs is their exceptional agility and mobility [78]. The single-rotor structure enables superb lift and directional control, allowing varieties of aerobatic performance and swift turns. A high agility gives them the ability to hover, which other types of UAVs would find difficult to emulate. However, their extensive capabilities require greater piloting abilities and experience, distinguishing them from more accessible and user-friendly multi-rotor UAVs. These distinguishing features make them a preferable option for experts and professionals for certain specific applications, including aerial mapping and surveying, aerial surveillance and patrol, heavy payload delivery, and search and rescue operations.

2.2. Multi-Rotor UAVs

UAVs with several rotors with fixed-pitch spinning blades to produce lift and thrust are called multi-rotor UAVs or multi-copters. Multi-rotor UAVs may rise, hover, drop, move in different directions, and carry out a variety of other maneuvers by varying the speed of these rotors [79]. They are adaptable and have uses in a wide range of industries, including deliveries, mapping and surveying, aerial photography and videography, search and rescue missions, surveillance and inspection, asset inspection, crop monitoring, and short-range product delivery.

The classification of multi-rotor UAVs is based on their number of rotors: quad-copters have four rotors, hexa-copters have six, and octocopters have eight [80]. An application's specific requirements determine the configuration used. While hexacopters and octocopters are more stable and have larger payload capacities, making them ideal for commercial and industrial applications, quad-copters are popular due to their ease of operation—conditions such as weather, UAV size, weight, and payload influence flight durations. Thanks to the continuous improvement in battery life, obstacle avoidance, cameras, and user-friendly controls, multi-rotor UAVs are now more accessible, dependable, and powerful.

Multi-rotor UAVs are controlled by a radio transmitter and fitted with gyroscopes, accelerometers, and barometers to maintain stability, detect acceleration, and provide altitude data. Certain versions are equipped with autopilot systems that allow for autonomous flight. These systems provide various functionalities, such as way-point navigation and the ability to return to the designated home location.

2.3. Fixed Wing UAVs

Fixed-wing UAVs are designed with one or two wings, similar to traditional UAVs, in contrast to multi-rotor UAVs. These UAVs are known for their efficiency and swiftness [81]. Fixed-wing UAVs are perfect for activities requiring them to quickly cover wide areas, because they are faster than multi-rotor UAVs. Through the implementation of an aerodynamic configuration, these aircraft are capable of achieving energy conservation and prolonged flight durations, sometimes for several hours, before needing refueling or recharging [27]. However, their takeoff and landing requirements are one of the main differences between fixed-wing and multi-rotor UAVs. Fixed-wing UAVs require more space for these movements, frequently requiring runways or open areas, which limits their usability in settings within a narrow space.

Fixed-wing UAVs have a wide range of applications where their speed and durability are useful. Their proficiency in covering vast regions quickly, such as for crop monitoring or topographical surveys, makes them ideal for activities like aerial photography, mapping, surveying, aerial mapping and surveying, asset inspection, long-range payload delivery, and unmanned aerial refueling. They have also established themselves in the long-distance package delivery market, especially in isolated or rural locations.

3. An Overview of Trust And Reputation Systems in UAV Networks

UAVs have become an indispensable technology today, with a wide range of applications across military, commercial, agricultural, healthcare, and security sectors. One of the most significant benefits of UAV systems is their ability to operate autonomously, without requiring a human pilot onboard. UAV autonomy has revolutionized surveillance and information gathering in both civilian and state air domains. UAVs maintain connectivity through a data link that bridges the vehicles with ground stations and extends from the ground controller to satellites, bolstering the UAV communication network. With minimal latency, UAVs use wireless communications to transmit data and information efficiently. Moreover, these vehicles excel at delivering crucial data in disaster-affected areas or regions with poor terrestrial network infrastructure, facilitating immediate communication with ground stations or controllers. In surveillance and monitoring, UAVs enhance operational efficiency by ensuring seamless communication between network nodes and ground controllers, highlighting their invaluable role in modern surveillance and monitoring operations.

3.1. A Brief Overview

Although UAV applications have demonstrated outstanding potential to enhance community safety and comfort, they could also have disastrous consequences if UAV networks are compromised and utilized improperly. Due to inherent resource constraints, UAVs are vulnerable to physical and digital attacks. The limited storage and battery capacity of UAVs can make it easier for attackers to hack and interfere with the chips and sensors embedded inside a UAV's circuit, potentially allowing them to obtain the stored data if the necessary precautions are not taken. To address these concerns, various research studies have been conducted on the reputation systems of UAV networks, and a series of models have been proposed to mitigate the issues and challenges related to trust and reputation systems in these networks.

Trust and reputation in various sectors have been discussed in the research community. The challenges and issues related to trust and reputation systems have been discussed, including unfair ratings, lack of incentives for rating providers, and the difficulty of schol-

arly ideas [4]. Research agendas for trust and reputation systems have been suggested to examine current trends and advancements, highlighting the necessity of finding appropriate online alternatives to conventional cues for reputation and trust, identifying pertinent information for determining reputation and trust measures and creating effective mechanisms for gathering and determining these metrics. As further evidence of the acceptance and acknowledgment of reputation systems in practical contexts, their use in profitable commercial web applications has been discussed [4]. It is acknowledged that commercial implementations tend to decide on relatively simple schemes, whereas academic proposals are frequently centered on advanced features.

In an Internet of Things (IoT) middleware survey, the significance of trust in security, privacy, usability, and user experience was highlighted [28]. A trust-based, privacy-protected method for promoting nodes in social online networks was proposed [29]. For devices with limited resources, a trust model was created that included a privacy-preserving methodology to assess trust and increase immunity to malevolent users [25]. For determining service reputation, a two-phase procedure was suggested [68], while a survey that focuses on enforcement principles for tackling quality of service (QoS) and quality of experience (QoE) guarantee challenges in cloud computing was conducted in [30]. There is a need for specific models adapted to the particular difficulties of the IoT. These works offer insights into trust and reputation evaluation in various scenarios.

Analytical frameworks for reputation systems allow the framework to decompose, analyze, and compare reputation systems using a standard set of metrics [31]. They facilitate comparisons within a single framework and offer insights into the advantages and disadvantages of various systems. The above paper also examined the system components susceptible to each attack category and class assaults against reputation systems [31]. In addition, the paper examined extant defense mechanisms for reputation systems and their applicability to various system components.

The drawbacks of current trust architectures and reputation assessment techniques were addressed in [54]. As an innovative method of managing trust in the IoT, they created the IoTrust architecture. A cross-layer authorization procedure is included in this architecture, which also effortlessly integrates software-defined network (SDN) technologies. The IoTrust protocol's major goal is to restrict access to malicious tags and permit and record all interactions with tags so that their reputation can be assessed.

A flexible and universal architecture is required to manage trust in the dynamic IoT context. IoTrust, a trust architecture incorporating SDN into the IoT, offers a novel method of managing trust by incorporating a cross-layer authorization protocol [54]. It established an organization reputation evaluation scheme (ORES) and a behavior-based reputation evaluation scheme for the node (BES), to build trust [55]. The effectiveness of BES and ORES was confirmed through theoretical analysis and simulation findings.

3.2. Trust in UAVs

Regarding UAVs, trust can be denoted as the confidence service providers have in a UAV system's capability to perform tasks securely and reliably and to enhance the integrity of the data sent over the network. UAVs must consistently perform their assigned tasks with high accuracy and dependability. This includes maintaining stable communication links, proper navigation, and successful mission execution, thereby enhancing the system's reliability [56]. This builds confidence in the technology's ability to meet expectations and perform under diverse circumstances. Trust is enhanced when entities regard UAV operations as being carried out with integrity and honesty and in the best interests of society. Trust may be effectively established and sustained in UAV networks by ensuring their reliability, security, safety, transparency, and adherence to ethical standards, enabling successful integration into diverse applications [5].

3.3. Security and Privacy in UAVs

Ensuring security and privacy in UAV networks is crucial for effectively integrating and using these systems in varied applications. Security measures are implemented to safeguard UAV systems and their data from unauthorized access, cyber-attacks, and other threats [84]. Security centers on two crucial elements: data transmissions are encrypted to prevent unwanted reading, and authentication methods are used to verify the identities of UAVs and operators [32], thus preventing unauthorized access [33]. Intrusion detection systems (IDS) enhance security by monitoring network traffic for anomalous behavior and triggering defensive actions upon detecting potential threats. Securing communication channels is crucial for maintaining the security and integrity of data shared within the UAV network, protecting it from external threats.

Privacy in UAV networks entails protecting confidential data gathered and sent by UAVs from unauthorized intrusion and attack [25]. Privacy measures encompass techniques such as data anonymization, safe storage solutions, and policies that regulate data access and exchange. These procedures guarantee the protection of personal and proprietary information following legal and ethical standards. UAV networks can earn the trust of stakeholders by establishing strong security and privacy rules, which ensure the integrity and confidentiality of data [34]. Establishing this trust is essential for extensively implementing UAV technology in various fields, including commercial delivery, critical infrastructure monitoring, and public safety missions.

3.4. Novelty of this Survey

While numerous survey papers have extensively covered the security and privacy aspects of UAV networks [12,84–86], there is a distinct need for a comprehensive overview addressing reputation systems within UAV networks. Our paper fills this gap by exclusively focusing on the mechanisms and frameworks that establish and maintain trust and reputation in UAV networks. Our work differs from existing surveys, as they primarily address broad security concerns in general. Here, we carefully examine the design details of reputation systems for defense against attacks to further improve safety in UAV operations. Existing works often overlooked the subtle differences in reputation-system-specific challenges and solutions, such as how to deal with malicious nodes influencing trust metrics or integrating decentralized approaches like blockchain. As we focus on these aspects, this survey not only covers the research areas complementary to existing surveys but also provides practical insights and target problems for improving trust and reputation in UAV networks. This rigor within a focused area of interest makes our paper stand out as an essential reference for researchers and practitioners working to make UAV systems more trustworthy and capable.

4. Survey On UAV Reputation, Trust, and Feedback Systems

Sections 4–6 together provide a comprehensive view of the landscape for UAV network trust, reputation, and feedback systems, discussing the systems, presenting a taxonomy of attacks, and illustrating defense mechanisms.

4.1. Trust

Trust is a subjective term that differs from person to person [4]. What one user deems trustworthy, another may not, depending on personal experiences, cultural situations, and individual viewpoints. A user's prior interactions, the quality of their contributions, the authenticity of their information, and their consistency in behavior may all influence trust in UAV devices. Devices with higher trust levels are typically perceived as more trustworthy since their track record suggests that they provide non-malicious services and are reliable [4]. When members of an online community trust one another, they are more inclined to engage in transactions, collaborations, and interactions without fear of negative consequences. Trust reduces the perceived danger of communicating with unknown persons in an online setting [35].

A novel malicious node detection method, enhanced reputation calculation, involvement of a distributed trust concept in calculations, and overall performance improvements were proposed as a result of the challenges in unmanned aerial vehicle ad hoc network (UAANET) research, which include the lack of security and trustworthiness, resource over-usage, energy consumption, memory constraints, and preventing selfish node attacks [57]. These challenges were addressed to achieve a fully trusted network in UAANET. A trust-based distributed technique was introduced for UAANET using the hidden Markov model (HMM) to address security and trust issues, including preventing selfish node attacks [57].

Moreover, a trust-based security scheme for 5G UAV communication systems was proposed, which addresses the need to manage the reliability of UAVs, detect malicious attacks, and improve the quality of communication in the face of increasing interference and security threats [36]. The proposed model manages the reliability of UAVs, detects malicious attacks, and improves communication quality amid increasing interference and security threats. This trust-based security scheme and detection scheme based on Q-learning technology aims to address these challenges by filtering out malicious UAVs and enhancing security performance [36].

A lightweight asynchronous provable Byzantine fault-tolerant consensus mechanism for UAV networks, which incorporates a blockchain monitoring system for assessing node trustworthiness, a clustering algorithm for optimizing network coverage, and a consensus algorithm for achieving multi-valued Byzantine consensus, was proposed in [37]. The proposed solution aims to reduce communication overheads, computational complexity, and storage requirements in resource-constrained UAV networks, leading to improved throughput, consensus latency, and energy consumption compared to existing algorithms. The main challenges in establishing a lightweight and efficient consensus-based UAV trusted network include the Byzantine environment, the asynchronous nature of the UAV network, and resource constraints [37]. These challenges impact the ability to sense node state changes in real-time, accurately identify untrustworthy nodes, and effectively reach consensus in resource-constrained UAV networks.

Users may earn trust by consistently performing and contributing in favorable ways. Ethical behavior, transparency, and keeping promises may all help to develop trust. Negative encounters, dishonesty, or breaches of community standards can all undermine or harm trust [18]. Repeated instances of dishonest behavior can lead to a partial or complete loss of trust and a deterioration in the reputation score of the service providers. Several platforms utilize trust metrics or algorithms to measure and quantify trustworthiness based on user behavior, comments, and interactions. These metrics can assist users in making educated choices about who they can trust and engage with. There are various types and classes of trust systems, which include the following:

4.1.1. Reliability Trust

The ability to be accountable and consistently perform and deliver the service, promises, and commitments they claim to render establishes reliability and trust. This ensures trustworthiness and enhances dependability, which is essential in building and maintaining relationships between different entities. For example, Alice is said to exhibit reliability and trust when she delivers and fulfills the promises made to Bob. This refers to the confidence in someone's ability to deliver on their promises or fulfill their obligations consistently [4]. It is the belief that they will act dependably and competently. In UAVs, reliability trust is confidence in a UAV's ability to consistently perform its designated tasks without malfunctioning or encountering technical difficulties [13]. The reliability of UAV devices is enhanced by their consistency and accuracy in delivering packages within a designated time frame. In addition, factors like flight history with minimal technical issues, redundant systems (e.g., backup batteries) to ensure mission completion in case of failure, reliable communication systems, robust hardware and software, and consistent performance in diverse weather conditions further strengthen this trust.

4.1.2. Decision Trust

Decision trust is the extent to which one party is willing to depend on something or somebody in a given situation with a feeling of relative security, even though negative consequences are possible [4,13]. Moreover, it is the confidence, belief, and trust that individuals have in the decisions made by others. Decision trust focuses on the ability to make optimal choices in critical and dynamic situations, particularly when flying in autonomous flight modes. Decision trust in UAV systems is essential for the widespread acceptance and adoption of UAV technology across various domains [69]. Many UAVs are equipped with some level of autonomy, meaning they can make decisions based on sensor data and pre-programmed algorithms. Trust in these decisions is crucial. Transparent decision-making algorithms, rigorous testing of autonomous functions, and a clear understanding of the UAV's limitations are all essential for building decision trust.

Moreover, “decision trust” refers to the level of confidence or belief that stakeholders, such as operators, regulators, and the public, have in the UAV's decisions or associated systems. Since UAVs often operate autonomously or semi-autonomously, their decision-making capabilities are crucial in ensuring safe and effective mission execution [18]. Decision trust is linked to the reliability and performance of UAV systems. Service providers or operators must trust that UAVs will operate as intended and make sound decisions, even in challenging or unpredictable environments. In smart agriculture, there is trust in UAVs to accurately and consistently collect and analyze data related to crop health, soil conditions, irrigation, and other factors to maximize yields and optimize farming practices and productivity.

4.1.3. Behavioral Trust

Behavioral trust refers to the trust that is inferred or assessed based on observable behaviors, actions, and interactions rather than solely on explicit declarations or promises. It is the trust that individuals develop in others over time through repeated interactions, consistent behavior, and demonstrated reliability [13,18]. In the context of UAV devices, behavioral trust is essential for building confidence in the reliability, safety, and effectiveness of the technology and its operators. Behavioral trust can be a more reliable indicator of trust than self-reported attitudes. People's stated beliefs about trust might not always align with their actual behavior [16]. Traditional methods of measuring trust, like surveys, can be subjective and prone to bias. Behavioral trust offers a more objective way to assess trust dynamics. By observing behavior, researchers and practitioners can gain valuable insights into how trust is built, maintained, and broken in real-world interactions.

4.1.4. Direct Trust

Direct trust is established between different entities due to personal experience, interactions, and observations made among themselves, based on a local knowledge-based evaluation of interactions between individual UAVs. It involves forming beliefs about the reliability, integrity, and competence of an individual, organization, or system through direct evidence or firsthand knowledge [55]. Direct trust involves reciprocal relationships, where trust is built and acquired mutually based on shared experience and interactions. Considering that UAV A consistently received reliable data from UAV B during collaborative missions, UAV A may have a higher level of direct trust in UAV B. Continuity forms the foundation of trust in interpersonal relationships built over time and based on shared experience, mutual support, and open communication. UAV operators must trust that the UAV will operate as intended and perform its designated tasks without malfunctions or errors.

4.1.5. Derived Trust

Derived trust is inferred or conditional on external sources, such as recommendations, endorsements, or reviews. It involves relying on the decisions, opinions, or reputations of others to form beliefs about the trustworthiness of an entity. For instance, if multiple UAVs

in a network consistently report positive experiences with UAV Alice, UAV Bob may derive trust in UAV Alice based on this collective feedback. Individuals considering interacting with a UAV for personal or commercial use may rely on reviews and recommendations from a third party or trusted sources to inform their decision [18]. Suppose people see positive reviews and endorsements for a particular UAV model. In that case, they may derive trust in that model based on the opinions and experiences others had with the user or UAV. However, derived trust can be referred to as indirect trust.

4.2. Reputation Systems

UAV system reputation and trust are highly necessary, as they determine the genuineness and reliability of the data and information sent between the UAV systems in networks. The reputation system reflects the collaborative features of a system, which aim at collecting, aggregating, and distributing data about an entity or service that can be used to predict and characterize the entity's future. Reputation enables users to decide who they will trust or make transactions with and to what extent they will trust them based on the reputation data of the devices. Reputation can have both quantitative and qualitative components. Quantitatively, this might be numerical ratings, scores, or badges issued to users depending on their activities and interactions. On online platforms such as eBay, for example, users obtain feedback scores based on the number of successful transactions and reviews from other users. Qualitative reputation can be more sophisticated and incorporate subjective assessments about a user's conduct, such as politeness or community knowledge. Many online platforms have systems that allow users to offer feedback on other's behavior. Ratings, assessments, critiques, and recommendations are all forms of feedback that allow the community to assess a user's reputation collectively.

A high reputation score comes with various benefits. For example, people with a high reputation score may earn service provider rights or access to restricted site areas. Reputation scores motivate people to contribute positively to the system to retain or improve their reputation. Positive and negative behaviors may both impact one's reputation. Users who have unfavorable interactions with other users can attempt to enhance their reputation by making more good contributions and actions. Figure 5 shows the various types of reputation systems discussed in this section, along with their challenges.

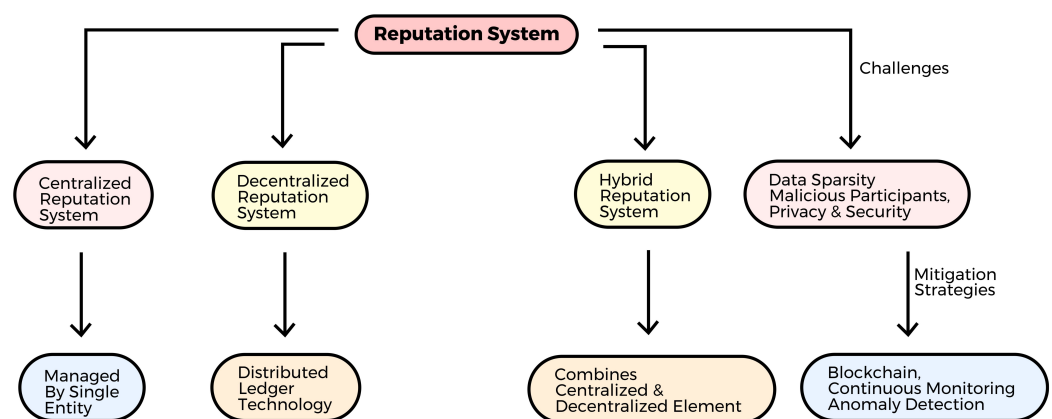


Figure 5. Reputation systems.

4.2.1. Centralized Reputation System

A centralized reputation system is run by a single identity or organization. In a centralized reputation system, a single organization manages the collection, storage, and handling of all reputation data and controls the system using a centralized database [4]. Various online marketplaces, like eBay, Amazon, and Yelp, employ this particular reputation system to effectively manage their data. A single governing authority facilitates the implementation of this specific system, making management reasonably simple [56]. Nevertheless, this approach has drawbacks, as it is more susceptible to single-point-of-failure attacks and

other cyberattacks. A compromise of the system may result in further possible problems and issues with the privacy of the data sent over the network.

Within UAV-centric network architectures, especially in dynamic operational scenarios like disaster response, there are significant issues in guaranteeing device authentication, data integrity, and privacy [38]. The 2015 Nepal earthquake highlighted UAVs' significant role in transmitting vital damage assessment data to command centers [82]. The rugged terrain and compromised infrastructure made UAV operations difficult. The accuracy and dependability of the data transmitted to command centers were frequently jeopardized by signals being broken by man-made and natural impediments [82]. Furthermore, there was a significant risk of data modification or interception by unauthorized parties, which might have resulted in incorrect rescue operations or inefficient use of vital resources. Ensuring the integrity of the data was crucial to allocate resources effectively.

To improve data reliability and address these issues, many methods have adopted blockchain technology. One notable example is the use of UAVs in Switzerland to transfer data to a centralized system for environmental monitoring [83]. Using blockchain technology guaranteed that each data entry was recorded in a tamper-resistant ledger, significantly lowering the risks of data tampering and loss and boosting data traceability and verifiability. This method ensured data accuracy and reliability and increased trust in the efficiency of using UAVs in crucial scenarios. Implementing blockchain technology offers a possible solution for tackling similar difficulties in future disaster-response scenarios. It can improve the reliability and trustworthiness of UAV systems during important missions [39].

4.2.2. Decentralized Reputation System

Using distributed ledger technology, or blockchain, each participant's reputation data are dispersed throughout the network of nodes in a decentralized reputation system, which is not governed by a single body like centralized reputation systems. Each participant's data are locally managed, saved, and controlled in their nodes [69], which collectively establish an agreement through a distributed consensus process to validate the data. Due to its distributed nature, a decentralized reputation system is more resilient to fraud, manipulation, and attacks than a centralized system because no single party controls the reputation data [4], increasing the transparency and confidence among network users. Systems that use a decentralized reputation system include Storj, Filecoin, Ethereum, Bitcoin, and others.

4.2.3. Hybrid Reputation System

A hybrid reputation system has elements from both centralized and decentralized systems. A centralized system is responsible for collecting and aggregating data, while a decentralized network is responsible for storing reputation data. By increasing resilience and security against manipulation and elevating the degree of trust and simplicity, a balance between centralization and decentralization is achieved according to the particular demands and requirements [56]. A hybrid reputation system is used by networks like Stack Overflow, Steemit, and GitHub.

4.3. Reputation Data

Reputation systems in many applications such as e-commerce, health care, agriculture, and more use data and information to generate and determine an entity's or service's reputation. Information can be grouped into two categories: manual and automatic data [26]. Manual data are obtained from feedback given by humans or entities with one or more interactions with the other entity. In contrast, automatic data are sourced directly from an event, such as the success or failure of an interaction or transaction, or indirectly in the form of information obtained from an entity with a direct interaction or transaction with the service providers. These data form the basic unit of the reputation system and may be discrete, continuous, or binary. The data can also be numeric or textual, requiring some computation to convert them into numerical data. The results are then used in the calcula-

tion of the reputation of an entity, which thereby decreases or increases the reputation of the users based on the proposed strategy and algorithm [26].

4.4. Challenges of Reputation Systems

Several challenges and issues are faced by reputation systems, as shown in Figure 5, and the data sent over the network, including the following.

4.4.1. Data Sparsity

Data sparsity is when a significant portion of transferred data contains empty or missing values. The design of UAV technologies allows for their remote operation in remote and hazardous environments without human interaction or involvement. Acquiring enough data and knowledge on other participants' reputations can be difficult due to the environment in which they operate. This implies that information needs to be gathered from various sources, including maintenance logs, flight logs, and eyewitness reports. This can be costly and time-consuming, potentially resulting in data that are not precise or dependable. Data sparsity can be caused by sampling bias, limited data collection, unstructured data, and sparse signals that can lead to biased results, as well as a reduction in the quality and accuracy of the data.

A paper that introduced and explored concepts and models for optimizing the efficiency of UAV-assisted data gathering in wireless sensor networks to prevent these attacks was presented in [40]. The proposed approach reduced data sparsity by optimizing the UAV trajectory to efficiently gather data from spatially dispersed wireless sensors, enhancing the coverage and communication with gateway-capable nodes. By selecting gateways strategically and improving UAV flight paths [40], the method increased the percentage of served sensor nodes and minimized the energy expenditure, ultimately reducing data sparsity in the network.

4.4.2. Malicious Participant

Malicious organizations can impact reputation systems by disseminating false or misleading reviews and participating in dishonest behavior. Ensuring the credibility of a reputation system necessitates prioritizing the discovery and correction of such actions. To address this concern, a proposal was made to detect and evaluate harmful behavior within IoT systems [54]. The paper suggested a behavior-based reputation assessment scheme for the node (BES) and an organization reputation evaluation scheme (ORES) as a solution. These are two reputation assessment methods. BES uses a node's behavior to assess its reputation by considering the behavioral data gathered from the information exchanges of nodes and tags. BES can recognize and evaluate negative node behavior, such as assaults or anomalous activities, by analyzing the evidence.

In contrast, ORES assesses an organization's standing by considering the present conditions of all its nodes. Based on the actions of its nodes, ORES can identify and assess an organization's reputation, giving an all-encompassing picture of its credibility throughout the Internet of Things. The article suggested using BES and ORES to stop and lessen bad behavior in IoT networks, so that nodes and organizations can be reliably found and judged on their reputation. This can improve the security and trust in an IoT system [54].

4.4.3. Privacy and Security

IoT devices, in general, encounter numerous difficulties and attacks [14,15]. Data confidentiality and integrity are crucial since UAV systems may handle sensitive information. Data privacy features may be lost if there is a disruption in the data that IoTs or UAV systems have collected. Unsecured data could give malevolent and unauthorized individuals access to manipulate the data. Decentralized architectures, on the other hand, can enhance privacy by lowering the number of central attack points. In a decentralized reputation system, spreading data across a network of nodes makes the system safer by making it harder for people who want to hack or change the data to do so. The use of

a decentralized architecture has the potential to enhance privacy and security measures through a reduction in central sources of vulnerability.

The security and privacy of reputation data for UAV systems can be preserved using various specialized methods in addition to these broad ones [41]. Differential privacy, for instance, can be used to anonymize data before sharing it with the reputation system. Differential privacy is a methodology that enables the aggregation and examination of data while safeguarding the confidentiality of individual participants' identities [41].

Another potential method for safeguarding the privacy and integrity of the reputation data given out to UAV systems involves the utilization of a blockchain-based anonymous reputation system (BARS) [70], which utilizes privacy-preserving authentication to enhance the conventional public key infrastructure (PKI) by incorporating a very efficient approach for preserving user privacy during authentication. The elimination of the linkability between the system's public key and its actual identification serves to protect privacy. The BARS system employs two distinct blockchains [70], namely certificate and revocation blockchains (CerBC and RevBC), which effectively execute CerBC and RevBC transparency mechanisms. The certificate authority (CA) records all of its actions transparently on the blockchain while maintaining the confidentiality of sensitive vehicle information. This process guarantees both confidence and privacy [70].

In summary, reputation systems can enhance UAV systems' safety, dependability, effectiveness, reliability, and trust. The utilization of reputation systems has several benefits and serves as a valuable tool in identifying, mitigating, and preventing fraudulent or malicious activities. Establishing and cultivating trust among system members can be facilitated using a reputation system. The reputation system serves as a mechanism to incentivize positive conduct and deter negative conduct among individuals inside the network. Regarding data sparsity, malicious participants, privacy, and security, among other issues, it is crucial to overcome the difficulties posed by utilizing robust reputation systems in UAV systems.

4.5. Feedback

Feedback techniques can be critical for ensuring UAV devices' safety and compliance. Reporting safety accidents or breaches can assist regulatory agencies, and organizations can take necessary safety measures. Data quality and trust are critical in applications where UAVs collect data. Accessing the data involves a cycle of inputs from the sensed environment. These are processed through computational devices, and the outputs are the actions the UAV's actuators take based on the processing results, as shown in Figure 6. These outputs are fed back to the input, which is called feedback. Feedback on data reliability and accuracy can affect the dependability of UAV data sources. Users who continuously offer high-quality data can establish a good reputation for what they do. UAV operators and enthusiasts frequently develop groups for collaboration and information exchange. By showcasing experienced and trusted members of these groups and promoting mentoring and information exchange, reputation systems can boost collaboration. Online marketplaces that link UAV service providers with customers can use reputation systems to assist customers in selecting trustworthy operators.

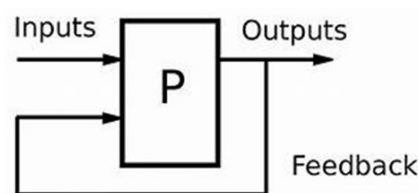


Figure 6. A feedback system, where P is a plant or process.

Users can rate UAV operators' service quality, timeliness, and professionalism, which can affect their reputation on the platform. The feedback given can be positive, negative,

or neutral. A feedback system implemented alongside blockchain technology to ensure anonymity and transparency in various industries was proposed in [71]. Rahman et al. discussed how the system could enhance trust and reliability in the feedback process, ultimately serving as a valuable tool for understanding user expectations and opinions. Additionally, the paper aimed to provide insights into the potential applications of blockchain technology in different sectors, such as corporate contexts, educational institutions, and rating-based companies [71].

Feedback systems have various components, including input, output, and processing.

4.5.1. Input Unit

The input unit refers to the data and signals that are received through sensed data from sensors like a barometer, GPS, camera, and LiDAR, which provide information like position altitude, longitude, latitude, speed, and certain other environmental factors [42]. An input system consists of the control commands containing instructions sent by a remote control or autopilot system, indicating what actions the UAV should perform.

4.5.2. The Processing Unit

The processing involves the computation and decision-making within the UAV's control system, typically an onboard flight controller or autopilot. This involves a control system that analyzes the sensor data to understand the current state of the UAV, including its orientation, position, and speed. It compares this with the desired state, setpoints, ground, and truth values. These also involve algorithms that determine appropriate actions based on the analyzed data. The control system identifies discrepancies or errors between the current and desired states, such as deviations in orientation. The control algorithms calculate the necessary adjustments to correct the UAV's behavior based on the identified errors.

4.5.3. Output Unit

The outputs are the actions the UAV's actuators took based on the processing results, consisting of both the hardware and software components. This refers to the components and processes responsible for implementing the decisions made during the processing phase of the feedback loop. In a feedback system [42], the output system translates processed data and control signals into physical or logical actions. This includes indicators or feedback mechanisms that inform operators about the UAV's state or the success of corrections.

5. Taxonomy Of Reputation Attacks

The significant changes in a node's reputation have been analyzed, whether it exhibits a substantial increase or decrease in reputation score [19]. When a node transmits a real or fake message, a way to update its reputation values gradually is introduced by increasing or decreasing the node's reputation. This continuous process of upgrading one's reputation enhances the accuracy and fairness of reputation assessment. Additionally, a global reputation hub, a central repository that maintains a record of every UAV node, was introduced in the proposed concept [19]. To determine the node's recommendation-bound reputation, the reputation of various recommenders is combined with its global reputation, which is updated each time an event is verified and carried out.

Overall, by establishing a progressive reputation update process and using a central hub for keeping global reputation data, the approach suggested in the study seeks to address the issue of abrupt reputation changes [19]. We can classify the challenges facing reputation in UAV systems into two classes, as shown in Figure 7.

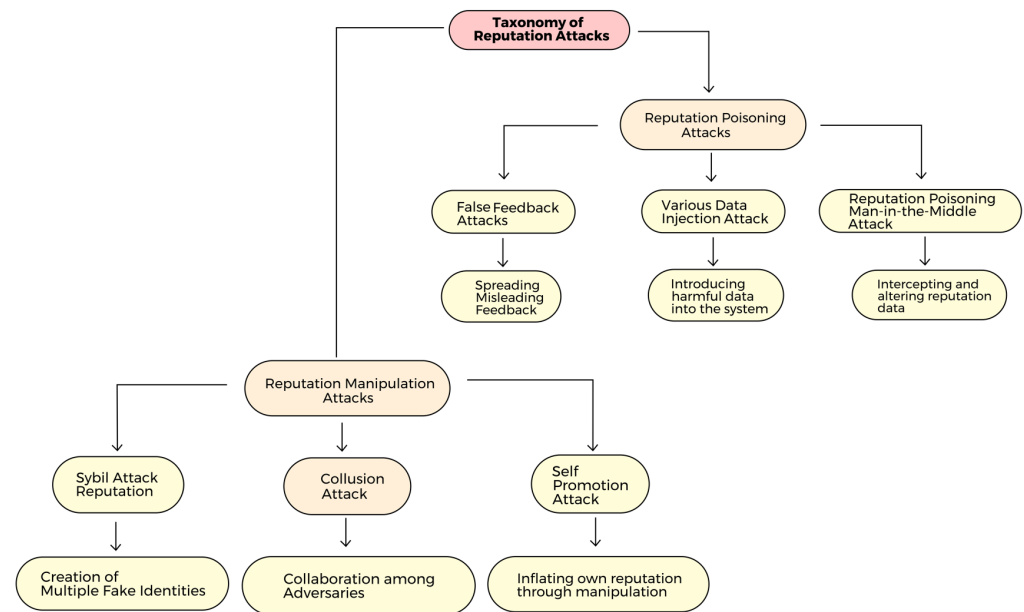


Figure 7. Taxonomy of reputation attacks.

5.1. Reputation Manipulation Attacks

A reputation manipulation attack tries to manipulate the reputation of a UAV or swarm of UAV systems to gain an advantage. For example, an attacker may attempt to falsely boost or increase the reputation of their system or reduce the reputation of a competitor's UAV by providing positive or negative feedback, respectively. Such manipulation can influence the decision-making process of systems relying on UAV reputation data, potentially leading to unplanned outcomes. Various examples of manipulation attacks are included below.

5.1.1. Sybil Attack

An attacker can create numerous fake identities or nodes using a deception tactic known as a Sybil attack to manipulate a network's trust or reputation system. More than one identity can correspond to a single entity. Entities in peer-to-peer networks use multiple identities for redundancy, resource sharing, reliability, and integrity. An adversary may present multiple identities to a peer-to-peer network to appear and function as multiple distinct nodes. The adversary may thus acquire disproportionate control over the network by affecting voting outcomes. The safety and integrity of UAV reputation systems are usually threatened by Sybil attacks.

In the context of a UAV reputation system, a Sybil attacker can generate numerous imaginary UAV identities, each accompanied by an artificial false positive reputation [43]. Subsequently, these malicious UAVs can be utilized for various false intentions. There are various methods via which individuals might attain anonymity, including online and offline. These methods include the utilization of multiple email addresses and social media identities, as well as the adoption of new identifications and locations. A substantial quantity of pseudonyms might be employed by attackers to exert an influence on the system through numerous tactics, including the ability to outvote other participants [44].

Sybil attacks present a substantial threat to diverse systems, including but not limited to online voting systems, social media platforms, and reputation systems. Within the realm of UAVs, the occurrence of a Sybil attack can hinder the operational effectiveness of a UAV network by flooding it with counterfeit UAVs. Furthermore, this method of assault can be utilized to spread deceptive data, by utilizing fraudulent UAVs as a means of distributing inaccurate information. Defending against Sybil attacks can pose challenges due to their susceptibility to exploitation by any individual possessing system access. Nevertheless, some methodologies can be employed to alleviate the potential threat posed by Sybil assaults. These techniques include the following:

- *Decentralized Blockchain:* Implementing a decentralized blockchain-based system for managing UAV reputation can significantly augment security measures [84]. The inherent characteristics of blockchain technology guarantee that once a reputation has been recorded and stored, it becomes resistant to modification or tampering. Verifying reputation updates is facilitated through a consensus process, mitigating a potential vulnerability to Sybil assaults. Incorporating a proof of work (PoW) or proof of stake (PoS) method can introduce a supplementary level of security. UAVs must solve a computational challenge or stake a certain amount of resources to provide reputation feedback [84]. Creating several fraudulent identities is rendered economically and computationally burdensome for potential attackers.
- *Reputation Source Validation:* One viable strategy for mitigating Sybil attacks involves verifying reputation data sources. UAVs ought to exclusively consider reputation inputs originating from trustworthy sources. Reputation information can be reliably sourced from trusted nodes or authorities, which can then be cryptographically authenticated to guarantee its veracity.
- *Continuous Monitoring and Anomaly Detection:* Continuous monitoring and anomaly detection play a crucial role in upholding the integrity and security of a UAV reputation system. These strategies facilitate detecting anomalous activities, such as abrupt increases in reputation scores, which could signify a Sybil attack or other types of manipulation [46]. Utilization of continuous monitoring and anomaly detection tools can detect abrupt increases in reputation scores or atypical patterns of conduct. When the UAV system identifies such irregularities, it can implement proactive measures to mitigate attacks on the system.

5.1.2. Collusion Attack

When numerous adversaries work together to compromise the trustworthiness of UAVs, this is known as a “collusion attack”. A collusion attack takes place when multiple agents act in their mutual interest to the detriment of other participants or when multiple agents act in their mutual interest to the detriment of other participants. A collusion attack’s main goal is to purposefully damage the reputation of particular targets or inadvertently improve the reputation of some UAVs [45]. The manipulation of UAV reputations can lead to various negative outcomes [31], such as weakened confidence in self-governing systems, skewed decision-making procedures, inaccurate information, security lapses, and compromised integrity in UAV-related operations. Attacks that involve collusion can take many forms, including concerted attempts to bypass security measures, compromise authentication procedures, or modify data for malicious or attack purposes. Detecting these attacks might pose a significant challenge due to the coordinated involvement of several actors.

5.1.3. Self-Promotion Attack

A self-promotion attack is a deceitful strategy employed by an individual or organization to deliberately enhance and increase their reputation inside a certain system or network, typically for personal advantage or gain [31]. A self-promotion attack commonly entails an attacker executing a series of acts to manipulate reputation ratings, to enhance their perceived trustworthiness or credibility. Self-promotion attacks can manifest in diverse settings, encompassing internet platforms, social networks, e-commerce websites, or autonomous systems such as UAV networks. These attacks may result in negative consequences, such as compromising the reliability of reputation systems, distorting trustworthiness, and influencing decision-making procedures [72]. Self-promotion attacks within UAV systems can have significant ramifications, encompassing the erosion of trust, unfair competition, and data quality degradation.

5.2. Reputation Poisoning Attack

A poisoning may refer to a specific attack that attempts to taint a UAV system’s or its operator’s reputation. Attacks may entail disseminating misleading or negative information

through digital platforms or alternative methods to undermine the system's reputation, referred to as a slandering attack [72]. The nature of the attack does not necessarily entail manipulation but rather centers on the degradation of reputation by disseminating negative or inaccurate information. Utilization of a compromised UAV often characterizes reputation-poisoning assaults to introduce malevolent data into the reputation system [58]. This might potentially entail capitalizing on errors present in the software or hardware of the UAV or obtaining physical proximity to the UAV to manipulate its reputation data. By inserting harmful or inaccurate information into the reputation system, the attacker aims to damage the UAV's reputation and adversely affect its credibility. We can classify reputation poisoning attacks into false feedback, data injection, and man-in-the-middle attacks.

5.2.1. False Feedback Attack

A false feedback attack refers to intentionally disseminating misleading or inaccurate feedback in an attack to adversely impact the reputation of a UAV [73]. False information might encompass a range of strategies, including the fabrication of deceptive evaluations or ratings, the dissemination of false information via digital platforms, or the adoption of false identities to publish favorable or unfavorable remarks regarding the UAV system [47]. The main objective of this type of attack is to jeopardize the reputation of the UAV, its operator, or its manufacturer by manipulating public perception through the dissemination of deceptive or dishonest feedback.

5.2.2. Malicious Data Injection Attack

In a data injection attack, the hacker introduces or injects malicious data into the reputation system to improve the reputation of a malicious UAV or harm the reputation of a trusted UAV [47]. Methods can involve manipulating the reputation system to incorporate fabricated accounts of misconduct. An attacker aims to manipulate the reputation of UAVs by exploiting vulnerabilities within the reputation system or compromising trusted UAVs, where the manipulation can impact the perception of UAV trustworthiness among stakeholders.

5.2.3. Reputation Poisoning Man-in-the-Middle Attack

A Man-in-the-Middle attack involves an attacker intercepting and manipulating reputation data as they pass from the reputation system to the UAV system. The attacker deliberately positions themselves in the communication channel between two parties [48]. Different methods are available to achieve this, such as spoofing or hijacking unencrypted Wi-Fi. In the center, the attacker seizes messages or data being exchanged between the two parties. The attacker sends the modified messages to the intended recipient, deceiving the targeted party. This objective can be accomplished by capitalizing on vulnerabilities present in communication networks or engaging in active interception and manipulation of transmitted data. The attacker's primary objective is manipulating UAVs' reputation by altering reputation data. This manipulation can potentially negatively impact the reputation of legitimate UAVs or enhance the reputation of malevolent UAVs. All these attacks aim to damage the perception of and confidence in UAVs and their operators. They employ strategies to accomplish their objectives, including fabricating information, taking advantage of weaknesses, pretending to be users, and manipulating data. The mitigation of reputation attacks necessitates the implementation of robust cybersecurity protocols, establishing secure communication channels, and adopting reputation management tactics to uphold the credibility and reliability of UAV systems [50].

Table 2 focuses on relevant and recent research that addresses various aspects of UAV reputation systems, including the challenges, proposed models, and proposed solutions to diverse challenges, such as blockchain and machine learning (ML), for improving UAV network security and efficiency.

Table 2. Different approaches used, with their weaknesses

	Approach	Model/Method	Goals	Weaknesses
[62]	Computational intelligence approach, including ML algorithms for UAV systems	Semi-autonomous blockchain-based UAV framework	Enhancing the security, efficiency, and reliability of UAV communication networks using blockchain technology	The limited scalability of blockchain for UAV applications, as well as the potential vulnerabilities in smart contracts
[19]	Reputation management framework that determines the trust of an event message and the reputation of the message producer	Majority voting protocol	Enhances event detection, trust management, reliable data transmission, and security functions in UAVs and IoTs	It does not explicitly mention the trade-offs or limitations of the proposed reputation management framework
[59]	Auction-based game theory, ML, and blockchain	Machine Learning	The autonomous selection and operation of UAVs for network coverage, along with real-time service monitoring and SLA management in wireless networks	It does not explicitly mention the specific ML algorithm used in developing the service reputation-based trust model
[51]	Optimization models such as MILP, to achieve efficient task assignments and resource allocation for persistent and efficient missions	Optimization and scheduling aspects of surveillance missions	Enhances the ability to conduct continuous, long-term, and efficient surveillance missions with multiple UAVs	Mixed integer linear program (MILP) model
[60]	Analyzing the overall architecture of TM and its development	Subjective logic theory, fuzzy logic theory, theory of evidence, and neural network model	Addresses the need for trust management to detect false messages while enhancing the understanding of trust management in IoT environments and its impact on security and reliability	It does not explicitly mention the use of blockchain technology
[74]	Design and implementation of a blockchain-based reputation system, focusing on ensuring transparency, reliability, and privacy in reputation management	Cryptographic and blockchain-based design	High privacy guarantees for consumers, efficiency, and security when integrated with a PoS blockchain. Enhances transparency and reliability in reputation management	Implementation challenges of a blockchain-based architecture and the need for further improvement in the overall system efficiency
[70]	Exploits the features of blockchain to extend conventional public key infrastructure (PKI) with an efficient privacy-preserving authentication mechanism	Blockchain-based anonymous reputation system (BARS)	BARS extends conventional PKI with an efficient privacy-preserving authentication mechanism and eliminates linkability between the public key and the real identity of a vehicle	The paper makes assumptions about the security levels of the law enforcement authority (LEA) and the capability of adversaries to compromise roadside units (RSUs)

Table 2. Cont.

	Approach	Model/Method	Goals	Weaknesses
[75]	ReFIOV, which leverages ML and an artificial immune system (AIS) to address the data accessibility problem in vehicular networks	Bayesian learning and classification, K-Means clustering, and danger theory	Presents a slow convergence in reputation establishment	Enhances and solves the improvement of data accessibility in vehicular networks, providing incentives for caching and stimulating node cooperation
[24]	Dynamic decentralized reputation system that utilizes blockchain technology for reputation storage and update	Fully decentralization, general purpose, global reputation, privacy, and employed technologies	This enhances the security and decentralization of the reputation management system in decentralized environments	Potential limitations of blockchain scalability, which requires special attention for decentralized systems relying on blockchain
[32]	Use of blockchain technology, particularly the Ethereum blockchain, for privacy-preserving authentication in ITS networks	Not specific	The model aims to address the vulnerabilities and loopholes present in existing systems, such as fake message delivery and privacy concerns	Lack of detailed discussion on the specific ML techniques or classification models used in the proposed BPPAU model
[52]	A malicious UAV detection algorithm (MDA) based on linear regression and a Gaussian clustering algorithms	Linear regression and Gaussian clustering algorithms	It enhances the accuracy of malicious node detection, with the accuracy of MDA outperforming existing methods by 10–20%	Does not address the use of blockchain technology for enhancing security in a UAV ad hoc network
[63]	Leveraging blockchain technology to manage the reputation values of IoT devices based on their geographical location.	Tree data structure	geocoding techniques and geospatial smart contracts for system performance and efficiency, and the decentralized management of device services and their reputation values	Gas limits in Ethereum transactions, hardware limitations of fog devices, and the lack of a positioning module for edge devices
[33]	Incentive scheme to choose UAVs with a high reputation to perform sensing tasks, protecting data sharing between UAVs and task publishers from internal attacks	Deep reinforcement learning model	The security of data sharing among UAVs and task publishers, as well as the successful mining of probabilities and utilities of UAVs	It does not thoroughly discuss the potential scalability issues or computational overhead associated with a blockchain-based secure data transmission scheme
[76]	A temporary center node called the miner is elected from vehicles through specific rules to generate rating blocks and broadcast them to other vehicles	Message detection accuracy	Improve credibility assessment of received messages based on observations of traffic environments and the consensus of ratings stored in the blockchain	Lack of specific details about the consensus protocol used in the blockchain-based reputation system

Table 2. Cont.

	Approach	Model/Method	Goals	Weaknesses
[77]	Fully distributed, secure, scalable, and efficient reputation aggregation scheme	Gossip-based reputation aggregation and decentralized reputation management	Enhances trustworthiness and cooperation in P2P networks by discouraging maliciousness	It does not guarantee computational efficiency and scalability

6. Defense Mechanism

The community has recognized the importance of UAV network security and many strategies for vulnerability mitigation and insights from researchers and practitioners have been reported [86,87]. For example, blockchain technology was recommended to create a tamper-proof record of all transactions, enhancing data integrity and trust [88,89]; AI/ML algorithms were suggested to identify and respond to unusual patterns indicative of security threats [90,91]; encryption and secure communication are widely adopted in all data transmissions between UAVs and control stations, to prevent interception and unauthorized access [85]; authentication and access control mechanisms were implemented to verify the identities of users and devices accessing the network [92]; etc. This list could be very long. However, this work is dedicated to trust and reputation systems instead of trying to provide a general and comprehensive guideline for UAV network security. There have been multiple high-quality survey papers and tutorials such as [93–95], and interested readers can access them to obtain the needed knowledge.

With the numerous challenges and issues outlined, this section delves into the defense mechanisms proposed to secure trust and reputation systems. These technologies, ranging from blockchain to ML and intrusion detection systems, offer significant advancements in security, data integrity, and efficient management. As illustrated in Figure 8, each approach brings distinct advantages across different network domains.

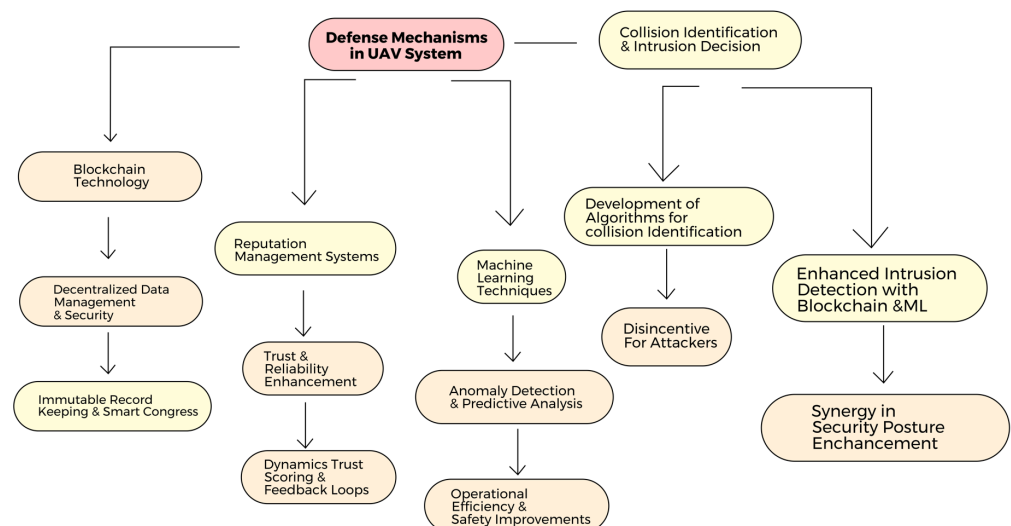


Figure 8. Defense mechanism.

6.1. Blockchain Technology

Blockchain technology is a decentralized system for maintaining a ledger, which establishes safe and transparent records. In the context of a reputation system based on blockchain technology, blockchain infrastructure facilitates the storage of reputation data, ensuring that only individuals with proper authorization can access such information. Establishing a decentralized, resilient, secured, distributed, public digital ledger and a transparent method that records blocks securely linked together through cryptographic hashes is an important

advantage of implementing technology in this system [32,76]. This technology enhances flexibility, survivability, security, and programmability and is suitable for 5G-oriented UAV networking [61]. Major attacks on IoT devices, which are single point of failure attacks, are reduced as a result of the distribution of the control functions over the network, which enhances and increases the robustness and security of the network [24,61].

Blockchain technology can be a defense technology that mitigates the various cyber threats in a network. Data integrity and verification of the authenticity of the data can be safeguarded in swarms of UAVs [49]. Integrity is essential in situations where secure data transmission is required, such as surveillance missions and remote sensing [49,74]. Moreover, the challenges of isolated applications operating on separate and different blockchain systems can be mitigated with the help of cross-blockchain platforms [63,64]. Sharing resources and data and efficiently collaborating and executing complex tasks are made easier by involving and implementing multiple blockchain-based applications that govern the inter-communication and transfer of assets in a UAV network context [33]. The introduction of a spectrum of scenarios related to UAV networks that can leverage the potential of the currently available cross-blockchain solutions was discussed in [64].

UAV-assisted blockchain systems have significantly contributed to optimizing energy for UAV devices and many battery-powered IoT devices [65]. To minimize the energy consumption of a UAV, joint optimization of the central processing unit (CPU) frequencies for data computation and block generation, the amount of offloaded industrial Internet of things (IIoT) data [70], the bandwidth allocation, and the trajectory of the UAV were formulated as a non-convex optimization problem and solved using a successive convex approximation (SCA) algorithm [65]. The SCA could reduce energy consumption, which helped extend the duration of missions and enhance operational efficiency [59,62].

6.2. Reputation Management System

Using reputation management systems for UAVs is crucial for mitigating different attacks on UAV systems. A management system involves a range of strategies, processes, and tools to effectively monitor, manage, and shape one's reputation and public perception. This requires tracking and monitoring data transmitted across different network nodes. An effective reputation management system for UAV technology requires a blend of proactive and reactive strategies, as well as continuous monitoring and adaptation to the constantly changing online environment. The control process is focused on protecting and improving the reputation, credibility, and reliability of UAV technology in the digital world.

Ensuring the preservation and improvement of an entity's reputation across different digital platforms is the main objective of a reputation management system. The purpose of these systems is to systematically monitor and evaluate the reputation of individual UAVs operating within a specified network or system. UAVs are granted reputation scores according to their past conduct, interactions, and performance. These systems are crucial in establishing and upholding confidence and dependability in autonomous operations. Through continuously monitoring and updating UAV reputations, identifying potential hazards and detecting anomalous patterns becomes feasible. Furthermore, reputation scores play a crucial role in enhancing the decision-making capabilities of autonomous systems by providing valuable insights into the reliability and trustworthiness of UAVs.

6.3. Machine Learning

One essential defense mechanism is the integration of ML techniques into a system. The utilization of ML techniques can greatly improve the identification and mitigation of collusion attacks. Anomaly detection methods are utilized to analyze the vast amount of data that UAV interactions generate. These algorithms are designed to recognize anomalous behavior or shifts in reputation that may point to malevolent conduct in the system. Collaborative filtering techniques are also utilized to reveal latent relationships among UAVs. Algorithms can discover suspicious cooperation that may result in reputation manipulation by examining these links through training models to identify and classify these actions,

and the system can rapidly detect and react to suspected instances of collusion. ML is an automated analytical tool that can adapt to shifting assault techniques, rendering it a dynamic and efficient protection mechanism against collusion.

ML, especially neural networks, has been implemented to enhance various UAV capabilities, such as obstacle avoidance, flying formation, and autonomous decision-making [66]. ML models enable UAVs to effectively navigate complex environments, precisely and accurately, in dynamic situations by processing large volumes of sensor data in real-time. In addition, zero-trust was proposed to enhance security by adopting a cautious approach to trust assumption due to the manipulations and adversarial attacks and vulnerabilities they are exposed to [67]. A methodology was proposed based on established security principles like zero-trust and defense-in-depth to help prevent and mitigate the consequences of security threats, including those emerging from ML-based components. In a distributed manner, federated learning (FL) is more suitable for UAV networks than traditional ML schemes for boosting the edge intelligence of UAVs. Considering the limited energy supply of UAVs, how to minimize a UAV's overall training energy consumption by jointly optimizing the local convergence threshold, local iterations, computation resource allocation, and bandwidth allocation, subject to the FL global accuracy guarantee and maximum training latency constraint, was studied [53].

6.4. Collusion Identification

Identifying collusion plays a vital role in the defense against collusion attacks. Developing algorithms and models specifically tailored to identifying collusion is paramount for effectively implementing this strategy. Collusion can take many forms, including when several UAVs work together to damage a target's reputation or to intentionally enhance the reputation of one of the members. Identification of collusion not only contributes to the integrity of UAV reputation systems but also acts as a disincentive to attackers, who could be wary of being discovered and facing challenges to their activities.

Implementation of intrusion detection also plays a vital role in safeguarding and mitigating against unauthorized access and malicious activities [47]. Incorporating blockchain technology and ML techniques can ensure integrity and security by enhancing intrusion detection. Combining blockchain and ML in intrusion detection enhances the overall security posture of UAV networks. Blockchain can ensure the integrity and tamper-proof nature of an intrusion detection log, while ML analyzes these data for patterns and anomalies. Blockchain's synergy strengthens the network's ability to detect and mitigate known and novel security threats, safeguarding critical UAV operations.

7. Conclusions

This paper provided a survey of trust and reputation systems, to give an overview of critical functions for securing the privacy of UAV networks and ensuring the reliable operation of UAVs. The results and contributions are summarized in Table 3.

This paper discussed several vulnerabilities posed by malicious actors who attempt to exploit UAV systems. These challenges, such as data tampering, privacy breaches, and trust dilution, are non-trivial and require sophisticated countermeasures. Therefore, integrating advanced technologies like blockchain and ML presents a promising solution. With its decentralized and immutable ledger capabilities, blockchain technology offers a way to secure the integrity of reputation data against tampering. Meanwhile, ML algorithms provide adaptive mechanisms for detecting and responding to anomalous behaviors, enhancing UAV networks' trustworthiness.

In addition, the strategies discussed in this paper provide a foundation for further research and development in UAV IoT system security. By addressing the current issues and potential solutions, our work contributes to the ongoing efforts to create a safer, more reliable, and more efficient UAV ecosystem. Likewise, there is a need for a broader integration of digital systems, including IoT devices and autonomous vehicles, paving the way for a more interconnected and automated future.

Finally, this paper presented a detailed analysis of the existing reputation and trust systems, elucidated crucial challenges, and explored innovative mitigation strategies. These are critical for advancing the field and ensuring the sustainable growth of UAV networks, other IoT networks, and smart city systems. We hope this work will inspire more discussions in the community and spark more novel ideas for safeguarding and enhancing the burgeoning landscape of UAV applications.

Table 3. Summary of key findings and contributions.

Key Area	Findings	Contributions
Trust in UAV Networks	Trust is critical for UAV operations, involving reliability, security, safety, transparency, and ethical conduct.	Detailed analysis of trust components and their impact on UAV network performance to improve the framework.
Security Measures	Essential security measures include encryption, authentication protocols, and intrusion detection systems.	Proposed robust security frameworks to protect data integrity and privacy in UAV networks.
Privacy Concerns	Privacy involves protecting sensitive data from unauthorized access and ensuring compliance with legal standards.	Suggested data anonymization and secure storage solutions to enhance privacy protections in UAV networks.
Centralized vs. Decentralized	Centralized networks face challenges from single points of failure and security risks, whereas decentralized architectures offer enhanced resilience.	Advocated for adopting decentralized systems, highlighting blockchain technology's role in improving security and trust.
Reputation Systems	Reputation systems are vital for assessing trustworthiness and ensuring reliable data exchange in UAV networks.	Comprehensive survey of existing reputation systems and their application in UAV networks.
Mitigation Strategies	Strategies for mitigating vulnerabilities include robust encryption, secure communication channels, and regular security audits.	Provided actionable insights and best practices for enhancing UAV network security.

Author Contributions: Conceptualization, Y.C., S.O., G.C. and E.B.; methodology, S.O. and Y.C.; software, S.O.; validation, S.O., G.C. and Y.C.; formal analysis, S.O. and Y.C.; investigation, S.O. and Y.C.; resources, Y.C., E.B. and G.C.; data curation, S.O.; writing—original draft preparation, S.O. and Y.C.; writing—review and editing, Y.C., G.C. and E.B.; visualization, S.O.; supervision, Y.C., E.B. and G.C.; project administration, Y.C. and G.C.; funding acquisition, Y.C. and G.C. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The data presented in this study are available on request from the corresponding author following the data management regulations of Binghamton University.

Conflicts of Interest: Author Genshe Chen was employed by Intelligent Fusion Technology, Inc. The remaining 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.

Abbreviations

The following abbreviations are used in this manuscript:

5G	Fifth Generation
AIS	Artificial Immune System
BARS	Blockchain-based Anonymous Reputation System

BES	Behavior-based Reputation Assessment Scheme
CA	Certificate Authority
CerBC	Certificate Blockchain
CPU	Central Processing Unit
FL	Federated Learning
HMM	Hidden Markov Chains
IDS	Intrusion Detection System
IIoT	Industrial Internet of Things
IoT	Internet of Things
LEA	Law Enforcement Authority
MDA	Malicious UAV Detection Algorithm
MILP	Mixed Integer Linear Program
ML	Machine Learning
ORES	Organization Reputation Evaluation Scheme
PKI	Public Key Infrastructure
PoS	Proof of Stake
PoW	Proof of Work
QoE	Quality of Experience
QoS	Quality of Service
RevBC	Revocation Blockchain
RSU	Roadside Units
SCA	Successive Convex Approximation
SDN	Software-Defined Network
UAANET	Unmanned Aerial Vehicle Ad Hoc Networks
UAV	Unmanned Aerial Vehicle

References

1. Muchiri, G.; Kimathi, S. A review of applications and potential applications of UAV. In Proceedings of the Sustainable Research and Innovation Conference, Daerah Istimewa Yogyakarta, Indonesia, 20–21 July 2022; pp. 280–283.
2. Utsav, A.; Abhishek, A.; Suraj, P.; Badhai, R.K. An IoT based UAV network for military applications. In Proceedings of the 2021 Sixth International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, India, 25–27 March 2021; pp. 122–125.
3. Hildmann, H.; Kovacs, E. Using unmanned aerial vehicles (UAVs) as mobile sensing platforms (MSPs) for disaster response, civil security and public safety. *Drones* **2019**, *3*, 59. [\[CrossRef\]](#)
4. Jøsang, A.; Ismail, R.; Boyd, C. A survey of trust and reputation systems for online service provision. *Decis. Support Syst.* **2007**, *43*, 618–644. [\[CrossRef\]](#)
5. Tsouros, D.C.; Bibi, S.; Sarigiannidis, P.G. A review on UAV-based applications for precision agriculture. *Information* **2019**, *10*, 349. [\[CrossRef\]](#)
6. Angraal, S.; Krumholz, H.M.; Schulz, W.L. Blockchain technology: applications in health care. *Circ. Cardiovasc. Qual. Outcomes* **2017**, *10*, e003800. [\[CrossRef\]](#)
7. Hein, D.; Kraft, T.; Brauchle, J.; Berger, R. Integrated uav-based real-time mapping for security applications. *ISPRS Int. J. Geo-Inf.* **2019**, *8*, 219. [\[CrossRef\]](#)
8. Xu, R.; Wei, S.; Chen, Y.; Chen, G.; Pham, K. LightMAN: A Lightweight Microchained Fabric for Assurance-and Resilience-Oriented Urban Air Mobility Networks. *Drones* **2022**, *6*, 421. [\[CrossRef\]](#)
9. Garau Guzman, J.; Baeza, V.M. Enhancing Urban Mobility through Traffic Management with UAVs and VLC Technologies. *Drones* **2024**, *8*, 7. [\[CrossRef\]](#)
10. Newswire, G. Global Commercial UAV Market Report 2023: Smart City Applications will Drive up to 36.5% of Drone Fleet Deployments by 2028, 2023. Available online: <https://www.globenewswire.com/en/news-release/2023/07/05/2699314/28124/en/Global-Commercial-UAV-Market-Report-2023-Smart-City-Applications-will-Drive-up-to-36-5-of-Drone-Fleet-Deployments-by-2028.html> (accessed on 15 May 2024).
11. Biswas, S.; Anavatti, S.G.; Garratt, M.A. Chapter 4—Path planning and task assignment for multiple UAVs in dynamic environments. In *Unmanned Aerial Systems*; Koubaa, A., Azar, A.T., Eds.; Advances in Nonlinear Dynamics and Chaos (ANDC); Academic Press: Cambridge, MA, USA, 2021; pp. 81–102. [\[CrossRef\]](#)
12. Hassija, V.; Chamola, V.; Agrawal, A.; Goyal, A.; Luong, N.C.; Niyato, D.; Yu, F.R.; Guizani, M. Fast, reliable, and secure drone communication: A comprehensive survey. *IEEE Commun. Surv. Tutor.* **2021**, *23*, 2802–2832. [\[CrossRef\]](#)
13. Fortino, G.; Fotia, L.; Messina, F.; Rosaci, D.; Sarné, G.M. Trust and reputation in the internet of things: State-of-the-art and research challenges. *IEEE Access* **2020**, *8*, 60117–60125. [\[CrossRef\]](#)

14. Blasch, E.; Sabatini, R.; Roy, A.; Kramer, K.A.; Andrew, G.; Schmidt, G.T.; Insaurralde, C.C.; Fasano, G. Cyber awareness trends in avionics. In Proceedings of the 2019 IEEE/AIAA 38th Digital Avionics Systems Conference (DASC), San Diego, CA, USA, 8–12 September 2019; pp. 1–8.
15. Krishna, C.L.; Murphy, R.R. A review on cybersecurity vulnerabilities for unmanned aerial vehicles. In Proceedings of the 2017 IEEE International Symposium on Safety, Security and Rescue Robotics (SSRR), Shanghai, China, 11–13 October 2017; pp. 194–199.
16. Fortino, G.; Messina, F.; Rosaci, D.; Sarné, G.M. Using blockchain in a reputation-based model for grouping agents in the Internet of Things. *IEEE Trans. Eng. Manag.* **2019**, *67*, 1231–1243. [\[CrossRef\]](#)
17. Liang, Q.; Gan, X. Research on trust evaluation algorithm for e-commerce based on reputation. In Proceedings of the 2011 International Conference on Business Computing and Global Informatization, Shanghai, China, 29–31 July 2011; pp. 39–42.
18. Fotia, L.; Delicato, F.; Fortino, G. Trust in edge-based internet of things architectures: State of the art and research challenges. *ACM Comput. Surv.* **2023**, *55*, 1–34. [\[CrossRef\]](#)
19. Bhoi, S.K.; Jena, K.K.; Jena, A.; Panda, B.C.; Singh, S.; Behera, P. A Reputation Deterministic Framework for True Event Detection in Unmanned Aerial Vehicle Network (UAVN). In Proceedings of the 2019 International Conference on Information Technology (ICIT), Bhubaneswar, India, 19–21 December 2019; pp. 257–262. [\[CrossRef\]](#)
20. Battah, A.A.; Iraqi, Y.; Damiani, E. A Trust and Reputation System for IoT Service Interactions. *IEEE Trans. Netw. Serv. Manag.* **2022**, *19*, 2987–3005. [\[CrossRef\]](#)
21. Mrabet, K.; El Bouanani, F.; Ben-Azza, H. Dynamic Decentralized Reputation System from Blockchain and Secure Multiparty Computation. *J. Sens. Actuator Netw.* **2023**, *12*, 14. [\[CrossRef\]](#)
22. Ogunbunmi, S.; Hatmai, M.; Xu, R.; Chen, Y.; Blasch, E.; Ardiles-Cruz, E.; Aved, A.; Chen, G. A Lightweight Reputation System for UAV Networks. In *Proceedings of the Security and Privacy in Cyber-Physical Systems and Smart Vehicles*; Chen, Y., Lin, C.W., Chen, B., Zhu, Q., Eds.; Springer Nature: Cham, Switzerland, 2024; pp. 114–129.
23. Qu, Q.; Ogunbunmi, S.; Hatami, M.; Xu, R.; Chen, Y.; Chen, G.; Blasch, E. A Digital Twins Enabled Reputation System for Microchain-based UAV Networks. In Proceedings of the 2023 IEEE 12th International Conference on Cloud Networking (CloudNet), New York, NY, USA, 1–3 November 2023; pp. 428–432.
24. Mrabet, K.; El Bouanani, F.; Ben-Azza, H. Generalized Secure and Dynamic Decentralized Reputation System with a Dishonest Majority. *IEEE Access* **2023**, *11*, 9368–9388. [\[CrossRef\]](#)
25. El Hussein, A.; M'hamed, A.; El Hassan, B.; Mokhtari, M. Trust-Based Authentication Scheme with User Rating for Low-Resource Devices in Smart Environments. *Pers. Ubiquitous Comput.* **2013**, *17*, 1013–1023. [\[CrossRef\]](#)
26. Pereira, R.H.; Gonçalves, M.J.; Magalhães, M.A.G. Reputation Systems: A framework for attacks and frauds classification. *J. Inf. Syst. Eng. Manag.* **2023**, *8*, 19218. [\[CrossRef\]](#)
27. Frew, E.W.; Argrow, B.; Houston, A.; Weiss, C. An Energy-Aware Airborne Dynamic Data-Driven Application System for Persistent Sampling and Surveillance. In *Handbook of Dynamic Data Driven Applications Systems: Volume 2*; Springer: Berlin, Germany, 2023; pp. 419–448.
28. Ngu, A.H.; Gutierrez, M.; Metsis, V.; Nepal, S.; Sheng, Q.Z. IoT Middleware: A Survey on Issues and Enabling Technologies. *IEEE Internet Things J.* **2017**, *4*, 1–20. [\[CrossRef\]](#)
29. Guo, L.; Zhang, C.; Fang, Y. A Trust-Based Privacy-Preserving Friend Recommendation Scheme for Online Social Networks. *IEEE Trans. Depend. Secur. Comput.* **2015**, *12*, 413–427. [\[CrossRef\]](#)
30. Ghahramani, M.H.; Zhou, M.; Hon, C.T. Toward cloud computing QoS architecture: Analysis of cloud systems and cloud services. *IEEE/CAA J. Autom. Sin.* **2017**, *4*, 6–18. [\[CrossRef\]](#)
31. Hoffman, K.; Zage, D.; Nita-Rotaru, C. A survey of attack and defense techniques for reputation systems. *ACM Comput. Surv. (CSUR)* **2009**, *42*, 1–31. [\[CrossRef\]](#)
32. Qureshi, K.N.; Jeon, G.; Hassan, M.M.; Hassan, M.R.; Kaur, K. Blockchain-Based Privacy-Preserving Authentication Model Intelligent Transportation Systems. *IEEE Trans. Intell. Transp. Syst.* **2023**, *24*, 7435–7443. [\[CrossRef\]](#)
33. Xie, L.; Su, Z.; Chen, N.; Xu, Q. Secure Data Sharing in UAV-assisted Crowdsensing: Integration of Blockchain and Reputation Incentive. In Proceedings of the 2021 IEEE Global Communications Conference (GLOBECOM), Madrid, Spain, 7–11 December 2021; pp. 1–6. [\[CrossRef\]](#)
34. Wu, H.; Zhang, W. Digital identity, privacy security, and their legal safeguards in the Metaverse. *Secur. Saf.* **2023**, *2*, 2023011. [\[CrossRef\]](#)
35. Malik, S.; Dedeoglu, V.; Kanhere, S.S.; Jurdak, R. Trustchain: Trust management in blockchain and iot supported supply chains. In Proceedings of the 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 14–17 July 2019; pp. 184–193.
36. Su, Y. A trust based scheme to protect 5G UAV communication networks. *IEEE Open J. Comput. Soc.* **2021**, *2*, 300–307. [\[CrossRef\]](#)
37. Kong, L.; Chen, B.; Hu, F. LAP-BFT: Lightweight asynchronous provable byzantine fault-tolerant consensus mechanism for UAV network. *Drones* **2022**, *6*, 187. [\[CrossRef\]](#)
38. Chen, C.L.; Deng, Y.Y.; Weng, W.; Chen, C.H.; Chiu, Y.J.; Wu, C.M. A traceable and privacy-preserving authentication for UAV communication control system. *Electronics* **2020**, *9*, 62. [\[CrossRef\]](#)
39. Aljumah, A. UAV-Based Secure Data Communication: Multilevel Authentication Perspective. *Sensors* **2024**, *24*, 996. [\[CrossRef\]](#)

40. Putra, G.D.; Dedeoglu, V.; Kanhere, S.S.; Jurdak, R. Trust management in decentralized iot access control system. In Proceedings of the 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Virtual, 2–6 May 2020; pp. 1–9.
41. Jain, P.; Gyanchandani, M.; Khare, N. Differential privacy: Its technological prescriptive using big data. *J. Big Data* **2018**, *5*, 1–24. [\[CrossRef\]](#)
42. Lee, H.; Yoon, J.; Jang, M.S.; Park, K.J. A robot operating system framework for secure uav communications. *Sensors* **2021**, *21*, 1369. [\[CrossRef\]](#)
43. Levine, B.N.; Shields, C.; Margolin, N.B. A survey of solutions to the sybil attack. *Univ. Mass. Amherst* **2006**, *7*, 224.
44. Zhang, K.; Liang, X.; Lu, R.; Shen, X. Sybil attacks and their defenses in the internet of things. *IEEE Internet Things J.* **2014**, *1*, 372–383. [\[CrossRef\]](#)
45. Meamari, E.; Guo, H.; Shen, C.C.; Hur, J. Collusion attacks on decentralized attributed-based encryption: Analyses and a solution. *arXiv* **2020**, arXiv:2002.07811.
46. Marche, C.; Nitti, M. Trust-related attacks and their detection: A trust management model for the social IoT. *IEEE Trans. Netw. Serv. Manag.* **2020**, *18*, 3297–3308. [\[CrossRef\]](#)
47. Sayghe, A.; Hu, Y.; Zografopoulos, I.; Liu, X.; Dutta, R.G.; Jin, Y.; Konstantinou, C. Survey of machine learning methods for detecting false data injection attacks in power systems. *IET Smart Grid* **2020**, *3*, 581–595. [\[CrossRef\]](#)
48. Salem, O.; Alsubhi, K.; Shaafi, A.; Gheryani, M.; Mehaoua, A.; Boutaba, R. Man-in-the-Middle attack mitigation in internet of medical things. *IEEE Trans. Ind. Inform.* **2021**, *18*, 2053–2062. [\[CrossRef\]](#)
49. Jensen, I.J.; Selvaraj, D.; Ranganathan, P. Blockchain Technology for Networked Swarms of Unmanned Aerial Vehicles (UAVs). In Proceedings of the 2019 IEEE 20th International Symposium on “A World of Wireless, Mobile and Multimedia Networks” (WoWMoM), Washington, DC, USA, 10–12 June 2019; pp. 1–7. [\[CrossRef\]](#)
50. Nigam, A.; Sharma, S.; Patel, R.K.; Agrawal, M. Man-in-the-middle-attack and proposed algorithm for detection. In Proceedings of the 2022 International Mobile and Embedded Technology Conference (MECON), Noida, India, 10–11 March 2022; pp. 83–88.
51. Leahy, K.; Zhou, D.; Vasile, C.I.; Oikonomopoulos, K.; Schwager, M.; Belta, C. Persistent surveillance for unmanned aerial vehicles subject to charging and temporal logic constraints. *Auton. Robots* **2016**, *40*, 1363–1378. [\[CrossRef\]](#)
52. Sun, S.; Ma, Z.; Liu, L.; Gao, H.; Peng, J. Detection of malicious nodes in drone ad-hoc network based on supervised learning and clustering algorithms. In Proceedings of the 2020 16th International Conference on Mobility, Sensing and Networking (MSN), Tokyo, Japan, 17–19 December 2020; pp. 145–152.
53. Shen, Y.; Qu, Y.; Dong, C.; Zhou, F.; Wu, Q. Joint Training and Resource Allocation Optimization for Federated Learning in UAV Swarm. *IEEE Internet Things J.* **2023**, *10*, 2272–2284. [\[CrossRef\]](#)
54. Chen, J.; Tian, Z.; Cui, X.; Yin, L.; Wang, X. Trust architecture and reputation evaluation for internet of things. *J. Ambient. Intell. Humaniz. Comput.* **2019**, *10*, 3099–3107. [\[CrossRef\]](#)
55. Chen, D.; Chang, G.; Sun, D.; Li, J.; Jia, J.; Wang, X. TRM-IoT: A trust management model based on fuzzy reputation for internet of things. *Comput. Sci. Inf. Syst.* **2011**, *8*, 1207–1228. [\[CrossRef\]](#)
56. Tu, Z.; Zhou, H.; Li, K.; Song, H.; Yang, Y. A blockchain-based trust and reputation model with dynamic evaluation mechanism for IoT. *Comput. Netw.* **2022**, *218*, 109404. [\[CrossRef\]](#)
57. Alaa, M.; Oumayma, A.; Mohamad, A. Towards Trust Model in Unmanned Aerial Vehicle Ad Hoc Networks. *J. Commun. Softw. Syst.* **2021**, *17*, 213–220. [\[CrossRef\]](#)
58. Sharma, A.; Pilli, E.S.; Mazumdar, A.P.; Gera, P. Towards trustworthy Internet of Things: A survey on Trust Management applications and schemes. *Comput. Commun.* **2020**, *160*, 475–493. [\[CrossRef\]](#)
59. Khan, A.S.; Chen, G.; Rahulamathavan, Y.; Zheng, G.; Assadhan, B.; Lambbotharan, S. Trusted UAV Network Coverage Using Blockchain, Machine Learning, and Auction Mechanisms. *IEEE Access* **2020**, *8*, 118219–118234. [\[CrossRef\]](#)
60. Li, X.; Li, R. A Comprehensive Review for Four-Dimensional Trust Management in Distributed IoT. *IEEE Internet Things J.* **2023**, *10*, 21738–21762. [\[CrossRef\]](#)
61. Hu, N.; Tian, Z.; Sun, Y.; Yin, L.; Zhao, B.; Du, X.; Guizani, N. Building Agile and Resilient UAV Networks Based on SDN and Blockchain. *IEEE Netw.* **2021**, *35*, 57–63. [\[CrossRef\]](#)
62. Ahamed Ahanger, T.; Aldaej, A.; Atiquzzaman, M.; Ullah, I.; Yousufudin, M. Distributed blockchain-based platform for unmanned aerial vehicles. *Comput. Intell. Neurosci.* **2022**, *2022*, 4723124. [\[CrossRef\]](#)
63. Weerapanisit, P.; Trilles, S.; Huerta, J.; Painho, M. A decentralized location-based reputation management system in the IoT using blockchain. *IEEE Internet Things J.* **2022**, *9*, 15100–15115. [\[CrossRef\]](#)
64. Alkadi, R.; Alnuaimi, N.; Yeun, C.; Shoufan, A. Blockchain Interoperability in Unmanned Aerial Vehicles Networks: State-of-the-Art and Open Issues. *IEEE Access* **2022**, *10*, 14463–14479. [\[CrossRef\]](#)
65. Lin, X.; Zhang, J.; Xiang, L.; Ge, X. Energy Consumption Optimization for UAV Assisted Private Blockchain-based IIoT Networks. In Proceedings of the 2021 IEEE 94th Vehicular Technology Conference (VTC2021-Fall), Virtual, 27–28 September 2021; pp. 1–7. [\[CrossRef\]](#)
66. Obaid, A.A.; Koyuncu, H. Obstacle Avoidance in Unmanned Aerial Vehicles Using Image Segmentation and Deep Learning. In Proceedings of the 2022 International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), Ankara, Turkey, 20–22 October 2022; pp. 912–915. [\[CrossRef\]](#)

67. Hale, B.; Bossuyt, D.L.V.; Papakonstantinou, N.; O'Halloran, B. A Zero-Trust Methodology for Security of Complex Systems With Machine Learning Components. In Proceedings of the 41st Computers and Information in Engineering Conference (CIE), Virtual, Online, 17–21 August 2021; Volume 2. [\[CrossRef\]](#)
68. Wu, Y.; Yan, C.; Ding, Z.; Liu, G.; Wang, P.; Jiang, C.; Zhou, M. A Novel Method for Calculating Service Reputation. *IEEE Trans. Autom. Sci. Eng.* **2013**, *10*, 634–642. [\[CrossRef\]](#)
69. Hendrikx, F.; Bubendorfer, K.; Chard, R. Reputation systems: A survey and taxonomy. *J. Parallel Distrib. Comput.* **2015**, *75*, 184–197. [\[CrossRef\]](#)
70. Lu, Z.; Wang, Q.; Qu, G.; Liu, Z. BARS: A Blockchain-Based Anonymous Reputation System for Trust Management in VANETs. In Proceedings of the 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science And Engineering (TrustCom/BigDataSE), New York, NY, USA, 1–3 August 2018; pp. 98–103. [\[CrossRef\]](#)
71. Rahman, M.M.; Rifat, M.M.H.; Tanin, M.Y.; Hossain, N. A feedback system using blockchain technology. In Proceedings of the 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS), Coimbatore, India, 3–5 December 2020; pp. 1114–1118. [\[CrossRef\]](#)
72. Huang, C.; Wang, Z.; Chen, H.; Hu, Q.; Zhang, Q.; Wang, W.; Guan, X. Repchain: A reputation-based secure, fast, and high incentive blockchain system via sharding. *IEEE Internet Things J.* **2020**, *8*, 4291–4304. [\[CrossRef\]](#)
73. Gyawali, S.; Qian, Y.; Hu, R.Q. Machine learning and reputation based misbehavior detection in vehicular communication networks. *IEEE Trans. Veh. Technol.* **2020**, *69*, 8871–8885. [\[CrossRef\]](#)
74. Liu, D.; Alahmadi, A.; Ni, J.; Lin, X.; Shen, X. Anonymous reputation system for IIoT-enabled retail marketing atop PoS blockchain. *IEEE Trans. Ind. Inform.* **2019**, *15*, 3527–3537. [\[CrossRef\]](#)
75. Magaia, N.; Sheng, Z. ReFloV: A Novel Reputation Framework for Information-Centric Vehicular Applications. *IEEE Trans. Veh. Technol.* **2019**, *68*, 1810–1823. [\[CrossRef\]](#)
76. Yang, Z.; Zheng, K.; Yang, K.; Leung, V.C.M. A blockchain-based reputation system for data credibility assessment in vehicular networks. In Proceedings of the 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Montreal, QC, Canada, 8–13 October 2017; pp. 1–5. [\[CrossRef\]](#)
77. Zhou, R.; Hwang, K. Gossip-Based Reputation Aggregation for Unstructured Peer-to-Peer Networks. In Proceedings of the 2007 IEEE International Parallel and Distributed Processing Symposium, Long Beach, CA, USA, 26–30 March 2007. [\[CrossRef\]](#)
78. Carholt, O.; Fresk, E.; Andrikopoulos, G.; Nikolakopoulos, G. Design, modelling and control of a single rotor UAV. In Proceedings of the 2016 24th Mediterranean Conference on Control and Automation (MED), Athens, Greece, 21–24 June 2016; pp. 840–845.
79. Ventura Diaz, P.; Yoon, S. High-fidelity computational aerodynamics of multi-rotor unmanned aerial vehicles. In Proceedings of the 2018 AIAA Aerospace Sciences Meeting, Kissimmee, FL, USA, 8–12 January 2018; p. 1266.
80. Cazaurang, F.; Cohen, K.; Kumar, M. *Multi-Rotor Platform Based UAV Systems*; Elsevier: Amsterdam, The Netherlands, 2020.
81. Panagiotou, P.; Yakinthos, K. Aerodynamic efficiency and performance enhancement of fixed-wing UAVs. *Aerosp. Sci. Technol.* **2020**, *99*, 105575. [\[CrossRef\]](#)
82. Bhandari, V. Use of Technology in Disaster Management. *Unity J.* **2022**, *3*, 292–304. [\[CrossRef\]](#)
83. Euronews. Researchers from Switzerland Are Using Drones to Monitor the Health of the Rainforest, 2023. Available online: <https://www.euronews.com/next/2023/07/28/researchers-from-switzerland-are-using-drones-to-monitor-the-health-of-the-rainforest> (accessed on 21 May 2024).
84. Hafeez, S.; Khan, A.R.; Al-Quraan, M.; Mohjazi, L.; Zoha, A.; Imran, M.A.; Sun, Y. Blockchain-Assisted UAV Communication Systems: A Comprehensive Survey. *IEEE Open J. Veh. Technol.* **2023**, *4*, 558–580. [\[CrossRef\]](#)
85. Fotouhi, A.; Qiang, H.; Ding, M.; Hassan, M.; Giordano, L.G.; Garcia-Rodriguez, A.; Yuan, J. Survey on UAV cellular communications: Practical aspects, standardization advancements, regulation, and security challenges. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 3417–3442. [\[CrossRef\]](#)
86. Gupta, L.; Jain, R.; Vaszkun, G. Survey of important issues in UAV communication networks. *IEEE Commun. Surv. Tutor.* **2015**, *18*, 1123–1152. [\[CrossRef\]](#)
87. Li, B.; Fei, Z.; Zhang, Y.; Guizani, M. Secure UAV communication networks over 5G. *IEEE Wirel. Commun.* **2019**, *26*, 114–120. [\[CrossRef\]](#)
88. Liu, Y.; Gao, J.; Lu, Y.; Cao, R.; Yao, L.; Xia, Y.; Han, D. Lightweight Blockchain-Enabled Secure Data Sharing in Dynamic and Resource-limited UAV Networks. *IEEE Netw.* **2024**. [\[CrossRef\]](#)
89. Mehta, P.; Gupta, R.; Tanwar, S. Blockchain envisioned UAV networks: Challenges, solutions, and comparisons. *Comput. Commun.* **2020**, *151*, 518–538. [\[CrossRef\]](#)
90. Alqahtani, H.; Kumar, G. Machine learning for enhancing transportation security: A comprehensive analysis of electric and flying vehicle systems. *Eng. Appl. Artif. Intell.* **2024**, *129*, 107667. [\[CrossRef\]](#)
91. Bithas, P.S.; Michailidis, E.T.; Nomikos, N.; Vouyioukas, D.; Kanatas, A.G. A survey on machine-learning techniques for UAV-based communications. *Sensors* **2019**, *19*, 5170. [\[CrossRef\]](#)
92. Tlili, F.; Ayed, S.; Fourati, L.C. Exhaustive distributed intrusion detection system for UAVs attacks detection and security enforcement (E-DIDS). *Comput. Secur.* **2024**, *142*, 103878. [\[CrossRef\]](#)
93. Zeng, Y.; Wu, Q.; Zhang, R. Accessing from the sky: A tutorial on UAV communications for 5G and beyond. *Proc. IEEE* **2019**, *107*, 2327–2375. [\[CrossRef\]](#)

-
94. Mozaffari, M.; Saad, W.; Bennis, M.; Nam, Y.H.; Debbah, M. A tutorial on UAVs for wireless networks: Applications, challenges, and open problems. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 2334–2360. [[CrossRef](#)]
 95. Mohsan, S.A.H.; Othman, N.Q.H.; Li, Y.; Alsharif, M.H.; Khan, M.A. Unmanned aerial vehicles (UAVs): Practical aspects, applications, open challenges, security issues, and future trends. *Intell. Serv. Robot.* **2023**, *16*, 109–137. [[CrossRef](#)]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.