Article

Not peer-reviewed version

A Survey on Reputation Systems for UAV Networks

Simeon Ogunbunmi , Yu Chen * , Erik Blasch , Genshe Chen

Posted Date: 1 May 2024

doi: 10.20944/preprints202405.0075.v1

Keywords: Reputation System; Unmanned Aerial Vehicle (UAV); Trust; Security; Feedback System

Article

A Survey on Reputation Systems for UAV Networks

Simeon Ogunbunmi [1], Yu Chen [1,*], Erik Blasch [2] and Genshe Chen [3]

[1] Binghamton University, Binghamton, NY 13902; {sogunbu1,ychen}@binghamton.edu
[2] The U.S. Air Force Research Laboratory, Rome, NY 13441; erik.blasch@gmail.com
[3] Intelligent Fusion Technology, Inc., Germantown, MD 20874; 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 UAV networks' highly dynamic and adaptable environments. Decentralized reputation systems emerge as a promising solution to enhance 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. It highlights the crucial role of reputation systems in strengthening trust, security, and privacy throughout these networks and discusses various strategies 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

1. Introduction

In the past decades, Unmanned Aerial Vehicles (UAVs), often called drones, have become very popular and useful in various sectors, not just in the military alone [1]. UAV technology has changed how we collect information and interact with our surroundings in various applications, ranging from military [2], public safety [3], delivery [4], agriculture [5], healthcare [6], security [7], to disaster responses [8]. One important thing about UAVs is the ability to work independently without being controlled by humans or pilots. This is a big change in how vehicles usually work. This ability allows UAVs to conduct challenging tasks in extreme environments like disaster recovery scenarios, where it is compelling 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 [9].

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. This data link is essential for timely communication and pivotal for delay-sensitive tasks. UAVs use radio waves to communicate, which allows them to send and receive data in places that are either difficult to access or hazardous for human operators [10].

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 [11]. Therefore, it is imperative to address the security requirements of UAVs comprehensively, particularly as their applications continue to expand and diversify. 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 [11]. This highlights the urgent need to develop robust security protocols and mechanisms to safeguard UAV networks from various threats [12].

 doi:10.20944/preprints202405.0075.v1

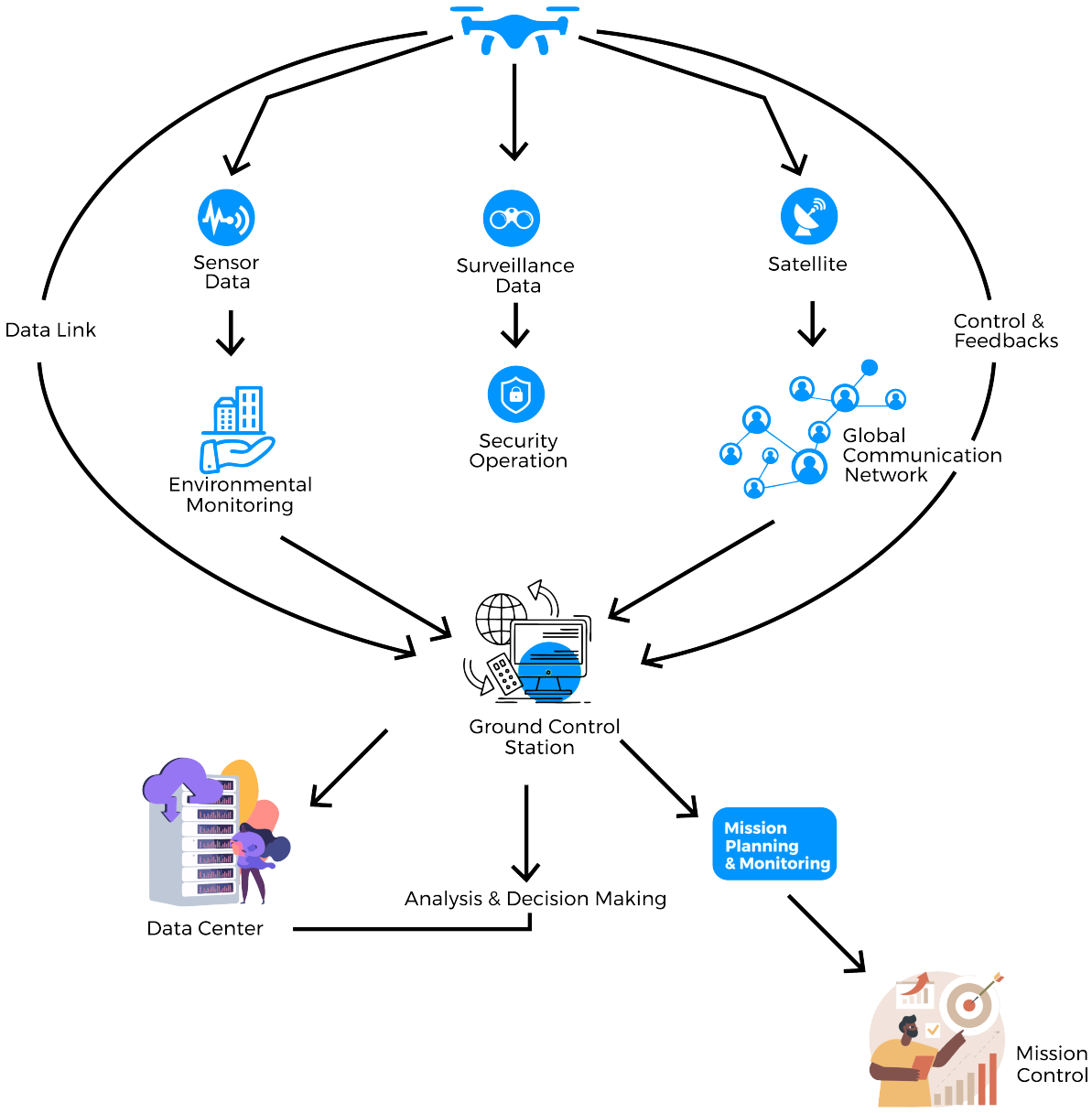

Figure 1. UAV Communication Infrastructure.

 doi:10.20944/preprints202405.0075.v1

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 [13]. 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 UAVs' safe and consistent functioning [14]. 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 [15]. 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 [16], 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. This platform rating has an impact on the reputation of UAV operators.

A high reputation score within the UAV ecosystem has various benefits, including enhanced access rights, motivating individuals to contribute positively, and upholding their trust [17]. Consistent rendering and providing of trustworthy service and deliveries enable service requesters to have more transactions done with the service providers, thereby increasing the trustworthiness and reputation of the providers [18]. Meanwhile, delivering poor quality jobs or a low task completion rate will ruin one's reputation score. However, by making worthwhile contributions to the system and providing non-malicious service, the reputation scores could be restored [19].

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 data collected by UAVs [20]. 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 [21].

This paper aims to present the big picture of the multifaceted landscape of UAV systems, focusing on security, reputation, and trust. A comprehensive 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 will provide valuable insights into the evolving dynamics of UAV systems in an era where they are poised to revolutionize industries.

To present a thorough view of the reputation systems in the context of UAV networks, 70 papers have been selected, which were published in the period from 2006 to the present time (April 2024), as shown in Figure 2, and published in well-recognized research journals and conferences, as shown in Figure 3. These papers contributed to the comprehensive understanding of the current state of the UAV reputation system. These contribute to a comprehensive view of the state-of-the-art research, challenges, and potential solutions in the field of reputation systems, underlining the diverse approach to addressing trust in complex networks.

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 various trust and reputation management that have been proposed. Section 4 describes the background knowledge of UAV 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 conclusions and future directions.

 doi:10.20944/preprints202405.0075.v1

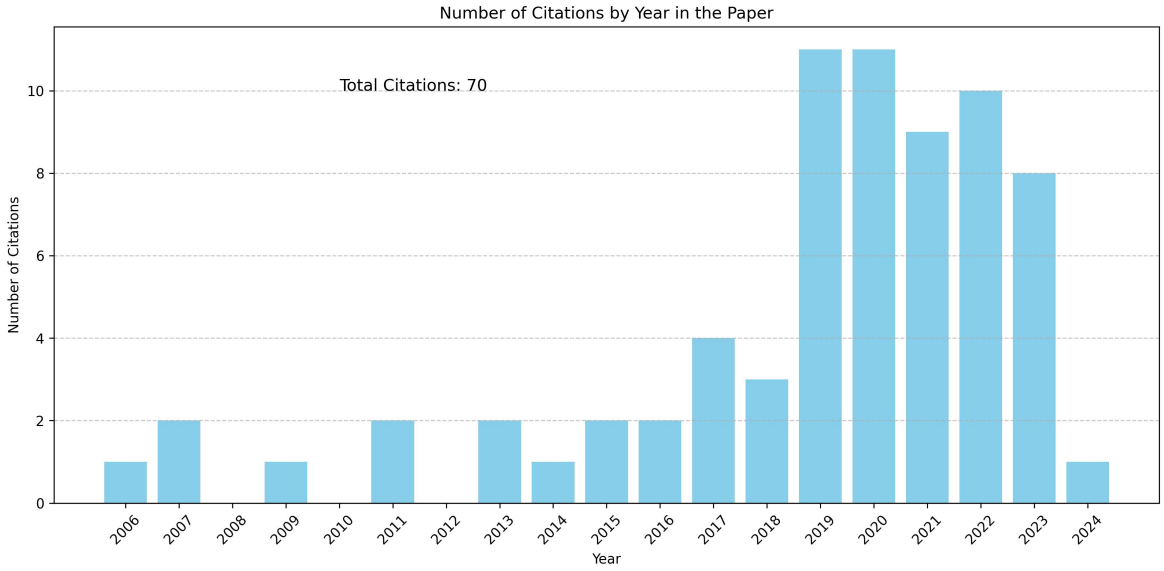

Figure 2. The distribution of selected papers.

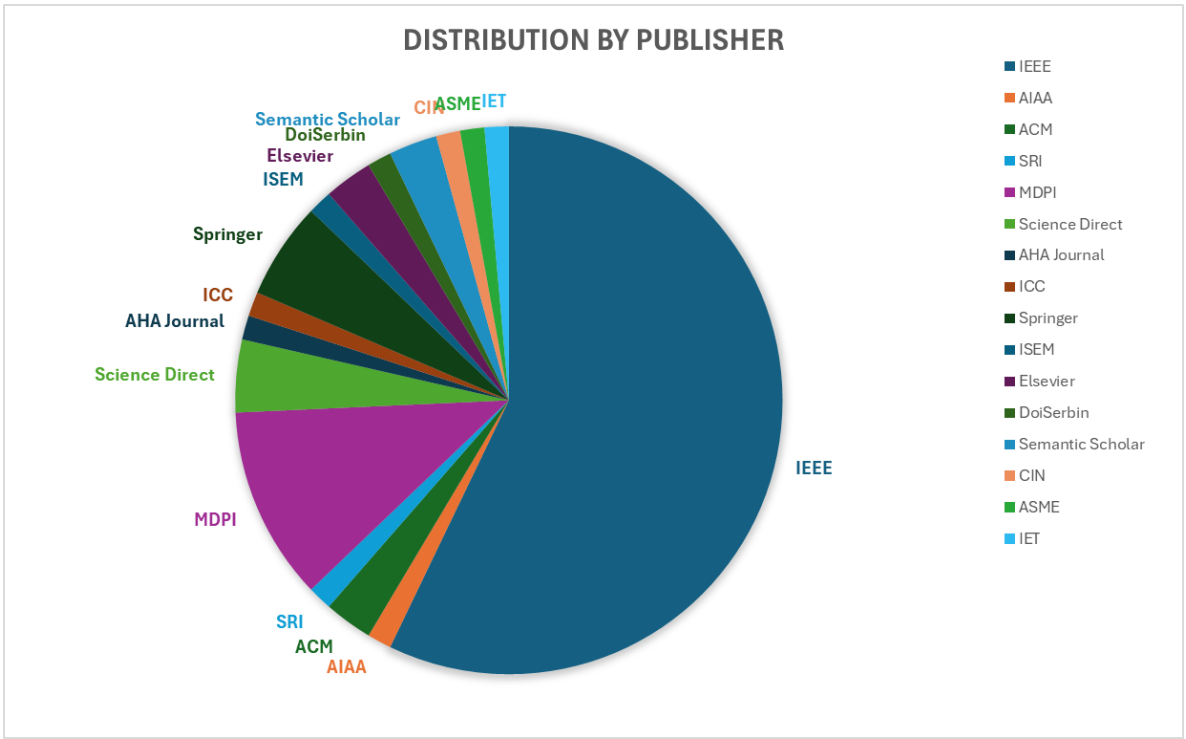

Figure 3. Distribution By Publisher

 doi:10.20944/preprints202405.0075.v1

2. Classes/Types of UAV Devices

There are various types and classes of UAVs or UAV systems based on their unique designs, flights, capacities, and applications. They can be classified 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 [22]. The single-rotor structure enables superb lift and direction control, allowing varieties of aerobatic performances and swift turns. High agility provides them the ability to hover around, 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. The distinguishing features make them a preferable option for both 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 [23]. 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, 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 [24]. The 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 sizes, weights, 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 outfitted 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 their multi-rotor UAVs. These UAVs are known for their efficiency and swiftness [25]. 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 duration, sometimes for several hours, before the need for refueling or recharging. 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 quite useful. Their proficiency in covering vast regions quickly, such as crop monitoring or topographical surveys, makes them ideal for activities like aerial photography, mapping, surveying, Aerial mapping

 doi:10.20944/preprints202405.0075.v1

and surveying, asset inspection, long-range payload delivery, and unmanned aerial refueling They have also established themselves in long-distance package delivery market, especially in isolated or rural locations.

3. A Glimpse on 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. This capability has revolutionized surveillance and information gathering in both civilian and national 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 radio waves 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.

Although UAV applications have demonstrated great potential to enhance community safety and comfort, they could also have disastrous consequences if the UAV networks are compromised and utilized improperly. Due to inherent resource constraints, UAVs are vulnerable to both 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 the UAV's circuit, potentially allowing them to obtain all the stored data if 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 addressed in the 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 scholarly ideas [4]. Research agendas for trust and reputation systems were suggested to examine current trends and advancements, highlighting the necessity of finding appropriate online alternatives to conventional cues of reputation and trust, identifying pertinent information pieces 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 IoT middleware survey, the significance of trust in security, privacy, usability, and user experience was highlighted [26]. A trust-based, privacy-protected method for promoting nodes in social online networks was proposed [27]. 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 [20]. For determining service reputation, a two-phase procedure was suggested [28], 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 [29]. 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 [30]. It facilitates comparisons within a single framework and offers insights into the advantages and disadvantages of various systems. The paper also examines the system components susceptible to each attack category and class assaults

 doi:10.20944/preprints202405.0075.v1

against reputation systems [30]. In addition, the paper examines 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 [31]. 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 SDN technologies. This protocol's major goal is to restrict access to malicious tags and permit and record all of their 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 Software-Defined Network (SDN) into the IoT, offers a novel method of managing trust by incorporating a cross-layer authorization protocol [31]. This established an Organization Reputation Evaluation Scheme (ORES) and a Behavior-based Reputation Evaluation Scheme for the Node (BES) to build trust [32]. The effectiveness of BES and ORES was confirmed by theoretical analysis and simulation findings.

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

Sections 4, 5, and 6 together provide a comprehensive view of the landscape for UAV networks' trust, reputation, and feedback systems, discussing the systems, presenting a taxonomy of attacks, and illustrating the 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, or interactions without fear of negative consequences. Trust reduces the perceived danger of communicating with unknown persons in an online setting [33].

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 [14]. 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 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 commitment 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 on behalf of the service it renders. 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 [11]. The reliability of UAV devices is enhanced by their consistency and accuracy in delivering packages within a designated time frame. Also, factors like flight history with minimal technical issues, redundant systems (e.g., backup batteries) to ensure mission completion in case of failure,

 doi:10.20944/preprints202405.0075.v1

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 [4,11]. Also, it is the confidence, belief, and trust that individuals have in the decisions made by others. This focuses on the ability to make optimal decisions 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 [34]. 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 [14]. 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. Behavioural 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 [11,14]. 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 [12]. 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

This is the trust established between different entities due to personal experience, interaction, or observation made among themselves, based on the 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 [32]. Direct trust involves reciprocal relationships where trust is built and acquired mutually based on shared experience and interaction. Considering that if 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. This 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.

 doi:10.20944/preprints202405.0075.v1

4.1.5. Derived trust

On the other hand, derived trust is inferred or derived from 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 third party or trusted sources to inform their decision [14]. Suppose they 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

These systems' reputation and trust are highly necessary, and they determine the genuineness and reliability of the data and information sent between the UAV systems in the 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. This enables the users to decide who they will trust or make transactions with and to what extent to which to trust them based on the reputation data of the devices. Reputation can have both quantitative and qualitative components. Quantitatively, it might be numerical ratings, scores, or badges issued to users depending on their activities and interactions. In 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 another behavior. Ratings, assessments, critiques, and recommendations are all forms of feedback. It allows the community to assess a user's reputation collectively.

A high reputation comes with various benefits. For example, people with a high reputation may earn service provider rights or access to restricted site areas. This motivates 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 activities. Figure 4 shows various types of reputation systems discussed in this section, along with the challenges.

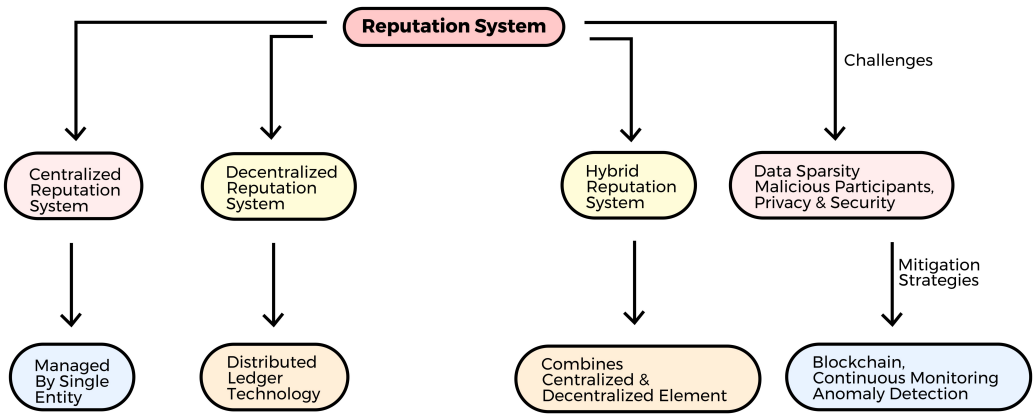

Figure 4. The Reputation System

 doi:10.20944/preprints202405.0075.v1

4.2.1. Centralized Reputation System

This is a reputation system that is run by a single, centralized 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 manage their data effectively. A single governing authority facilitates implementing this particular system, making management reasonably simple [35]. Nevertheless, this approach has drawbacks, as it is more susceptible to single-point-of-failure attacks and other cyberattacks. A compromise in the system may result in further possible problems and issues with the privacy of the data sent over the network.

4.2.2. Decentralized Reputation System

Using distributed ledger technology, or blockchain, each participant's reputation data is 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 is locally managed, saved, and controlled on their nodes [34], which collectively establish an agreement through a distributed consensus process to validate the data. Due to its distributed nature, the decentralized reputation system is more resilient to fraud, manipulation, and attacks than the centralized system because no single party controls the reputation data [4], increasing 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

This hybrid reputation system has elements from both centralized and decentralized systems. The centralized system is responsible for collecting and aggregating data, while the decentralized network is responsible for storing reputation data. By raising resilience and security against manipulation and elevating the degree of trust and simplicity, the balance between centralization and decentralization is achieved according to the particular demands and requirements[35]. This type of reputation system is used by networks like Stack Overflow, Steemit, and GitHub.

4.3. Reputation data

Reputation systems in any application, e-commerce, health care, agriculture, and more, use data and information to generate and determine an entity's or service's reputation. This can be grouped into two categories: Manual and Automatic data [21]. 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 it to numerical data. This is then used in the calculation of the reputation of an entity, which thereby decreases or increases the reputation of the users based on the proposed strategy and algorithm [21].

4.4. Challenges of Reputation System

Several challenges and issues are being faced by reputation systems, as shown in Figure 4, and their data sent over the network, which includes 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

 doi:10.20944/preprints202405.0075.v1

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 is 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 introduces and explores the concepts and models for optimizing the efficiency of UAV-assisted data gathering in wireless sensor networks to prevent this attack was proposed [36]. The proposed approach reduced data sparsity by optimizing 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 [36], the method increases the percentage of served sensor nodes and minimizes 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 the 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 [31]. The paper suggests the Behavior-based Reputation Assessment Scheme for the Node (BES) and the 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 nodes' and tags' information exchanges. BES can recognize and evaluate negative node behavior, such as assaults or anomalous activity, by analyzing this evidence.

In contrast, ORES assesses organizations' standing by considering the present conditions of all their 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 suggests 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 improved the security and trust in the IoT system [31].

4.4.3. Privacy and Security

IoT devices, in general, have encountered numerous difficulties and attacks. 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. This could give malevolent and unauthorized individuals access to manipulate the data. Decentralized architecture, 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 the reduction of 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 [37]. 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 [37].

Another potential method for safeguarding the privacy and integrity of the reputation data out to UAV systems involves the utilization of Blockchain-based Anonymous Reputation System (BARS) [38], 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 [38], namely Certificate and

 doi:10.20944/preprints202405.0075.v1

Revocation Blockchain (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 [38].

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 is facilitated by 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 handle the difficulties posed by utilizing robust reputation systems in UAV systems.

4.5. Feedback

Feedback techniques can be critical for assuring UAV devices' safety and compliance. Reporting safety accidents or breaches can assist regulatory agencies, and organizations take necessary safety measures. Data quality and trust are critical in applications where UAVs collect data. This involves a cycle of the inputs from the sensed environment and is processed through computational and outputs are the actions the UAV's actuators take based on the processing results as shown in Figure 5. These outputs are being 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 may 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 may use reputation systems to assist customers in selecting trustworthy operators.

Users can rate UAV operators' service quality, timeliness, and professionalism, which might 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 [39]. This discussed how the system can 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, educational institutions, and rating-based companies [39].

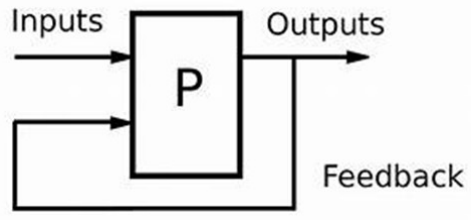

Figure 5. The Feedback System.

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

4.5.1. Input Unit

The input unit refers to the data and signals which is received through sensed data from sensors like the barometer, GPS, camera, and LiDAR, which provide information like position altitude, longitude, latitude, speed, and some other environmental factors [40]. The input system consists of the

 doi:10.20944/preprints202405.0075.v1

control commands containing instructions sent by a remote control or autopilot system, indicating what the UAV should do.

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 the control system, which 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, or truth values. These also involve the algorithms that determine the 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 taken by the UAV's actuators 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 [40], 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 correction's success.

5. Taxonomy Of Reputation Attacks

The paper analyzes the significant changes in a node's reputation, whether it exhibits a substantial increase or decrease in the reputation score [41]. When a node transmits a real or fake message, a way to update the reputation values gradually is introduced by increasing or decreasing the node's reputation. The 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 [41]. 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 suggested approach in the study seeks to address the issue of abrupt reputation changes[41]. We can classify the challenges facing reputation in UAV systems into two classes as shown in Figure **??**.

5.1. Reputation Manipulation Attacks

A reputation manipulation attack tends 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 the 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 deceptive 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.

 doi:10.20944/preprints202405.0075.v1

In the context of a UAV reputation system, a Sybil attacker can generate numerous imaginary UAV identities, each accompanied by an artificially false positive reputation [42]. Subsequently, these malicious UAVs might 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. The use of a substantial quantity of pseudonyms by attackers might be employed to exert influence on the system through numerous tactics, including the ability to outvote other participants [43].

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 might 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:

- *Decentralized Blockchain:* Implementing a decentralized blockchain-based system for managing UAV reputation can significantly augment security measures [44]. The inherent characteristic of blockchain technology guarantees that once a reputation is recorded and stored, it becomes resistant to modification or tampering. Verifying reputation updates is facilitated through a consensus process, mitigating 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 [44]. 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 input 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 activity, such as abrupt increases in reputation scores, which could signify a Sybil attack or other types of manipulation [45]. Utilization of continuous monitoring and anomaly detection tools to discern 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 systems.

5.1.2. Collusion Attack

When numerous adversaries work together to compromise the trustworthiness of these UAVs, this is known as a “Collusion Attack." Collusion 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 [46]. The manipulation of UAV reputations can lead to various negative outcomes [30], such as weakened confidence in self-governing systems, skewed decision-making procedures, inaccurate information, security lapses, or 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.

 doi:10.20944/preprints202405.0075.v1

5.1.3. Self Promotion attack

A self-promotion attack is a deceitful strategy employed by an individual or organization to deliberately enhance, gain, and increase their reputation inside a certain system or network, typically for personal advantage or gain [30]. This 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 [47]. Self-promotion attacks within UAV systems can yield significant ramifications, encompassing the erosion of trust, unfair competition, and data quality degradation.

5.2. Reputation Poisoning Attack

This term may refer to a specific attack that attempts to taint a UAV system's or its operator's reputation. This may entail disseminating misleading or negative information through digital platforms or alternative methods to undermine the system's reputation, which is referred to as a Slandering attack [47]. The nature of the attack does not necessarily entail manipulation but rather centers on the degradation of reputation by disseminating bad or inaccurate information. The utilization of compromised UAV characterizes a reputation-poisoning assault to introduce malevolent data into the reputation system [48]. 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 classify the reputation poisoning attack as:

5.2.1. False Feedback Attack

A false feedback attack refers to intentionally disseminating misleading or inaccurate feedback by an attack to impact the reputation of a UAV adversely [49]. This 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 [50]. The main objective of this 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 this type of 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 [50]. This may involve manipulating the reputation system to incorporate fabricated accounts of misconduct. This attacker aims to manipulate the reputation of UAVs by exploiting vulnerabilities within the reputation system or compromising trusted UAVs. This manipulation can impact the perception of UAV trustworthiness among stakeholders.

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

This attack involves an attacker intercepting and manipulating reputation data as it passes from the reputation system to the UAV system. The attacker deliberately positions themselves in the communication channel between two parties [51]. Different methods are available to achieve this, such as spoofing or hijacking unencrypted Wi-Fi. At 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 the transmitted data. The attacker's primary objective is manipulating UAVs' reputation by altering

 doi:10.20944/preprints202405.0075.v1

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 perceptions 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 [52].

Tables 1 - 3 focus on relevant and recent research that addresses various aspects of UAV reputation systems, including the challenges, proposed models, and proposed solutions for diverse challenges, such as blockchain and machine learning (ML), for improving the UAV network's security and efficiency.

Table 1. Different Approaches Used with their Weaknesses

	Approach	**Model/Method**	**Goals**	**Weaknesses**
[53]	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
[41]	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 purposes in UAVs and IoTs	It does not explicitly mention the trade-offs or limitations of the proposed reputation management framework
[54]	Auction-based game theory, ML, and blockchain	ML	The autonomous selection and operation of UAV 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
[55]	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
[56]	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
	Approach	**Model/Method**	**Goals**	**Weaknesses**

 doi:10.20944/preprints202405.0075.v1

Table 2. Different Approaches Used with their Weaknesses

	Approach	Model/Method	Goals	Weaknesses
[57]	Design and implementation of the 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
[38]	Exploit 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 eliminate 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)
[58]	ReFIoV, which leverages ML and the 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 nodes' cooperation
[19]	Dynamic decentralized reputation system that utilizes blockchain technology for reputation storage and update	Full Decentralization, General-Purpose, Global Reputation, Privacy, and employed Technologies	This enhances the security and decentralization of the reputation management system in decentralized environments	The potential limitations of blockchain scalability, which requires special attention in decentralized systems relying on blockchain
[59]	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

 doi:10.20944/preprints202405.0075.v1

Table 3. Different Approaches Used with their Weaknesses

	Approach	Model/Method	Goals	Weaknesses
[60]	The malicious UAV detection algorithm (MDA) based on linear regression and 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 the UAV ad-hoc network
	Approach	**Model/Method**	**Goals**	**Weaknesses**
[61]	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 the system's 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
[62]	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 probabilities and utilities of UAVs	It does not thoroughly discuss the potential scalability issues or computational overhead associated with the blockchain-based secure data transmission scheme
[63]	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
[64]	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

Having discussed various challenges and issues faced by Trust and Reputation systems, different defending mechanisms have been proposed by different authors, which have offered significant advancements in terms of security, data integrity, and efficient management ranging from blockchain to ML approach and Intrusion Detection approach as shown in Figure 7 as they host various advantages across various domains in the networks. Several solutions can be adopted to mitigate these attacks, which include:

 doi:10.20944/preprints202405.0075.v1

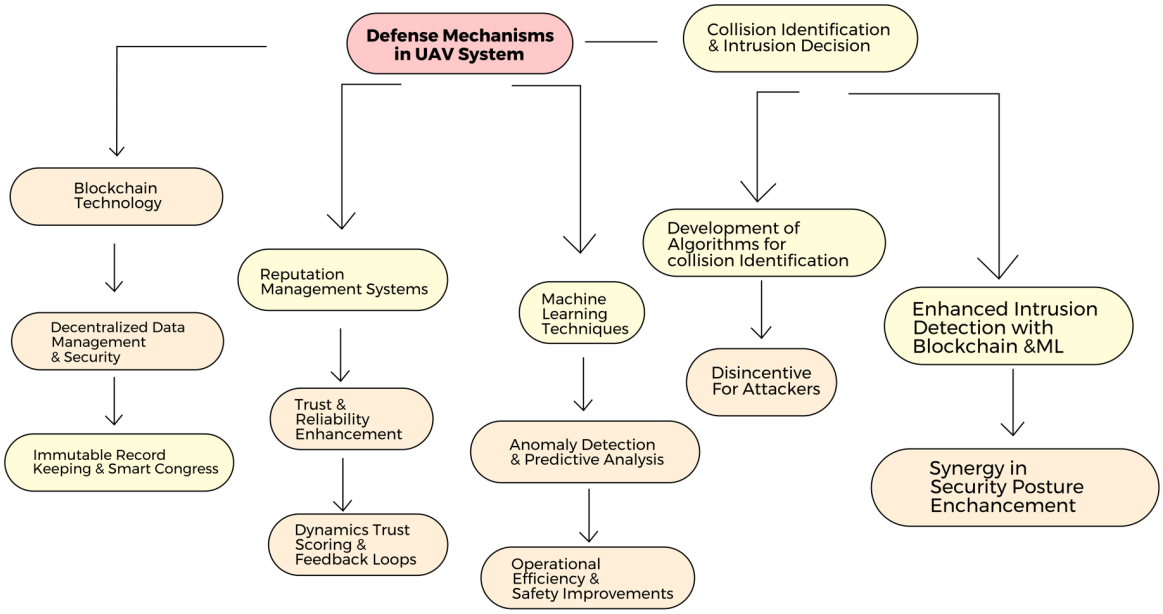

Figure 7. Defense Mechanism.

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, the blockchain infrastructure would facilitate 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 that records blocks securely linked together through cryptographic hashes is a vital advantage of implementing the technology in the system, [59,63]. This technology enhances flexibility, survivability, security, and programmability and is suitable for 5G-oriented UAV networking [65]. A major attack in IoT devices, which is the single point of failure attack, is 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 [19,65].

Across several cyber threats in a network, blockchain technology has been a defense technology to mitigate this threat. Data integrity and the verification of the authenticity of the data have been safeguarded in swarms of UAVs [66]. This is essential in situations where secure data transmission is required and necessary, such as surveillance missions and remote sensing [57,66]. Moreover, the challenges of isolated applications operating on separate and different blockchain systems are being mitigated with the help of cross-blockchain platforms [61,67]. 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 the UAV networks context [62]. The introduction of a spectrum of scenarios related to UAV networks that may leverage the potentials of the currently available cross-blockchain solutions was also discussed [67].

UAV-assisted blockchain systems have significantly contributed to optimizing energy for UAV devices and most battery-powered IoT devices [68]. To minimize the energy consumption of the 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 [38], the bandwidth allocation and the trajectory of the UAV is formulated as a non-convex optimization problem and solved via a Successive Convex Approximation (SCA) algorithm [68]. This can reduce energy consumption, which has helped extend the duration of missions and enhance operational efficiency [53,54].

 doi:10.20944/preprints202405.0075.v1

6.2. Reputation Management System

Using reputation management systems for UAVs is crucial in mitigating different attacks on UAV systems. This 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 and continuous monitoring and adaptation to the constantly changing online environment. This 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 or 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 the 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 data 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. This includes obstacle avoidance, flying formation, and autonomous decision-making [69]. 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. Also, 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 [70]. This paper proposes a methodology 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 to boost edge intelligence for UAVs. Considering the limited energy supply of UAVs, how to minimize UAVs' 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 [71].

6.4. Collusion Identification

Identifying collusion plays a vital role in the defense against collusion attacks. Developing algorithms and models specifically tailored to identify 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 enhance the reputation of one of the members intentionally. 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 the challenges of their activities.

 doi:10.20944/preprints202405.0075.v1

Implementation of Intrusion Detection also plays a vital role in safeguarding and mitigating unauthorized access and malicious activities [50]. Incorporating Blockchain Technology and ML techniques ensures integrity and security by enhancing Intrusion Detection. Combining blockchain and ML in Intrusion Detection enhances the overall security posture of UAV networks. Blockchain ensures the integrity and tamper-proof nature of the intrusion detection log, while ML analyzes this data for patterns and anomalies. This synergy strengthens the network's ability to detect and mitigate known and novel security threats, safeguarding critical UAV operations.

7. Conclusions

This paper aims to provide a comprehensive overview of the critical role of reputation systems in the security and privacy of unmanned aerial vehicle (UAV) networks. As UAVs become increasingly popular in more and more applications, from delivery services to public safety surveillance, robust reputation and trust mechanisms are paramount. These systems bolster the security framework and enhance the reliability and efficiency of UAV operations within the broader context of smart cities, the Internet of Things (IoT), and autonomous systems.

This paper has discussed several vulnerabilities posed by malicious actors who attempt to exploit UAV systems. The 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 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 efficient UAV ecosystem. This, in turn, supports the broader integration of digital systems, including IoT devices and autonomous vehicles, paving the way for a more interconnected and automated future.

In conclusion, this paper presents a detailed analysis of the existing reputation and trust systems, elucidation of key challenges, and exploration of innovative mitigation strategies. They are critical for advancing the field and ensuring the sustainable growth of UAV networks and other IoT networks or smart city systems. We hope this work will inspire more discussions in the community and spark more novel ideas to safeguard and enhance the burgeoning landscape of UAV applications.

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 work was partially supported by the U.S. Air Force Office of Scientific Research (AFOSR) STTR Program via contracts FA9550-22-P-0011.

Acknowledgments: The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the U.S. Air Force.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

 doi:10.20944/preprints202405.0075.v1

5G	the 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
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
UAV	Unmanned Aerial Vehicles

References

1. Muchiri, G.; Kimathi, S. A review of applications and potential applications of UAV. Proceedings of the Sustainable Research and Innovation Conference, 2022, pp. 280–283.
2. Utsav, A.; Abhishek, A.; Suraj, P.; Badhai, R.K. An IoT based UAV network for military applications. 2021 Sixth International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET). IEEE, 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.
4. Jøsang, A.; Ismail, R.; Boyd, C. A survey of trust and reputation systems for online service provision. *Decision support systems* **2007**, *43*, 618–644.
5. Tsouros, D.C.; Bibi, S.; Sarigiannidis, P.G. A review on UAV-based applications for precision agriculture. *Information* **2019**, *10*, 349.
6. Angraal, S.; Krumholz, H.M.; Schulz, W.L. Blockchain technology: applications in health care. *Circulation: Cardiovascular quality and outcomes* **2017**, *10*, e003800.
7. Hein, D.; Kraft, T.; Brauchle, J.; Berger, R. Integrated uav-based real-time mapping for security applications. *ISPRS International Journal of Geo-Information* **2019**, *8*, 219.
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.
9. 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, 2021; pp. 81–102. doi:https://doi.org/10.1016/B978-0-12-820276-0.00011-X.
10. 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 Communications Surveys & Tutorials* **2021**, *23*, 2802–2832.
11. 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.

12. 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 Transactions on Engineering Management* **2019**, *67*, 1231–1243.
13. Liang, Q.; Gan, X. Research on trust evaluation algorithm for e-commerce based on reputation. 2011 International Conference on Business Computing and Global Informatization. IEEE, 2011, pp. 39–42.
14. Fotia, L.; Delicato, F.; Fortino, G. Trust in edge-based internet of things architectures: state of the art and research challenges. *ACM Computing Surveys* **2023**, *55*, 1–34.
15. 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). 2019 International Conference on Information Technology (ICIT). IEEE, 2019, pp. 257–262.
16. Battah, A.A.; Iraqi, Y.; Damiani, E. A Trust and Reputation System for IoT Service Interactions. *IEEE Transactions on Network and Service Management* **2022**, *19*, 2987–3005.
17. Mrabet, K.; El Bouanani, F.; Ben-Azza, H. Dynamic Decentralized Reputation System from Blockchain and Secure Multiparty Computation. *Journal of Sensor and Actuator Networks* **2023**, *12*, 14.
18. Ogunbunmi, S.; Hatmai, M.; Xu, R.; Chen, Y.; Blasch, E.; Ardiles-Cruz, E.; Aved, A.; Chen, G. A Lightweight Reputation System for UAV Networks. Security and Privacy in Cyber-Physical Systems and Smart Vehicles; Chen, Y.; Lin, C.W.; Chen, B.; Zhu, Q., Eds.; Springer Nature Switzerland: Cham, 2024; pp. 114–129.
19. 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.
20. El Husseini, A.; M'hamed, A.; El Hassan, B.; Mokhtari, M. Trust-Based Authentication Scheme with User Rating for Low-Resource Devices in Smart Environments. *Personal Ubiquitous Comput.* **2013**, *17*, 1013–1023. doi:10.1007/s00779-012-0548-8.
21. Pereira, R.H.; Gonçalves, M.J.; Magalhães, M.A.G. Reputation Systems: A framework for attacks and frauds classification. *Journal of Information Systems Engineering and Management* **2023**, *8*.
22. Carholt, O.; Fresk, E.; Andrikopoulos, G.; Nikolakopoulos, G. Design, modelling and control of a single rotor UAV. 2016 24th Mediterranean Conference on Control and Automation (MED). IEEE, 2016, pp. 840–845.
23. Ventura Diaz, P.; Yoon, S. High-fidelity computational aerodynamics of multi-rotor unmanned aerial vehicles. 2018 AIAA Aerospace Sciences Meeting, 2018, p. 1266.
24. Cazaurang, F.; Cohen, K.; Kumar, M. *Multi-rotor Platform Based UAV Systems*; Elsevier, 2020.
25. Panagiotou, P.; Yakinthos, K. Aerodynamic efficiency and performance enhancement of fixed-wing UAVs. *Aerospace Science and Technology* **2020**, *99*, 105575.
26. Ngu, A.H.; Gutierrez, M.; Metsis, V.; Nepal, S.; Sheng, Q.Z. IoT Middleware: A Survey on Issues and Enabling Technologies. *IEEE Internet of Things Journal* **2017**, *4*, 1–20. doi:10.1109/JIOT.2016.2615180.
27. Guo, L.; Zhang, C.; Fang, Y. A Trust-Based Privacy-Preserving Friend Recommendation Scheme for Online Social Networks. *IEEE Transactions on Dependable and Secure Computing* **2015**, *12*, 413–427.
28. Wu, Y.; Yan, C.; Ding, Z.; Liu, G.; Wang, P.; Jiang, C.; Zhou, M. A Novel Method for Calculating Service Reputation. *IEEE Transactions on Automation Science and Engineering* **2013**, *10*, 634–642. doi:10.1109/TASE.2013.2238231.
29. Ghahramani, M.H.; Zhou, M.; Hon, C.T. Toward cloud computing QoS architecture: analysis of cloud systems and cloud services. *IEEE/CAA Journal of Automatica Sinica* **2017**, *4*, 6–18. doi:10.1109/JAS.2017.7510313.
30. Hoffman, K.; Zage, D.; Nita-Rotaru, C. A survey of attack and defense techniques for reputation systems. *ACM Computing Surveys (CSUR)* **2009**, *42*, 1–31.
31. Chen, J.; Tian, Z.; Cui, X.; Yin, L.; Wang, X. Trust architecture and reputation evaluation for internet of things. *Journal of Ambient Intelligence and Humanized Computing* **2019**, *10*, 3099–3107.
32. 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. *Computer Science and Information Systems* **2011**, *8*, 1207–1228.
33. Malik, S.; Dedeoglu, V.; Kanhere, S.S.; Jurdak, R. Trustchain: Trust management in blockchain and iot supported supply chains. 2019 IEEE International Conference on Blockchain (Blockchain). IEEE, 2019, pp. 184–193.
34. Hendrikx, F.; Bubendorfer, K.; Chard, R. Reputation systems: A survey and taxonomy. *Journal of Parallel and Distributed Computing* **2015**, *75*, 184–197.
35. Tu, Z.; Zhou, H.; Li, K.; Song, H.; Yang, Y. A blockchain-based trust and reputation model with dynamic evaluation mechanism for IoT. *Computer Networks* **2022**, *218*, 109404.
36. Putra, G.D.; Dedeoglu, V.; Kanhere, S.S.; Jurdak, R. Trust management in decentralized iot access control system. 2020 IEEE international conference on blockchain and cryptocurrency (ICBC). IEEE, 2020, pp. 1–9.

37. Jain, P.; Gyanchandani, M.; Khare, N. Differential privacy: its technological prescriptive using big data. *Journal of Big Data* **2018**, *5*, 1–24.
38. Lu, Z.; Wang, Q.; Qu, G.; Liu, Z. BARS: A Blockchain-Based Anonymous Reputation System for Trust Management in VANETs. 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), 2018, pp. 98–103. doi:10.1109/TrustCom/BigDataSE.2018.00025.
39. Rahman, M.M.; Rifat, M.M.H.; Tanin, M.Y.; Hossain, N. A feedback system using blockchain technology. 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS), 2020, pp. 1114–1118. doi:10.1109/ICISS49785.2020.9315989.
40. Lee, H.; Yoon, J.; Jang, M.S.; Park, K.J. A robot operating system framework for secure uav communications. *Sensors* **2021**, *21*, 1369.
41. 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). 2019 International Conference on Information Technology (ICIT), 2019, pp. 257–262. doi:10.1109/ICIT48102.2019.00052.
42. Levine, B.N.; Shields, C.; Margolin, N.B. A survey of solutions to the sybil attack. *University of Massachusetts Amherst, Amherst, MA* **2006**, *7*, 224.
43. Zhang, K.; Liang, X.; Lu, R.; Shen, X. Sybil attacks and their defenses in the internet of things. *IEEE Internet of Things Journal* **2014**, *1*, 372–383.
44. 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 Journal of Vehicular Technology* **2023**.
45. Marche, C.; Nitti, M. Trust-related attacks and their detection: A trust management model for the social IoT. *IEEE Transactions on Network and Service Management* **2020**, *18*, 3297–3308.
46. Meamari, E.; Guo, H.; Shen, C.C.; Hur, J. Collusion attacks on decentralized attributed-based encryption: analyses and a solution. *arXiv preprint arXiv:2002.07811* **2020**.
47. 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 of Things Journal* **2020**, *8*, 4291–4304.
48. Sharma, A.; Pilli, E.S.; Mazumdar, A.P.; Gera, P. Towards trustworthy Internet of Things: A survey on Trust Management applications and schemes. *Computer Communications* **2020**, *160*, 475–493.
49. Gyawali, S.; Qian, Y.; Hu, R.Q. Machine learning and reputation based misbehavior detection in vehicular communication networks. *IEEE Transactions on Vehicular Technology* **2020**, *69*, 8871–8885.
50. 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.
51. Salem, O.; Alsubhi, K.; Shaafi, A.; Gheryani, M.; Mehaoua, A.; Boutaba, R. Man-in-the-Middle attack mitigation in internet of medical things. *IEEE Transactions on Industrial Informatics* **2021**, *18*, 2053–2062.
52. Nigam, A.; Sharma, S.; Patel, R.K.; Agrawal, M. Man-in-the-middle-attack and proposed algorithm for detection. 2022 International Mobile and Embedded Technology Conference (MECON). IEEE, 2022, pp. 83–88.
53. Ahamed Ahanger, T.; Aldaej, A.; Atiquzzaman, M.; Ullah, I.; Yousufudin, M. Distributed blockchain-based platform for unmanned aerial vehicles. *Computational Intelligence and Neuroscience* **2022**, *2022*.
54. Khan, A.S.; Chen, G.; Rahulamathavan, Y.; Zheng, G.; Assadhan, B.; Lambotharan, S. Trusted UAV Network Coverage Using Blockchain, Machine Learning, and Auction Mechanisms. *IEEE Access* **2020**, *8*, 118219–118234. doi:10.1109/ACCESS.2020.3003894.
55. 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. doi:10.1007/s10514-015-9519-z.
56. Li, X.; Li, R. A Comprehensive Review for Four-Dimensional Trust Management in Distributed IoT. *IEEE Internet of Things Journal* **2023**.
57. Liu, D.; Alahmadi, A.; Ni, J.; Lin, X.; Shen, X. Anonymous reputation system for IIoT-enabled retail marketing atop PoS blockchain. *IEEE Transactions on Industrial Informatics* **2019**, *15*, 3527–3537.
58. Magaia, N.; Sheng, Z. ReFIoV: A Novel Reputation Framework for Information-Centric Vehicular Applications. *IEEE Transactions on Vehicular Technology* **2019**, *68*, 1810–1823. doi:10.1109/TVT.2018.2886572.

59. Qureshi, K.N.; Jeon, G.; Hassan, M.M.; Hassan, M.R.; Kaur, K. Blockchain-Based Privacy-Preserving Authentication Model Intelligent Transportation Systems. *IEEE Transactions on Intelligent Transportation Systems* **2023**, *24*, 7435–7443. doi:10.1109/TITS.2022.3158320.
60. 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. *2020 16th International Conference on Mobility, Sensing and Networking (MSN)* **2020**, pp. 145–152.
61. Weerapanpisit, P.; Trilles, S.; Huerta, J.; Painho, M. A decentralized location-based reputation management system in the IoT using blockchain. *IEEE Internet of Things Journal* **2022**, *9*, 15100–15115.
62. Xie, L.; Su, Z.; Chen, N.; Xu, Q. Secure Data Sharing in UAV-assisted Crowdsensing: Integration of Blockchain and Reputation Incentive. 2021 IEEE Global Communications Conference (GLOBECOM), 2021, pp. 1–6. doi:10.1109/GLOBECOM46510.2021.9685632.
63. Yang, Z.; Zheng, K.; Yang, K.; Leung, V.C.M. A blockchain-based reputation system for data credibility assessment in vehicular networks. 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), 2017, pp. 1–5. doi:10.1109/PIMRC.2017.8292724.
64. Zhou, R.; Hwang, K.; Cai, M. Gossip-Based Reputation Management for Unstructured Peer-to-Peer Networks. *IEEE Transactions on Knowledge and Data Engineering - TKDE* **2007**.
65. 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 Network* **2021**, *35*, 57–63. doi:10.1109/MNET.011.2000176.
66. Jensen, I.J.; Selvaraj, D.; Ranganathan, P. Blockchain Technology for Networked Swarms of Unmanned Aerial Vehicles (UAVs). *2019 IEEE 20th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM)* **2019**, pp. 1–7. doi:10.1109/WoWMoM.2019.8793027.
67. 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. doi:10.1109/ACCESS.2022.3145199.
68. feng Lin, X.; Zhang, J.; Xiang, L.; Ge, X. Energy Consumption Optimization for UAV Assisted Private Blockchain-based IIoT Networks. *2021 IEEE 94th Vehicular Technology Conference (VTC2021-Fall)* **2021**, pp. 1–7. doi:10.1109/VTC2021-Fall52928.2021.9625316.
69. Obaid, A.A.; Koyuncu, H. Obstacle Avoidance in Unmanned Aerial Vehicles Using Image Segmentation and Deep Learning. *2022 International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)* **2022**, pp. 912–915. doi:10.1109/ISMSIT56059.2022.9932865.
70. Hale, B.; Bossuyt, D.L.V.; Papakonstantinou, N.; O'Halloran, B. A Zero-Trust Methodology for Security of Complex Systems With Machine Learning Components. *Volume 2: 41st Computers and Information in Engineering Conference (CIE)* **2021**. doi:10.1115/detc2021-70442.
71. Shen, Y.; Qu, Y.; Dong, C.; Zhou, F.; hui Wu, Q. Joint Training and Resource Allocation Optimization for Federated Learning in UAV Swarm. *IEEE Internet of Things Journal* **2023**, *10*, 2272–2284. doi:10.1109/JIOT.2022.3152829.