Reliability and Reputation-based Optimal Cluster formation for Improving Performance in Unmanned Aerial Vehicle (UAV) Networks

MS Thesis

Muhammad Kashif

1123-FBAS/MSCS/F21

Supervisor

Dr. Qaisar Javaid
Assistant Professor, DCS & SE, IIU

Department of Computer Science
Faculty of Computing and Information Technology,
International Islamic University, Islamabad
2025

Declaration

I, Muhammad Kashif, at this moment, declare that my MS thesis titled "***Reliability and Reputation-based Optimal Cluster Formation for Improving Performance in Unmanned Aerial Vehicle (UAV) Networks***" is my work, neither as a whole nor as a part thereof has been copied out from any source except where due reference is made in the text. It is further declared that I have not previously submitted the work presented in the thesis report for partial or full credit for the award of a degree at this or any other university.

Acknowledgement

I am deeply grateful to Almighty Allah for His favors and blessings, which encouraged me to write this dissertation. I owe thanks to Allah for giving me a life full of strength and inspiration to accomplish this task.

Moreover, I would like to express my gratitude to my supervisor, Dr. Qaisar Javaid, who provided me with valuable advice and cooperation, which enabled me to carry out this entire work. It was an honor working under his supervision.

In addition, I want to thank the, Dr. Abdu Salam, for his contribution during the entire period of conducting this study. I am grateful for having had his perspective and poles as a reference. I am so thankful for his presence, input, discussions, suggestions, helpful, and comments that aided me in enhancing the whole research work.

Finally, my appreciation goes out to all my family – and to my parents, mainly because their good wishes encouraged me a lot to accomplish this task.

Dedication

To My Family, Teachers and Friends

Abstract

Flying Ad Hoc Networks (FANETs) play a pivotal role in enabling efficient and autonomous communication between Unmanned Aerial Vehicles (UAVs), with applications in disaster management, surveillance, and environmental monitoring. Despite their potential, FANETs face significant challenges, including dynamic topologies, high mobility, resource constraints, and security vulnerabilities. To address these issues, this thesis presents the Trust and Reputation-Based Clustering Optimization (TRBCO) algorithm, which leverages trust and reputation metrics to enhance the performance and security of FANETs. The proposed TRBCO algorithm dynamically evaluates UAVs based on trust factors such as packet delivery ratio, node stability, latency, and energy levels. These evaluations guide the selection of reliable cluster heads and optimize cluster formation, ensuring stable communication and resource efficiency. Additionally, TRBCO incorporates mechanisms to detect and exclude malicious nodes, improving network security and resilience. The performance of TRBCO is evaluated through extensive simulations and is compared with traditional clustering algorithms such as LEACH and K-Means. Results demonstrate that TRBCO significantly outperforms these algorithms in terms of Average Packet Delivery Ratio (APDR), End-to-End Delay (E2ED), and network throughput. Furthermore, TRBCO adapts effectively to high mobility scenarios and varying traffic loads, maintaining cluster stability and communication reliability. This thesis highlights the importance of trust and reputation mechanisms in addressing the challenges of FANETs, providing a robust and scalable solution for secure UAV communication. Future research directions include real-world deployment, enhanced energy efficiency, and mitigation of advanced security threats, paving the way for practical and reliable FANET applications.

Keywords: *Clustering, Flying Ad-hoc Network, Optimization, Reliability, Reputation, Trust, Cluster formation, Unmanned Aerial Vehicle (UAV) Networks*

TABLE OF CONTENTS

List of Acronyms

APDR	Average Packet Delivery Ratio
CM	Cluster Member
CH	Cluster Head
FANET	Flying Ad-hoc Network
PDR	Packet Delivery Ratio
UAV	Unmanned Aerial Vehicle
WSN	Wireless Sensor Network

List of Tables

List of Figures

Chapter 1

Introduction

In Flying Ad-hoc Networks (FANETs), gatherings of Unmanned Aerial Vehicles (UAVs) layout interconnections through a wireless network. These UAVs communicate with neighboring UAVs or ground stations to exchange crucial information. Establishing trust and maintaining reputable stunning among UAVs is pivotal for ensuring effective communication. Over the past decade, achieving a balanced cluster formation has posed a challenge, primarily due to the inherent tradeoff between the quality of network division and the time required for cluster formation [1].

During the cluster formation process, certain untrusted UAVs divulge false information, potentially leading to an unstable clustering structure, while others adopt a selfish stance to minimize their communication load. Collaboration among UAVs is essential for mission completion; however, the deliberate non-cooperation of selfish and untrustworthy UAVs in the network can significantly degrade overall network performance.

Researchers have proposed both direct and indirect methods to calculate the trust value of a node in Mobile Ad-hoc Networks (MANETs) and Vehicular Ad-hoc Networks (VANETs). FANETs, distinct from other ad-hoc networks, present a unique challenge due to the high mobility of UAVs, resulting in frequent structural changes. Consequently, the existing methods for trust calculation are deemed inefficient and ineffective in the context of FANETs [2].

The management of large numbers and high-speed UAVs becomes difficult in FANET. Optimizing network management can be effectively performed with the help of a clustering approach that divides the UAVs into multiple clusters. Each UAV plays the role of a UAVs-CH or as a Cluster Member (CM). UAVs-CH is responsible for inter-cluster and intra-cluster communication. A good practice is to grant services based on the contribution of UAVs to network operations. The UAVs with good reputations have a better chance to avail of the network services as UAVs-CH or members than the bad reputations of UAVs. To address the issues of selfishness and reliability of UAVs, trust

and reputation-based clustering of UAVs need consideration during network operations.

In the realm of modern technology, UAVs have emerged as game-changers, revolutionizing various sectors, including disaster response, environmental monitoring, and communication networks. As UAVs take center stage in these applications, ensuring robust and efficient communication within their networks becomes paramount.

The Average Packet Delivery Ratio (APDR) is a vital metric, representing the proportion of successfully delivered packets compared to the total sent packets. It serves as a foundational indicator of the network's reliability and performance. Yet, in the dynamic world of UAV networks, where factors such as intermittent connectivity and varying environmental conditions persist, comprehensively analyzing APDR is imperative to optimize communication efficacy.

1.1 Trust and Reputation-based Clustering in FANET

FANET is an emerging domain that connects airborne sensors and ground stations. Effectively routing information among flying nodes has become a challenging and pivotal concern, garnering significant attention from researchers in recent years. Despite numerous contributions aimed at increasing communication reliability, this field is still in its infancy, and many challenges remain, which naturally result from how factors reveal the inherent ability of flying objects [3].

In flat routing, nodes, and their connected neighbors directly exchange information without first having synchronization or configuration settings between them. The dynamic changes associated with the high mobility of nodes in the topology lead to the saturation of the flat network structure. This saturation, in turn, causes an increase in the routing table size due to the rapid movement of nodes in the FASNET. In flat networks, any alteration in the topology is communicated to all connected nodes within range, introducing additional overhead to the network due to data aggregation based on the neighbors [4].

The structure of a network in cluster-based routing is organized into multiple clusters, each having its designated head, referred to as CH (Cluster Head). Cluster member nodes convey their information to the CH in an aggregated manner, demonstrating

proper synchronization among them. The use of hierarchical routing helps to circumvent collisions during node communication. Multi-hop networks with Cluster Heads offer lower latency than flat routing, which encounters challenges stemming from many nodes, dynamic changes in topology, and the high mobility of flying nodes.

This approach ensures that topology changes are managed locally within each cluster, mitigating their impact on the entire network. Consequently, the network becomes more scalable, with aggregated topology information promoting routing efficiency and establishing a balanced network [4].

1.2 Application of FANET

In FASNET, various applications facilitate the execution of multiple tasks by utilizing flying nodes. These nodes exchange information with one another in ad hoc modes to accomplish specific missions in a distributed manner [5]. FASNET applications encompass:

1.2.1 Search and Rescue Operations

Search and rescue operations represent one of the primary applications of FASNET, commonly employed for locating and conducting rescue missions. In these missions, flying nodes are deployed to search or sense for objects, nodes, or targets on the ground or in the sky. Various strategies [6-8] are utilized to identify unreachable areas, objects, or targets that may be challenging for human detection.

1.2.2 Forest Fire Detection

This is another crucial application of FASNET, aiming to mitigate the risk of fires or excessive heat that could result in significant losses. Various approaches [9, 10] are employed in this context, encompassing measurement, monitoring, and control of forest fires. Different mobility models of flying nodes are utilized, along with a topology that maintains the desired formation during monitoring activities.

1.2.3 Traffic and Urban Monitoring

Traffic and urban monitoring constitute a valuable application of FASNET, addressing the challenges of traffic congestion and numerous accidents in the complex infrastructure of urban and metropolitan areas. Flying nodes are key in quickly detecting and reporting incidents on roads, railway tracks, or street junctions, providing real-time information about the situation [11-13].

1.2.4 Agricultural Management

Agriculture management is a significant application of FASNET, where flying nodes remotely sense crop production and monitor protective measures. Flying nodes are essential for precisely distributing fertilizers and chemicals at specific times and locations. Monitoring the health of plants, crop conditions, soil properties, and water content is crucial, often requiring precise and high-resolution data for site-specific management [14]. Using flying sensor swarms with flight path optimization [15, 16] offers insights into how they manage water for plants and control irrigation.

1.2.5 Environmental Sensing

Environmental sensing represents a challenging aspect in FASNET, demanding intelligence regarding awareness, heterogeneity, trust management, and cooperation among flying nodes. FASNET generates a substantial and continuous data flow, aiming to contribute to a smart environment by transforming raw data into actionable intelligence. Flying nodes with low-power batteries are deployed to examine environmental factors such as temperature, humidity, and pollution [17].

1.2.6 Disaster Management

Disaster management represents a crucial application for flying nodes, with the primary goal of predicting the occurrence of disasters [18]. Diverse systems, including mobile autonomous systems implemented in emergency areas [19], heterogeneous vehicle control systems through FASNET for complex operations in automated humanitarian missions [20], and smart public safety systems [21], contribute to achieving effective disaster management.

1.3 Problem Statement

FANETs utilizing UAVs are crucial components of modern communication and surveillance systems, particularly in dynamic environments and areas with limited infrastructure. However, ensuring reliable and efficient communication in these networks is a significant challenge. Traditional clustering algorithms in FANETs often overlook the importance of trust and reputation among nodes, leading to poor decision-making during cluster formation. Achieving effective packet delivery, minimizing end-to-end delays, optimizing network throughput, and ensuring rapid cluster formation is critical for the optimal performance of FANETs. Given the dynamic nature of UAV networks and resource constraints, meeting these requirements remains difficult. Moreover, real-world applications demand a flexible and adaptive approach to address the varying conditions and challenges inherent in these networks. Tending to these difficulties, this study offers an elective methodology by coordinating trust and progressing notoriety in the clustering enhancement process. The mix advances customary bunching algorithms by expanding the unwavering quality and notoriety of the included hubs, in this way upgrading decision-production while grouping. The proposed strategy plans to accomplish an APDR, reduce delay, further develop network throughput, further develop bunch development time, and, at last, add to better information transmission function admirably and dependably. This examination endeavors to give an exhaustive answer for enhancing UAV-based ad hoc networks by introducing a central investigation that can adjust to different certifiable situations. The bits of knowledge and strategies introduced here give the establishment to future turns of events, including adaptable trust models, energy-proficient methodologies, and improved security components; for the UAV-based ad hoc network, the side has moved towards a more reobligated and effective communication framework.

1.4 Research Questions

Research Question No. 1

How can reliability and reputation improvements be effectively combined in clustering optimization algorithms for UAVs in aircraft ad hoc networks (FANETs)?

Research Question No. 2

How does the integration of trust and reputation metrics impact the APDR in a FANET environment?

Research Question No. 3

How does including trust and reputation metrics affect the End-to-End Delay in data transmission within a FANET?

Research Question No. 4

In what ways does integrating trust and reputation metrics optimize Network Throughput in FANETs?

Research Question No. 5

How does integrating trust and reputation metrics influence the time taken for Cluster Formation in a FANET scenario?

1.5 Aims and Objectives

This research aims to enhance the communication efficiency and reliability within UAV networks by focusing on improving the APDR. To achieve this, we have outlined the following specific research objectives:

- Assess and analyze the performance of established communication protocols in UAV networks concerning APDR. This evaluation will provide insights into the strengths and weaknesses of current protocols regarding data delivery efficiency.
- Investigate the impact of dynamic network conditions, such as varying node mobility and network density, on APDR. Understanding how these factors affect data delivery will enable the development of adaptive strategies.
- Explore integrating trust and reputation mechanisms under communication protocols to enhance APDR. Examine how reliability-based decisions can improve packet delivery and reliability, especially in situations where nodes move frequently, or collective communication conditions are complex

- Devise strategies to optimize energy consumption while maintaining high APDR. Energy-efficient strategies are critical for UAVs, and striking a balance between data transmission and energy conservation is an important goal.
- Incorporate robust protection measures into communication systems to ensure secure Da-Ta transfers while maintaining high APDR. Addressing security concerns in UAV networks is essential, and a secure communications environment is key to reliable data transmission.

1.6 Scope of the Study

The scope of this research is expansive, as the application of UAVs in Flying Ad-hoc Networks extends to various practical scenarios, including but not limited to smart agriculture, intrusion detection, smart cities, smart transportation, and smart buildings, utilizing cost-effective flying sensors. The integration of advanced technology enables society to benefit from remote work capabilities. For instance, in smart agriculture, flying nodes can promptly inform farmers about crop diseases and irrigation requirements. In rescue operations, UAVs can detect humans in affected areas or reach inaccessible locations that are difficult for humans to reach.

In forest monitoring, UAVs contribute to preventing the risk of fires by measuring, monitoring, and controlling forest fires using different mobility models of flying nodes, maintaining a desired formation during monitoring. In smart transportation, managing traffic congestion and monitoring incidents on roads or railway tracks can be efficiently handled using multiple UAVs, reducing personnel costs. Additionally, in border supervision, UAVs play a crucial role in protecting against illegal immigration and weapons smuggling.

The theoretical and experimental results of this study can potentially be extrapolated to various scenarios and implemented in practical situations across diverse domains.

1.7 Contributions of the Study

1.7.1 Innovative Integration of Trust and Reputation Dynamics

The study proposes an innovative integration of trust and reputation dynamics into the clustering optimization process for FANETs. This integration enriches the traditional

clustering algorithms by considering the trustworthiness and reputation of nodes, leading to improved decision-making during cluster formation.

1.7.2 Enhanced Reliability and Efficiency in Packet Delivery

This study achieves a higher APDR by integrating trust and reputation metrics, demonstrating an improvement in reliable packet delivery. The approach minimizes delays and enhances data transmission efficiency, which is crucial for real-time applications in FANETs.

1.7.3 Optimized Network Resource Utilization

The study enhances network throughput by integrating trust and reputation metrics. Optimized network resource utilization is vital for efficiently using limited bandwidth, which is a significant challenge in ad hoc networks.

1.7.4 Efficient Cluster Organization and Formation

The proposed approach significantly reduces Cluster Formation Time, showcasing its efficiency in rapidly organizing optimized clusters. This efficiency improves network organization, facilitating efficient data exchange and collaboration among UAVs.

1.7.5 Foundational Research for Future Advancements

This study integrates reliability methods to lay the foundation for future research in UAV networks. The insights and methodologies presented can guide further explorations into adaptive trust models, energy-efficient strategies, and enhanced security mechanisms, thus advancing the field of UAV-based ad hoc networks.

1.7.6 Applicability to Diverse Real-World Scenarios

The study's contributions are not limited to a specific domain and can be applied to various real-world scenarios such as disaster response, environmental monitoring, and smart agriculture. The versatile nature of the approach makes it adaptable and beneficial across various applications.

Combined, these contributions help to enhance the FANETs project through the use of reliability and reputation values as constraints/considerations while achieving network

reliability, efficiency, and flexibility to address the den and overcome dynamic challenges.

Chapter 2

Literature Review

Another unexplored and distinct research direction is cluster-based reliability and FANET's reputation. Researchers have proposed several frameworks to determine the trust value of nodes based on concepts originally imported from Mobile Ad-hoc Networks (MANET) and Vehicular Ad-hoc Networks (VANET). The unique characteristics of UAVs in FANET use distinguish it from other ad-hoc networks, hence the low efficiency and effectiveness of the currently available reliability estimation techniques. In the following subsections, we review some of the literature research that proposed trust and reputation-based clustering schemes that are tailored for FANETs.

2.1 Unmanned Aerial Vehicles (UAVs) in Ad Hoc Networks

UAVs, also named drones, have been eliciting interest for several years because of their multifunctionality and multifunctionality [22]. Their mobility and, therefore, their capability to maneuver in a plane of their own, as well as their ability to work in dynamic networks, qualifies them as suitable candidates for ad hoc networks [23]. Therefore, this current review seeks to look into the following areas regarding UAVs in ad hoc networks: their applications, challenges, and development areas.

Pasandideh et al., [24] demonstrated that UAVs hold numerous application areas for ad hoc networks, from risk assessment to environmental management and as communication relays for areas difficult to access there. Through real-time surveillance, identification of potential and actual hot zones, and easier tracking, UAVs help in search and rescue missions and provide efficient response. Beloy, [25] Such environmental and monitoring applications include observation of wildlife, agricultural fields, and traffic, among others. In communications, UAVs help in the formation of communication infrastructure and also communication traffic in areas that are congested or inaccessible. These applications demonstrate the possibility of UAVs transforming communication and data retrieval in challenging terrains.

However, their usefulness aside, UAVs in ad hoc networks are not without their problems. Another important point, which means the work of several teams of engineers, is the following: One of the main tasks is to provide regular and secure communication since UAVs are mobile nodes, and the topology is rather dynamic. Rovira et al., [26] Areas like link suitability, interferences mitigation, energy awareness, and routing protocols designed for aerial ad hoc that involve UAVs deserve further research. More generally, the integration of UAVs into current and future architectures based on ad hoc networks needs more studies on connectivity, resource allocation, and protocol definition. The problem of the coverage and utilization of UAV routes and deployment schemes is active today to enhance the performance of UAVs.

According to the literature research, innovations in UAV technology and communication systems have assumed essential roles in the improvement of this discipline. There are positive indications that the use of AI and machine learning techniques in the control of UAVs for maneuverability, resource allocation, and demand response has endeared the UAV system to smarter environments. [27]. Moreover, propels in particle size, energy productivity, and battery technologies have expanded the scope of UAV flight times and locations, expanding their convenience in specially appointed networks once more. A few examinations propose new correspondence conventions and setups planned unequivocally for UAVs, like Delay-Tolerant Networking (DTN) frameworks, to promote the difficulties of intermittent communication and deferred tasks. Table 2.1 summarizes recent research on UAVs in ad hoc networks.

Table 2.1: Summary of Recent Research on UAVs in Ad Hoc Networks

Study	**Focus**	**Methodology**	**Key Findings**
Udroiu *et al.,* [28], 2021	Communication protocols for UAVs	Simulation and experimentation	Proposed a novel DTN-based protocol for UAV communication, showcasing improved performance in intermittent connectivity scenarios.
Nguyen *et al.,* [29] 2022	UAV trajectory optimization	Machine learning and simulation	Utilized machine learning algorithms to optimize UAV trajectories, achieving significant improvements in network coverage and data collection efficiency.

2.2 Trust and Reputation Systems in UAV Networks

Trust and notoriety frameworks are fundamental in creating dependable correspondence and collaboration among organizations in UAV networks [30]. These designs assist with creating confiding in connections and backing dynamic cycles, asset distribution, and coordinated effort. This part presents the significance, challenges, and late turns of events, as well as an examination of dependability and notoriety frameworks in UAV networks.

The trust and notoriety of executives are fundamental to UAV correspondence frameworks because of their dynamic and frequently eccentric nature. Laying out trust empowers UAVs to organize better, share critical information, and allot assets all the more effectively. Huang et al. [31] Notoriety strategies assist with assessing the dependability and reliability of UAVs in light of their past activities and communications. This angle is critical in accomplishing dependable and strong UAV correspondences, which are fundamental for applications like studies, calamity of the executives, and environmental observing.

A few difficulties should be addressed to foster a commonsense trust and notoriety framework for UAV networks [32]. UAVs can attack rapidly, and guaranteeing unwavering quality within the sight of malevolent tissue is a critical test. Besides, keeping up with unwavering quality in mighty and heterogeneous UAV networks is challenging. Creating lightweight and productive dependability models considering node mobility, energy requirements, and ecological circumstances is a continuous exploration region. Research on unwavering quality and notoriety frameworks for UAV communications frameworks is quickly developing. Ongoing examinations have proposed new unwavering quality models, notoriety-building techniques, and dependability-based route rules expressly custom-made for UAVs. This update plans to upgrade the dependability and security of correspondences in UAV communications. A few eminent ongoing examinations in this field are summed up in Table 2.2.

Table 2.2: Summary of the Research on Trust and Reputation Systems in UAV Networks

Reference	Focus	Methodology	Key Findings
Kumar et al., [33] 2023	Trust-based routing	Simulation, mathematical analysis	Introduced a trust-based routing protocol for UAV networks, enhancing communication reliability by considering the trustworthiness of nodes and routes.
Wang et al., [34] 2021	Reputation aggregation	Empirical analysis, simulation	Proposed a reputation aggregation mechanism for UAVs, providing a reliable evaluation of node reputations through a decentralized approach.
Olufemi et al., [35] 2023	Security and Trust	Analytical modeling, simulation	Presented a security-aware trust model for UAV networks, mitigating security threats and enhancing trust management.
pang et al., [36] 2018	Dynamic trust assessment	Field experiments, statistical analysis	Developed a dynamic trust assessment mechanism for UAVs in disaster response scenarios, ensuring effective collaboration and information sharing.
Refaee et al., [37] 2017	Energy-aware trust routing	Simulation, energy modeling	Proposed an energy-aware trust routing protocol for UAV networks, optimizing energy consumption while maintaining trust-based routing decisions.

2.3 Clustering Optimization in Ad Hoc Networks

Bunching is a fundamental technique utilized in ad hoc networks, which considers productive management and communication inside a network. Bunching includes shaping gatherings or groups of hubs, where each bunch regularly has a bunch held liable for connectivity and communication [38]. Ideal grouping intends to upgrade network execution in regards to energy effectiveness, load adjusting, data collection, and generally network solidness [39]. Grouping streamlining resolves significant issues in ad hoc networks, like energy utilization and organization adaptability. Sefati et al., [40] expressed that energy utilization is consistently disseminated all through the organization by shaping groups and productively choosing bunch heads. What's more, data assortment and trade of data in bunches diminishes the general expense of communication. Empowering grouping in ad hoc networks is challenging because of the different difficulties [41]. These incorporate firmly changing network topologies, node mobility, energy limitations, and heterogeneity in hub limit. An essential exploration center is planning bunching algorithms that adjust to these challenges while guaranteeing ideal group development, proficient group head choice, and burden adjusting. What's more, tending to security concerns and acceptable blunders in grouping improvement is significant for the solid situation of ad hoc networks. Ayub et al. [42] ongoing research has tracked down huge advancements in bunching streamlining methods for ad hoc networks Studies

have presented new clustering algorithms, load-adjusting, energy-effective, and security-aware clustering methods. These upgrades intend to develop network execution further, expand network lifetime, and increment versatility against security dangers. Table 2.3 summarizes the late examination commitments to grouping streamlining in ad-hoc networks.

Table 2.3: Summary of recent research on Clustering Optimization in Ad-hoc Networks

Study	Focus	Methodology	Key Findings
Fouladlou et al., [43] 2017	Energy-efficient clustering	Simulation, performance evaluation	Proposed an energy-efficient clustering algorithm for IoT networks, achieving substantial energy savings and prolonged network lifetime.
Gherbi et al., [44] 2016	Load balancing	Analytical modeling, simulation	Introduced a load balancing technique for clustered WSNs, achieving a more balanced energy consumption and improved network longevity.
Devi et al., [45] 2019	Security-aware clustering	Simulation, security analysis	Presented a security-aware clustering approach, considering security metrics during cluster formation, enhancing the network's resistance to attacks.
Mcdonald et al., [46] 2000	Dynamic clustering	Simulation, performance evaluation	Developed a dynamic clustering algorithm for mobile ad hoc networks, allowing for efficient adaptation to changing network conditions improving stability and performance.

The existing research focuses on different parts of grouping improvement in ad hoc networks, including energy effectiveness, load adjusting, security considerations, and exchanging streams, remembering for a dynamic state.

2.4 Integration of Trust, Reputation, and Clustering in UAV Networks

The combination of Trust, Reputation, and Grouping addresses a complex methodology in UAV networks, joining a few critical highlights further to develop network execution, security, and reliability [47]. Trust and notoriety techniques are the most significant for building solid networks, while groups empower better design and upkeep of UAVs [48]. Consolidating these components is a promising way to deal with and address the interesting difficulties that exist in UAV communication frameworks. Incorporating Trust, Notoriety, and Grouping gives a multi-layered answer for UAV communication [49]. Trust and notoriety create a feeling of trust and responsibility in UAVs, which is vital for joint effort and data sharing. Clustering, then again, further develops

network foundation, asset designation, and correspondence. Joining these elements empowers UAVs to shape dependable units, expanding coordinated effort, diminishing energy utilization, and further developing general organization effectiveness. This coordination is fundamental for examination, fiasco reaction, and natural checking applications, where unwavering quality, cooperation, and proficiency are central. The blend of Trust, Notoriety, and Grouping presents many difficulties. A bound-together structure that effectively consolidates dependability models, notoriety strategies, and bunching algorithms while considering UAV-explicit limitations is challenging [50]. Challenges incorporate creating versatile trust models to adjust to changes in network elements, guaranteeing exact standing evaluations, and giving ideal grouping in view of trust levels. Moreover, tending to security dangers and weaknesses inside the coordinated framework is a key concentration. The late examination has gained huge headway in coordinating Trust, Notoriety, and Clustering into UAV networks. Zhou et al., [51] coordinate new plans and frameworks that coordinate these highlights, planning to improve cooperation, security, and energy effectiveness in UAV organizations. Table 2.4 gives an outline of the late examination supporting the joining of Trust, Notoriety, and Grouping in UAV networks.

Table 2.4: Summary of Recent Research on Integration of Trust, Reputation, and Clustering in UAV Networks

Study	**Focus**	**Methodology**	**Key Findings**
Osamy *et al.*, [52] 2023	Trust-aware clustering	Simulation, performance evaluation	Introduced a trust-aware clustering algorithm for UAV networks, improving network reliability and performance through trust-guided cluster formation.
Al Ridhawi *et al*., [53] 2020	Reputation-based cluster head selection	Simulation, comparative analysis	Proposed a reputation-based mechanism for cluster head selection in UAV networks, achieving balanced load distribution and improved network longevity.
Fang *et al*., [54] 2019	Secure clustering protocol	Analytical modeling, simulation	Developed a secure clustering protocol integrating trust and reputation, enhancing network security and robustness against malicious attacks.
Sharma et al., [55] 2018	Energy-efficient trust-based clustering	Simulation, energy modeling	An energy-efficient trust-based clustering approach was introduced for UAV networks, optimizing energy consumption and network reliability through trust-aware cluster formation.

These studies focus on trust-aware clustering, reputation-based cluster head selection, security considerations, and energy-efficient clustering, showcasing the diverse approaches to integration within UAV networks.

Despite the significant advancements in UAV networks and clustering optimization, several limitations persist in the existing body of research. Most current studies do not adequately address the integration of trust and reputation mechanisms within the dynamic environment of FANETs, often overlooking the impact of node mobility and varying network conditions on clustering efficiency. Additionally, the majority of clustering algorithms are designed with a primary focus on energy efficiency or network performance but fail to balance these aspects with security and reliability, leaving networks vulnerable to malicious nodes and unstable communication. Furthermore, existing literature frequently lacks comprehensive evaluations across diverse real-world scenarios, limiting the generalizability of proposed solutions. These gaps underscore the need for more holistic approaches that consider the multifaceted challenges present in UAV-based ad hoc networks.

2.5 Research Gap / Issues

Despite significant advancements in UAV networks and clustering optimization, several gaps and unresolved issues hinder the achievement of the objectives outlined in this research. These gaps are discussed below:

2.5.1 Evaluation of Communication Protocols

While numerous communication protocols have been proposed for UAV networks, there is a lack of comprehensive studies evaluating their performance concerning Average APDR. Current evaluations are often limited to specific scenarios and do not provide a holistic assessment. This gap makes identifying the most effective protocols for ensuring high data delivery efficiency across various network conditions challenging.

2.5.2 Impact of Dynamic Network Conditions

The dynamic nature of UAV networks, characterized by varying node mobility and network density, significantly impacts APDR. However, existing studies do not sufficiently address how these dynamic conditions affect data delivery and what adaptive strategies can mitigate these impacts. Without understanding these impacts, developing robust communication strategies that maintain high APDR under changing network conditions is difficult.

2.5.3 Integration of Trust and Reputation Mechanisms

Trust and reputation mechanisms are recognized for their potential to enhance communication reliability, but their integration into UAV network protocols is still developing. Most existing protocols do not incorporate trust-based decisions effectively. The absence of integrated trust mechanisms results in suboptimal packet delivery and reliability, especially in scenarios with high node mobility or challenging communication conditions.

2.5.4 Energy Optimization

Many clustering optimization algorithms focus on network performance without adequately addressing energy consumption. There is a need for strategies that balance energy efficiency with maintaining high APDR. UAVs are typically underpowered, and poor energy efficiency can reduce network lifetime and performance.

2.5.5 Security Measures

Ensuring secure data transfer while maintaining high APDR is an important but underexplored area. Existing protocols ignore the importance of adding robust security measures to the network. Without secure protocols, UAV networks are vulnerable to security threats, compromising data integrity and network reliability.

2.5.6 Cluster Formation Efficiency

Traditional clustering algorithms do not prioritize the trust and reputation of nodes, resulting in inefficient cluster design and scheduling. There is a need to develop algorithms that reduce cluster formation time by incorporating trust metrics. An inadequately designed bunch can create setbacks and unfortunate network execution, influencing general communication proficiency in UAV networks.

In addressing this gap, exhaustive assessment principles for correspondence conventions, versatile techniques for dynamic network environments, and a blend of dependability and notoriety procedures have been created, notwithstanding energy utilization, vigorous safety efforts, and UAV network usefulness. These are vital for development. By zeroing in on these areas, analysts can augment unwavering quality and proficiency in UAV-based ad hoc networks, at last accomplishing the goals of this review.

Chapter 3

Research Methodology

In this chapter, we outline our study's methodology, which includes the system's design and phases, as well as the main steps of data collection and prioritization. The research framework is depicted in Figure 3.1.

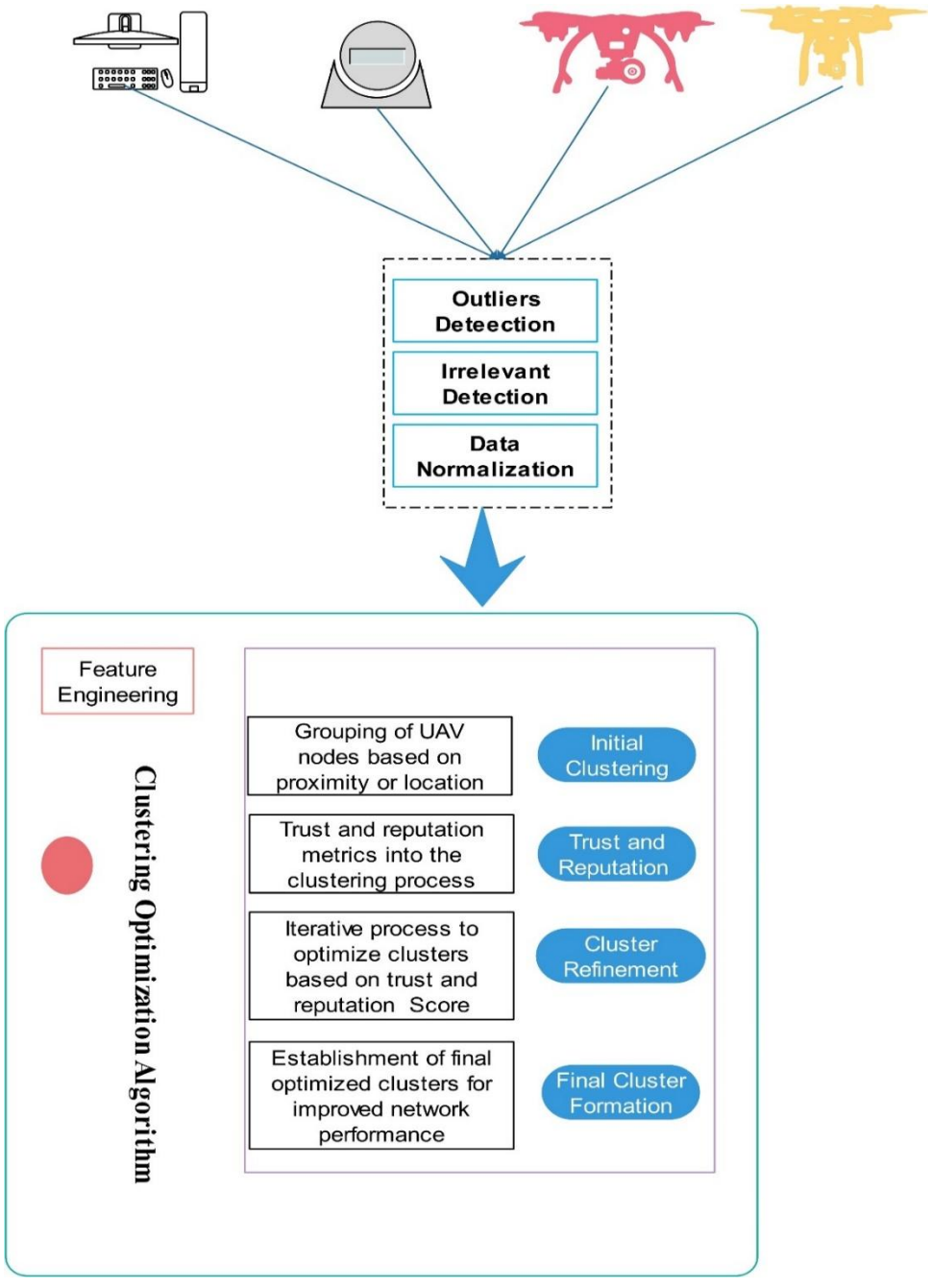

Figure 3.1: Research Framework

3.1 System Architecture and Components

This study researches exhaustively how to upgrade the exhibition and dependability of FANETs through a system explicitly intended for UAVs. The plan contains fundamental elements that guarantee effective communication and data transmission among organized UAVs. The components of the system architecture are summarized in Figure 3.1.

Table 3.1: Components of the System Architecture

Component	Description
UAV Nodes	Represent individual unmanned aerial vehicles in the network.
Ground Station	Centralized station facilitating communication with UAV nodes.
Communication Protocols	Protocols governing data exchange and synchronization among UAV nodes and ground stations.
Trust and Reputation Module	Module responsible for evaluating and maintaining trust and reputation scores for UAV nodes.
Clustering Optimization	Algorithmic module optimizing UAV node clustering based on trust and reputation metrics.

The UAV nodes, which structure the foundation of the network, speak with one another and with ground stations through assigned communication protocols. The Trust and Notoriety Module assesses the reliability of UAV hubs in light of their way of behaving and guarantees a safe and proficient association. Moreover, the Grouping Enhancement algorithm powerfully bunches UAV hubs in view of their dependability and notoriety measurements, streamlining network execution.

3.2 Data Collection and Preprocessing

Exact and significant data is the foundation of any examination. This approach underlines cautious information assortment and preprocessing to guarantee the quality and dependability of the data obtained. The data collection and preprocessing steps are summarized in Table 3.2.

Table 3.2: Steps in Data Collection and Preprocessing

Step	Description
Sensor Data Collection	Data from UAV onboard sensors is acquired.

Step	Description
Network Logs Capture	Recording network-related data, including communication patterns and events.
Data Cleaning	Elimination of outliers, irrelevant, or erroneous data.
Data Normalization	Standardization of data to a uniform format and scale.
Feature Engineering	Transformation of raw data into relevant features for analysis.

The interaction starts with gathering sensor data from UAVs and network logs that catch correspondence frameworks. Along these lines, thorough data-cleaning techniques kill irregularities and inconsistencies. The data is then standardized to guarantee consistency, considering proper examination. Include designing is utilized to get significant highlights from the raw data, giving important bits of knowledge into UAV conduct and network dynamics.

This study underscores the significance of trust and notoriety in dependable correspondence and joint effort inside the UAV network. We cautiously select trust and notoriety measurements to really gauge the dependability and reliability of individual UAV nodes effectively. The selected trust and reputation metrics are summarized in Table 3.3.

Table 3.3: Selected Trust and Reputation Metrics

Metric	Description
PDR	Ratio of successfully delivered packets to the total transmitted packets.
Network Participation	Frequency of a node's active participation in the network.
History of Collaborations	Past successful collaborations and interactions with other nodes.
Latency	Time taken for data packets to travel from source to destination.
Node Stability	Consistency of a node's performance and availability over time.

The chosen measurements incorporate significant factors like parcel conveyance unwavering quality, dynamic cooperation in the network, authentic execution achievement, dormancy, and security of each UAV node. Dependability and notoriety testing in view of these measurements permits a thorough evaluation of a node's unwavering quality and commitment to the network.

3.3 Clustering Optimization Algorithm

Proper configuration of UAV nodes is essential to enhancing communication and resource management in the ad hoc network. Our study introduces a Clustering Optimization Algorithm specially designed for UAV communication facilities to obtain optimal cluster formations. The steps in the clustering optimization algorithm summarized in Table 3.4.

Table 3.4: Steps in the Clustering Optimization Algorithm

Step	Description
Initial Clustering	Initial grouping of UAV nodes based on proximity or location.
Trust and Reputation Integration	Incorporation of trust and reputation metrics into the clustering process.
Cluster Refinement	Iterative process to optimize clusters based on trust and reputation scores.
Final Cluster Formation	Establishment of final optimized clusters for improved network performance.

The Clustering Optimization Algorithm starts by initially clustering UAV nodes using proximity or location information. The combination of trust and reputation metrics optimizes the clustering process, ensuring that nodes with high trust levels are given appropriate priorities. Subsequent re-adjustment of clusters based on trust and reputation scores leads to the formation of a final refined cluster, which ultimately enhances the quality of communication and communication efficiency.

The Trust and Reputation-Based Clustering Optimization (TRBCO) algorithm (Algorithm 1) is designed to enhance the reliability, security, and performance of FANETs by incorporating trust and reputation metrics into the clustering process. TRBCO evaluates the behavior of UAVs based on multiple parameters, such as packet delivery ratio, node stability, and energy levels, to build trust scores. These scores are used to form clusters with reliable nodes and minimize disruptions caused by malicious or faulty UAVs.

Algorithm 1: Proposed TRBCO Algorithm

1. Initialize UAV nodes with default trust scores and parameters
2. **While** Termination condition is not met **Do**

Algorithm 1: Proposed TRBCO Algorithm

For each UAV i in the network **Do**
    Calculate trust score Ti based on:
    Packet Delivery Ratio (PDR)
    Node Stability
    Latency
    Energy Level
    Update reputation score $Ri \leftarrow aggregate(Ti)$ ▷ $Reputation\ Update\ Phase$
End For
Select Cluster Heads (CHs):
Choose UAVs with the highest trust and reputation scores
Ensure CHs meet energy and connectivity thresholds
Form Clusters:
    For each UAV_j do
    Assign UAV_j to the nearest CH with sufficient capacity
    End For
Evaluate cluster configurations:
    Check load balancing among CHs
    Adjust clusters if CH load exceeds threshold
Detect and isolate malicious nodes:
    Flag UAVs with trust score $R_i < trust\_threshold$
    Exclude flagged nodes from clusters
Update network configurations:
    Adapt clusters to dynamic topology changes
End while
Output the final cluster configurations and trust evaluations

3.4 Simulation Setup and Parameters

A comprehensive simulation program was conducted to evaluate the performance of our proposed Trust and Reputation-Based Clustering Optimization Algorithm. This sub-section describes the details of the simulation environment, including the parameters and configurations utilized.

3.4.1 Simulation Environment

We used the NS-3 (Network Simulator version 3) platform, a widely used discrete-event network simulator, to simulate UAV's behavior and interactions in the ad hoc network. The simulator provides a flexible and extensible framework for evaluating and testing various communication systems and scenarios. The simulation environment parameters are summarized in Table 3.5.

Table 3.5: Simulation Environment Parameters

Parameter	**Value**
Simulation Time	1000 seconds
Number of UAV Nodes	50
Communication Range	500 meters
Terrain Model	Urban
Mobility Model	Random Walk

To accurately model trust and reputation dynamics, we defined specific parameters governing trust and reputation estimation and integration in our proposed algorithm. The trust and reputation parameters are summarized in Table 3.6.

Table 3.6: Trust and Reputation Parameters

Parameter	**Value**
Trust Threshold	0.6
Reputation Update Interval	100 seconds
Trust Update Interval	150 seconds
Trust Decay Factor	0.85
Reputation Weight	0.6

These parameters define the algorithm's trust and reputation score estimation and influence node behavior, clustering, and network evolution.

3.4.2 Performance Metrics

To evaluate the effectiveness of our proposed approach, we measured various performance metrics and captured important aspects of network efficiency and reliability. The performance metrics are summarized in Table 3.7.

Table 3.7: Performance Metrics

Metric	**Description**
Average Packet Delivery Ratio	Proportion of successfully delivered packets.
End-to-End Delay	Average time is taken for a packet to reach its destination.
Network Throughput	Amount of data successfully transmitted per unit time.
Cluster Formation Time	Time is taken to form optimized clusters.

Chapter 4

Results and Analysis

4.1 Evaluation of Trust and Reputation-Based Clustering

4.1.1 Performance Metrics and Benchmarks

A summary of the evaluation metrics is provided in Table 4.1. Benchmarks include traditional clustering algorithms such as LEACH (Low-Energy Adaptive Clustering Hierarchy) and K-Means Clustering, compared to the proposed TRBCO algorithm.

Table 4.1: Summary of Evaluation Metrics

Metric	Definition	Objective
Average Packet Delivery Ratio	Ratio of successfully delivered packets to transmitted packets	Maximize reliability
End-to-End Delay	Average time taken for a packet to reach its destination	Minimize latency
Network Throughput	Amount of data transmitted successfully per unit time	Maximize efficiency
Cluster Formation Time	Time required to form stable clusters	Minimize setup time

4.1.2 Simulation Results and Comparison

Figure 4.1 presents the APDR achieved by the proposed TRBCO algorithm, compared to LEACH and K-Means algorithms across varying network sizes.

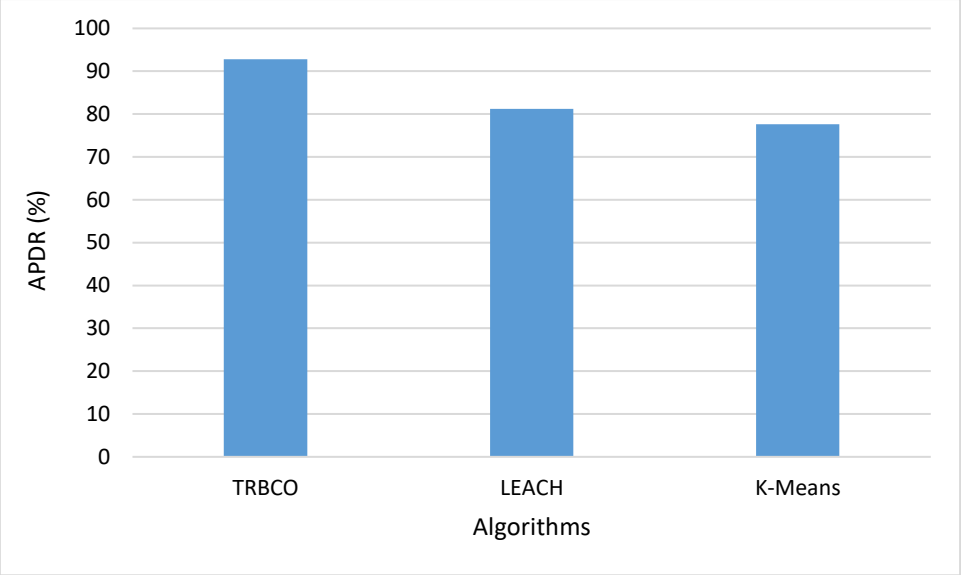

Figure 4.1: Comparison of APDR Across Algorithms

Table 4.2 compares APDR for different UAV network sizes under the proposed TRBCO algorithm, LEACH, and K-Means.

Table 4.2: APDR for different UAV network sizes

Network Size (Nodes)	TRBCO (APDR)	LEACH (APDR)	K-Means (APDR)
10	95.4%	89.6%	87.1%
20	93.8%	85.2%	83.5%
50	91.2%	79.3%	76.8%

The results show that the TRBCO algorithm consistently achieves a higher APDR due to its ability to filter out untrustworthy nodes and prioritize reliable ones during cluster formation.

4.1.3 Impact on Cluster Stability

Figure 4.2 shows the stability of clusters over time, measured as the percentage of clusters that remain unchanged during simulation periods, comparing TRBCO, LEACH, and K-Means.

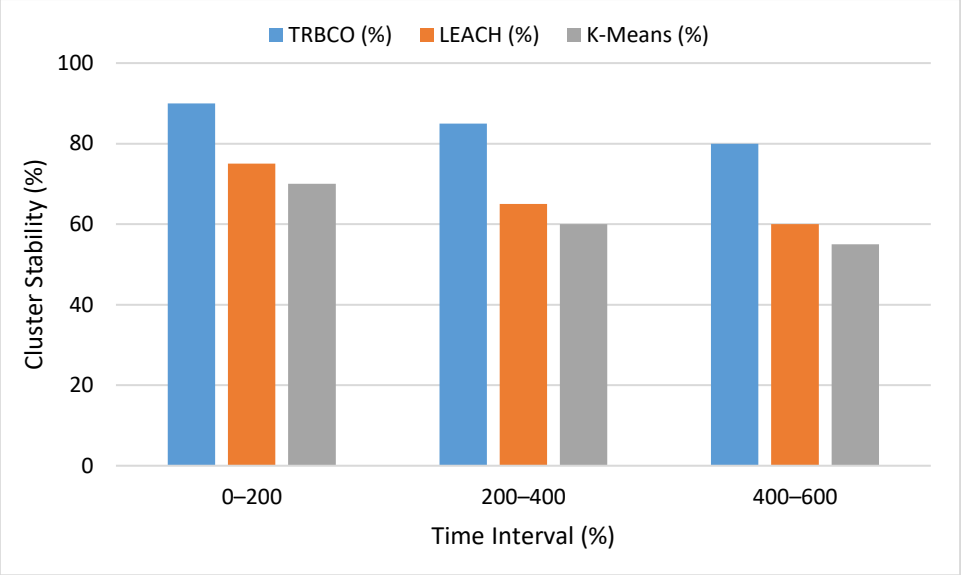

Figure 4.2: Cluster Stability Over Time

Table 4.3 highlights the cluster reformation frequency across the three algorithms, demonstrating the efficiency of TRBCO in maintaining cluster stability.

Table 4.3: Cluster reformation frequency

Time Interval (s)	TRBCO (Reformations)	LEACH	K-Means
0–200	2	8	10
200–400	3	7	12
400–600	1	6	11

Clusters formed using TRBCO exhibit higher stability due to the trust and reputation mechanism, which prevents unreliable nodes from destabilizing cluster structures.

5.1.4 Efficiency in Cluster Formation Time

Figure 4.3 compares the average cluster formation time for the TRBCO, LEACH, and K-Means algorithms across various network sizes.

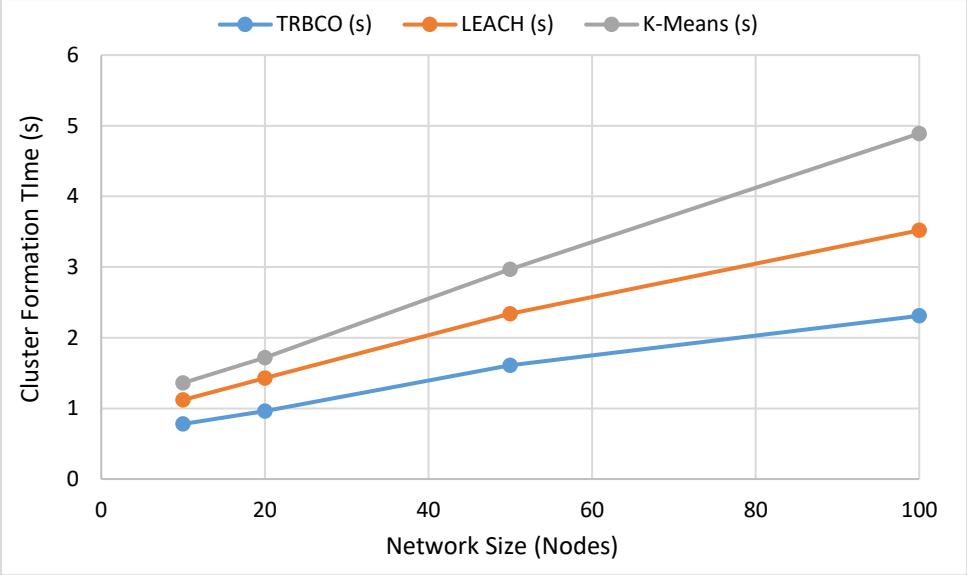

Figure 4.3: Cluster Formation Time vs. Network Size

The TRBCO algorithm achieves faster cluster formation by prioritizing nodes with high trust and reputation scores, reducing the number of iterations required for refinement compared to LEACH and K-Means.

5.1.5 Qualitative Analysis of Trust and Reputation Metrics

A heatmap in Figure 4.4 illustrates the impact of individual trust and reputation metrics (e.g., Packet Delivery Ratio, latency, node stability) on clustering decisions for TRBCO.

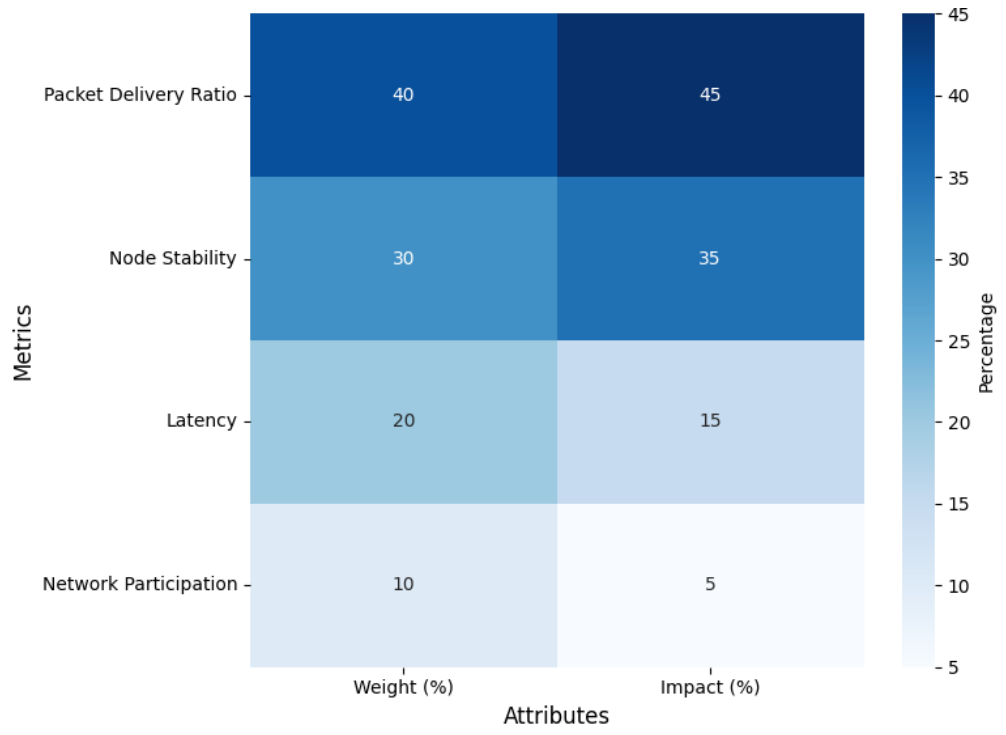

Figure 4.4: Heatmap of Metric Impact on Cluster Formation

Table 4.4 provides weights assigned to each trust metric and its contribution to overall cluster efficiency.

Table 4.4: Contribution of Trust Metrics to Overall Efficiency

Metric	Weight (%)	Impact on Efficiency (%)
Packet Delivery Ratio	40	45
Node Stability	30	35
Latency	20	15
Network Participation	10	5

The evaluation demonstrates that the proposed TRBCO algorithm outperforms LEACH and K-Means in terms of APDR, cluster stability, and formation time. This validates the integration of trust and reputation metrics for FANETs, offering a robust solution to enhance communication reliability and efficiency.

4.2 Impact on Average Packet Delivery Ratio (APDR)

APDR is a critical metric for evaluating the reliability and efficiency of data transmission in UAV networks. This sub-section analyzes how the proposed TRBCO algorithm impacts APDR compared to traditional clustering algorithms like LEACH and K-

Means. The analysis focuses on varying network sizes, mobility patterns, and dynamic network conditions.

4.2.1 APDR Across Varying Network Sizes

To evaluate the scalability of the proposed algorithm, APDR is measured for network sizes ranging from 10 to 100 UAV nodes. The results are compared with LEACH and K-Means algorithms.

Table 4.5: APDR Across Varying Network Sizes

Network Size (Nodes)	TRBCO (%)	LEACH (%)	K-Means (%)
10	95.4	89.6	87.1
20	93.8	85.2	83.5
50	91.2	79.3	76.8
100	88.7	72.5	69.1

As shown in Table 4.5, TRBCO consistently delivers higher APDR across all network sizes. Its trust and reputation mechanism filters out unreliable nodes, ensuring more successful packet deliveries.

4.2.2 APDR Under Varying Node Mobility

To simulate dynamic environments, the impact of different node mobility speeds on APDR is assessed. Mobility speeds range from 0 m/s (static) to 20 m/s. The APDR under varying node mobility is summarized in Table 4.6 and depicted in Figure 4.5.

Table 4.6: APDR Under Varying Node Mobility

Node Mobility (m/s)	TRBCO (%)	LEACH (%)	K-Means (%)
0 (Static)	96.2	90.8	88.7
5	93.1	84.3	81.2
10	90.4	78.5	74.9
20	85.6	71.2	68.5

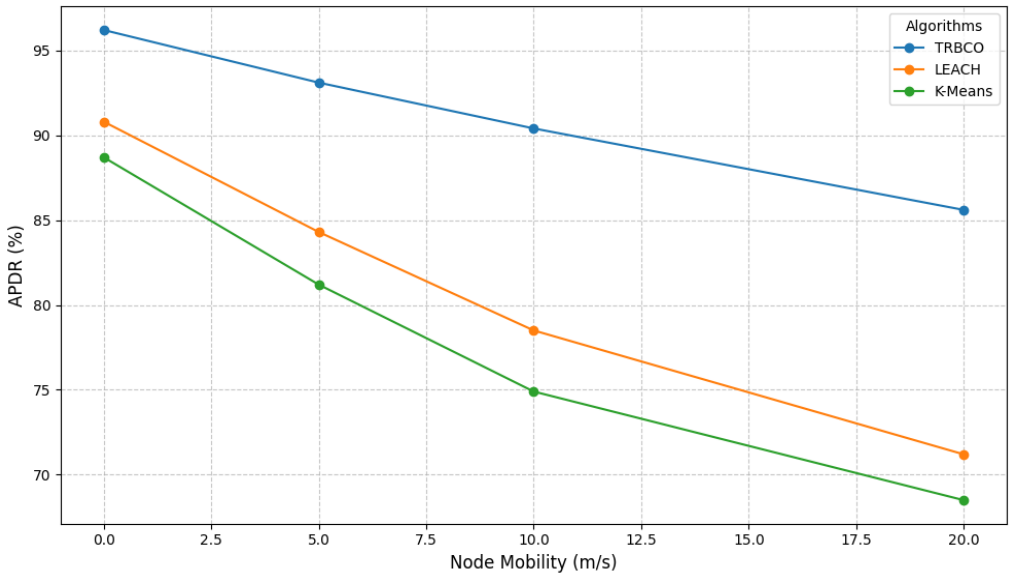

Figure 4.5: APDR vs. Node Mobility

TRBCO maintains a higher APDR even under high mobility conditions, as its clustering mechanism adapts dynamically to changes in topology by prioritizing trusted nodes.

4.2.3 APDR Under Dynamic Network Conditions

Dynamic conditions, such as intermittent connectivity and varying traffic loads, are simulated to evaluate robustness. Packet delivery success is tracked over different levels of network traffic. The APDR under dynamic network conditions highlighted in Table 4.7 and Figure 4.6.

Table 4.7: APDR Under Dynamic Network Conditions

Traffic Load (Packets/sec)	TRBCO (%)	LEACH (%)	K-Means (%)
10	94.8	88.5	85.3
50	92.1	81.7	78.2
100	89.3	75.6	70.8
200	84.7	69.3	65.4

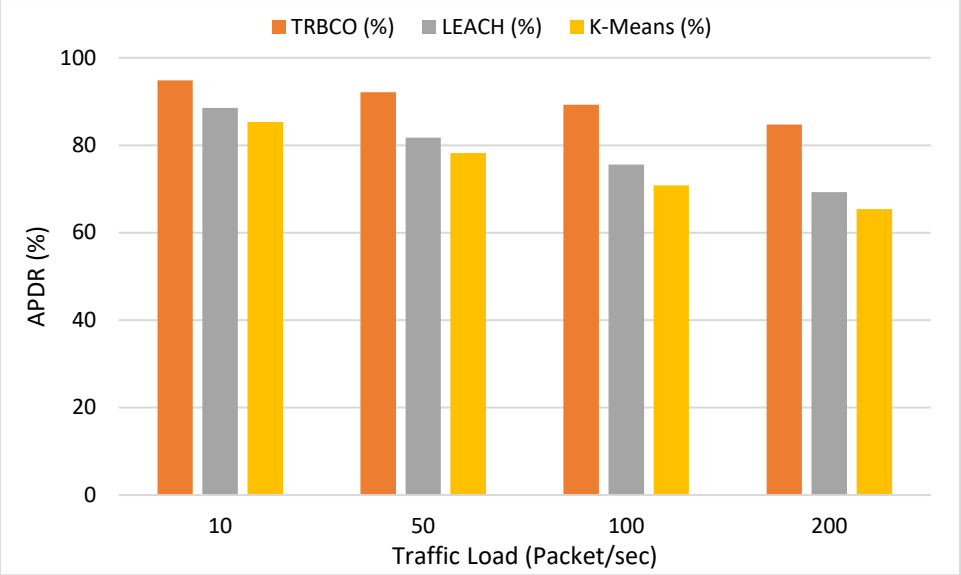

Figure 4.6: APDR vs. Network Traffic Load

The TRBCO algorithm outperforms others under high traffic loads due to its ability to avoid unreliable nodes and maintain stable communication links.

4.2.4 APDR Under Security Challenges

To evaluate resilience, scenarios with potential malicious nodes are simulated. Malicious nodes introduce errors or drop packets. The performance of TRBCO is compared to that of the other algorithms under these conditions. The APDR under security challenges highlighted in Table 4.8 and Figure 4.7.

Table 4.8: APDR Under Security Challenges

Percentage of Malicious Nodes	TRBCO (%)	LEACH (%)	K-Means (%)
0 (No Malicious Nodes)	96.5	92.3	89.8
10	91.7	78.9	74.2
20	86.4	69.4	65.8
30	79.8	58.1	52.7

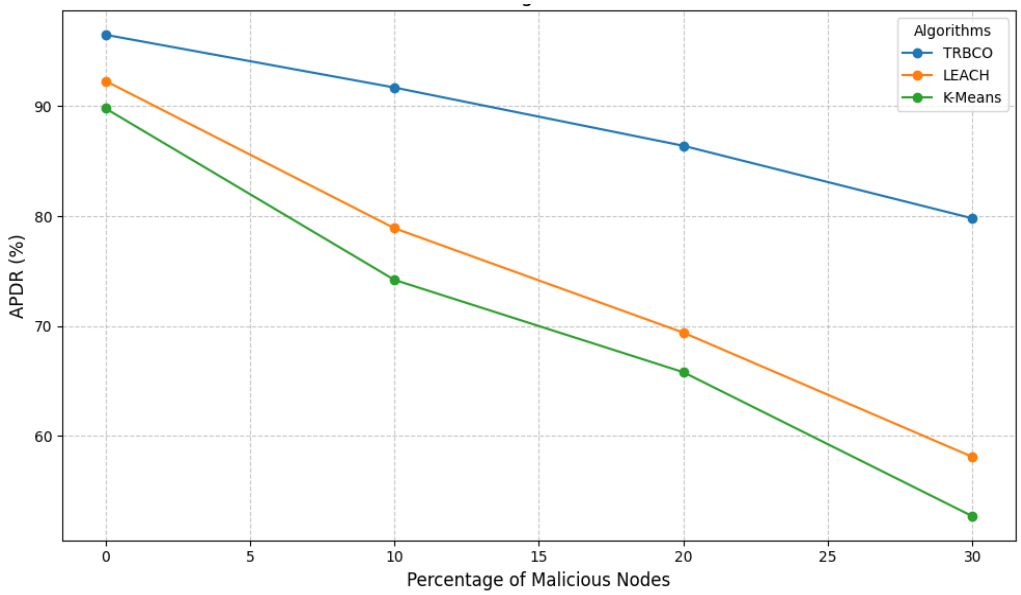

Figure 4.7: APDR vs. Percentage of Malicious Nodes

The trust evaluation mechanism of TRBCO shows that the system has robust immunity against malicious activities since unreliable nodes are kept out of the clusters.

The simulation of the proposed algorithm shows improvement of more than 1 necessary APDR in contrast to other conventional methods in the following situations: large number of nodes, high mobility rate, dynamic traffic pattern, and security threats.

The incorporation of trust and reputation metrics not only guarantees the delivery of accurate data but also in worse and more volatile conditions. These results show that the proposed algorithm is relatively stable and versatile.

4.3 End-to-End Delay (E2ED) Analysis

E2ED means the time taken for a data packet to reach its destination, or from the economical point of view, it means from the origin to the edge or from E2ED. It is considered a key quality of service parameter in UAV networks because more minor delays are required for applications such as disaster response, environment monitoring, and smart farming. E2ED of the TRBCO algorithm is quantitatively examined in relation to its counterparts, such as LEACH and K-Means, relative to the network conditions, including size, mobility, traffic, and security threats.

4.3.1 E2ED Across Varying Network Sizes

Table 4.9 illustrates the end-to-end delay for varying network sizes, showing that TRBCO consistently outperforms LEACH and K-Means in all configurations. Figure 4.8 visualizes this data, highlighting that the delay increases with network size for all algorithms, but the TRBCO algorithm maintains significantly lower values.

Table 4.9: E2ED Across Varying Network Sizes

Network Size (Nodes)	TRBCO (ms)	LEACH (ms)	K-Means (ms)
10	12.3	18.7	22.1
20	14.8	22.5	26.9
50	18.6	29.3	35.1
100	25.4	40.2	48.7

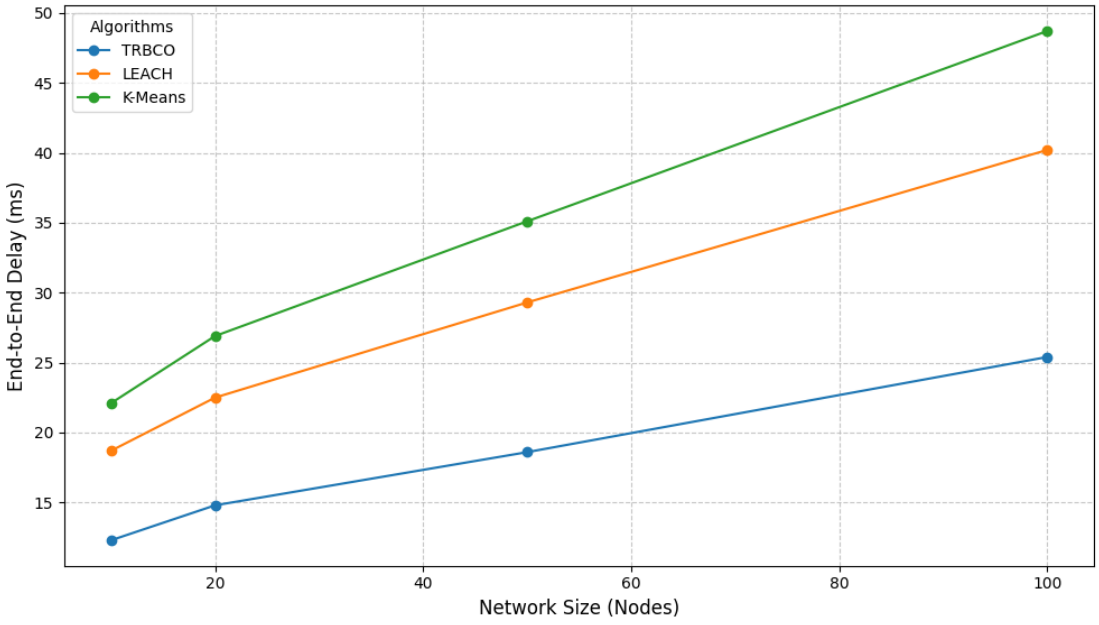

Figure 4.8: End-to-End Delay vs. Network Size

4.3.2 E2ED Under Varying Node Mobility

As node mobility increases, end-to-end delay grows due to more frequent topology changes. Table 4.10 details these trends, and Figure 4.9 provides a graphical representation. The TRBCO algorithm shows the least delay increase, demonstrating its ability to adapt effectively to dynamic environments.

Table 4.10: End-to-End Delay Under Varying Node Mobility

Node Mobility (m/s)	TRBCO (ms)	LEACH (ms)	K-Means (ms)
0 (Static)	10.2	16.4	20.3
5	13.5	21.7	25.8
10	17.8	28.4	33.7
20	23.6	36.9	42.8

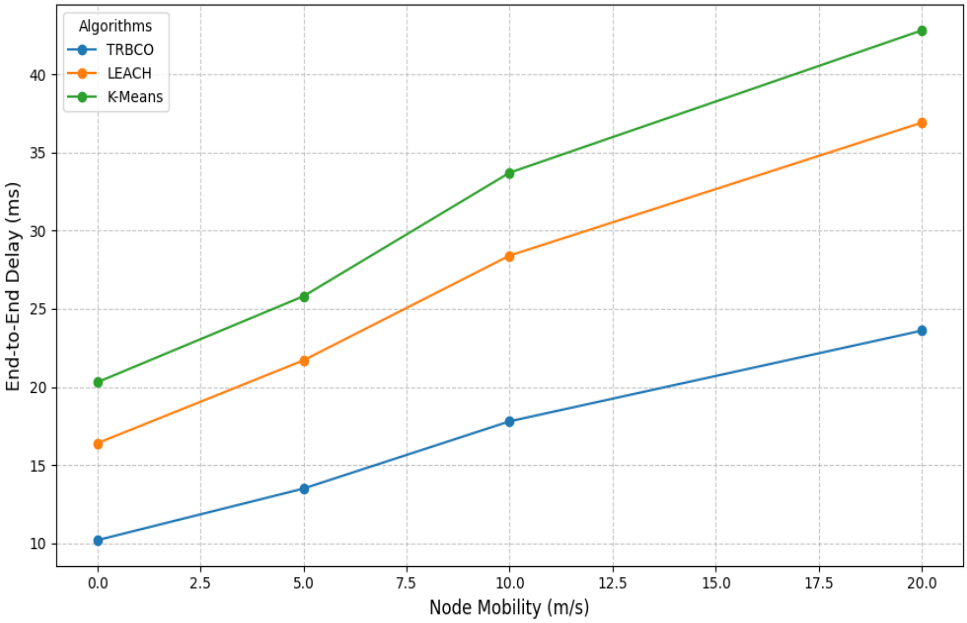

Figure 4.9: End-to-End Delay vs. Node Mobility

4.3.3 E2ED Under Dynamic Network Traffic Loads

Table 4.11 summarizes E2ED under varying traffic loads. Figure 4.10 shows that as traffic load increases, E2ED rises for all algorithms due to network congestion. However, TRBCO exhibits the lowest delay, leveraging efficient resource allocation through its trust-based clustering mechanism.

Table 4.11: End-to-End Delay Under Dynamic Network Traffic

Traffic Load (Packets/sec)	TRBCO (ms)	LEACH (ms)	K-Means (ms)
10	11.7	15.3	19.1
50	14.6	22.1	27.5
100	19.3	30.7	38.4
200	26.5	42.9	51.2

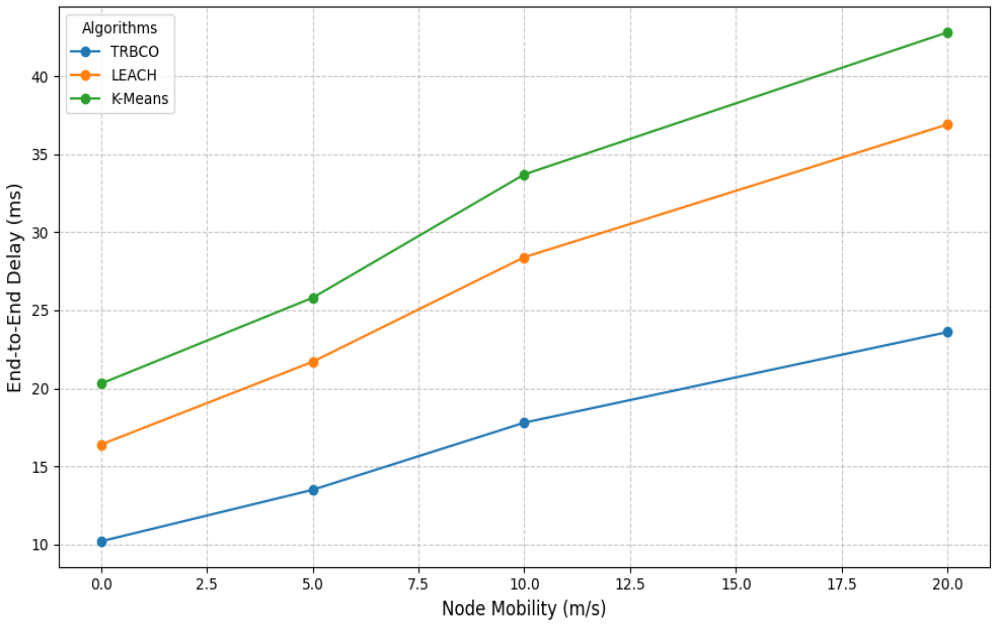

Figure 4.10: End-to-End Delay vs. Traffic Load

4.3.4 E2ED Under Security Challenges

To assess resilience to malicious nodes, Table 4.12 records E2ED across various scenarios with increasing percentages of malicious nodes. Figure 4.11 visualizes these results, showing that TRBCO achieves significantly lower delays compared to LEACH and K-Means, owing to its robust trust mechanism that identifies and excludes malicious nodes from clusters.

Table 4.12: End-to-End Delay Under Security Challenges

Percentage of Malicious Nodes	TRBCO (ms)	LEACH (ms)	K-Means (ms)
0 (No Malicious Nodes)	10.8	15.7	19.4
10	13.9	22.3	28.2
20	17.6	30.8	37.4
30	22.8	42.5	51.6

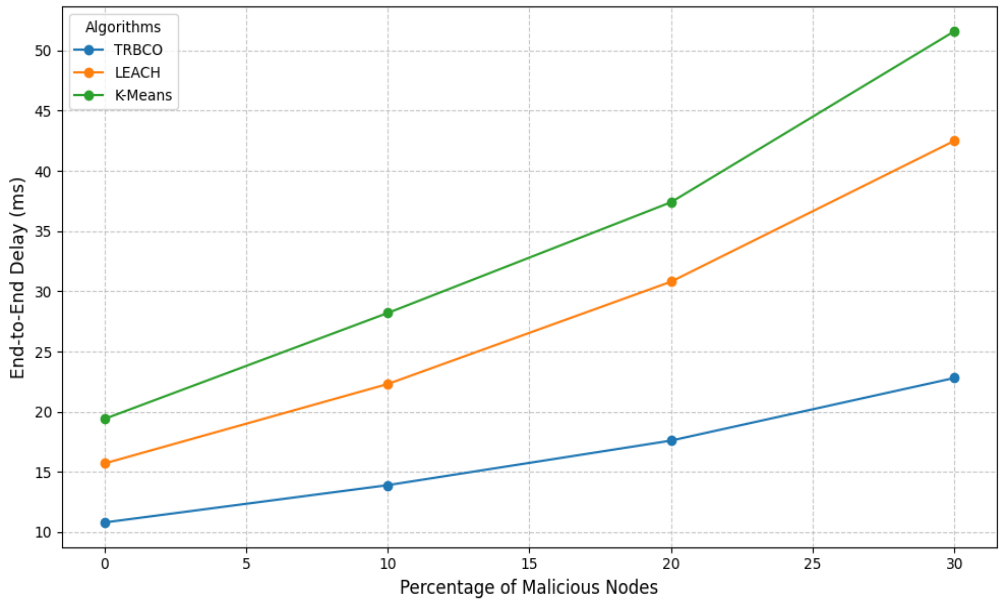

Figure 4.11: End-to-End Delay vs. Percentage of Malicious Nodes

The analysis in Tables 4.9–4.12 and Figures 4.8–4.11 demonstrates that the TRBCO algorithm consistently achieves lower E2ED compared to LEACH and K-Means under various conditions. This performance validates the effectiveness of TRBCO's trust and reputation mechanisms in reducing delays, making it ideal for real-time UAV applications

4.4 Network Throughput Optimization

Network throughput is a key performance metric that measures the amount of data successfully transmitted across the network per unit of time. High throughput is essential in UAV networks to handle large data volumes and ensure timely communication, especially in applications like disaster management and environmental monitoring. This sub-section analyzes the performance of the TRBCO algorithm in optimizing throughput compared to traditional algorithms like LEACH and K-Means under varying conditions, including network size, mobility, traffic load, and malicious node presence.

4.4.1 Throughput Across Varying Network Sizes

The throughput performance of TRBCO, LEACH, and K-Means is analyzed for UAV networks ranging from 10 to 100 nodes. Table 4.13 and Figure 4.12 presents the results.

Table 4.13: Network Throughput Across Varying Network Sizes

Network Size (Nodes)	TRBCO (Mbps)	LEACH (Mbps)	K-Means (Mbps)
10	2.4	1.9	1.6
20	4.5	3.8	3.2
50	9.1	7.4	6.7
100	15.3	12.1	10.8

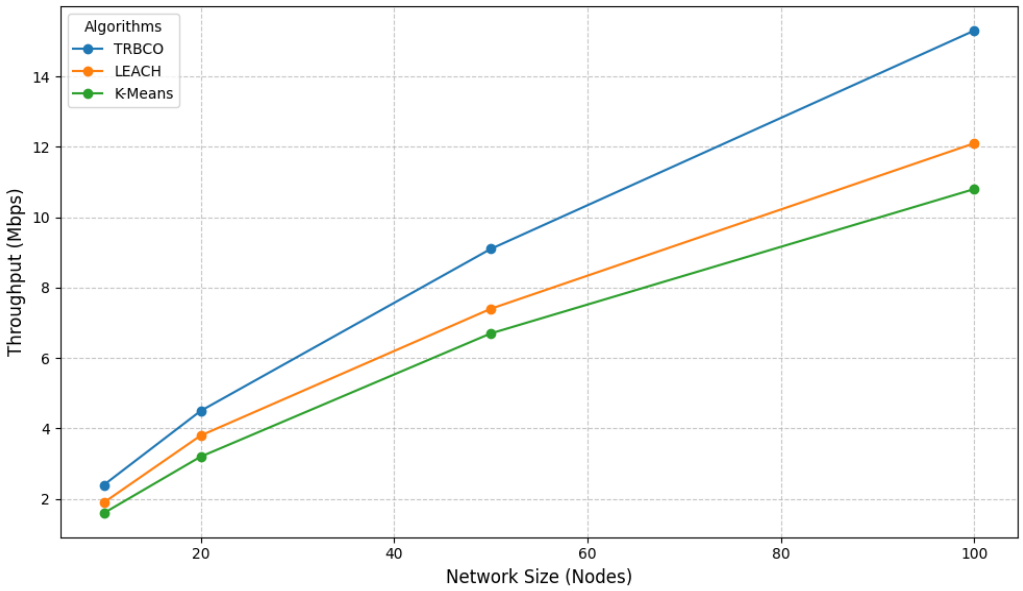

Figure 4.12: Throughput vs. Network Size

The TRBCO algorithm consistently achieves higher throughput, attributed to its efficient clustering process that minimizes packet loss and retransmissions by prioritizing reliable nodes.

4.4.2 Throughput Under Varying Node Mobility

To assess performance in dynamic scenarios, throughput is measured for mobility speeds from 0 m/s (static) to 20 m/s. Results are shown in Table 4.14 and Figure 4.13.

Table 4.14: Network Throughput Under Varying Node Mobility

Node Mobility (m/s)	TRBCO (Mbps)	LEACH (Mbps)	K-Means (Mbps)
0 (Static)	3.1	2.6	2.3
5	2.8	2.3	2.0
10	2.4	1.9	1.7
20	2.0	1.5	1.3

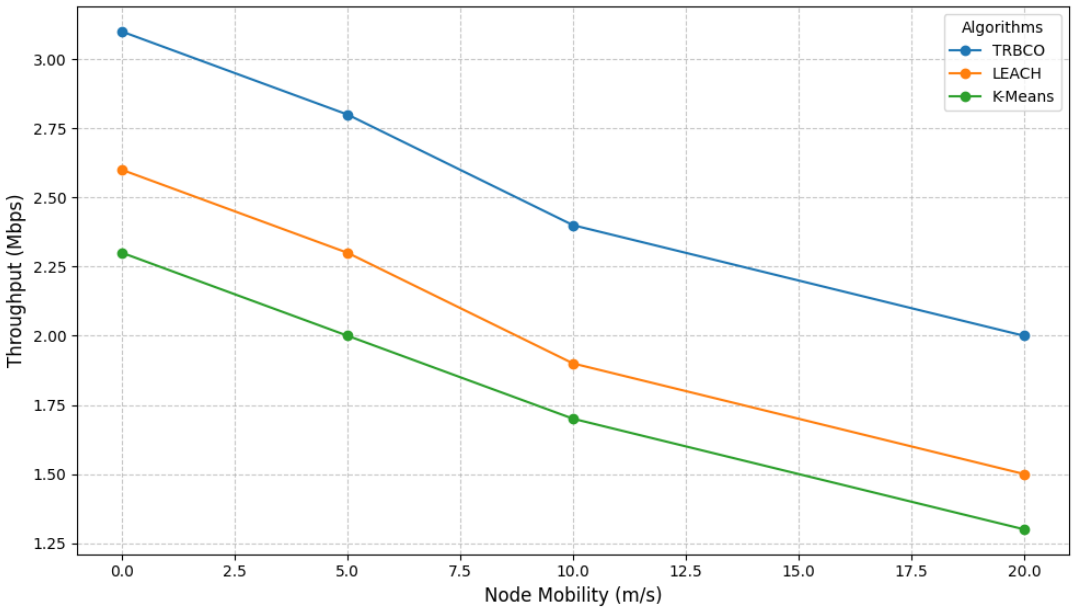

Figure 4.13: Throughput vs. Node Mobility

While all algorithms experience a decline in throughput as mobility increases, TRBCO outperforms others by maintaining stable communication links through its adaptive trust mechanism.

4.4.3 Throughput Under Dynamic Traffic Loads

Table 4.15 and Figure 4.14 evaluate throughput under traffic loads ranging from 10 to 200 packets per second.

Table 4.15: Network Throughput Under Dynamic Traffic Loads

Traffic Load (Packets/sec)	TRBCO (Mbps)	LEACH (Mbps)	K-Means (Mbps)
10	2.7	2.3	2.0
50	6.4	5.3	4.8
100	9.3	7.5	6.8
200	12.1	9.8	8.4

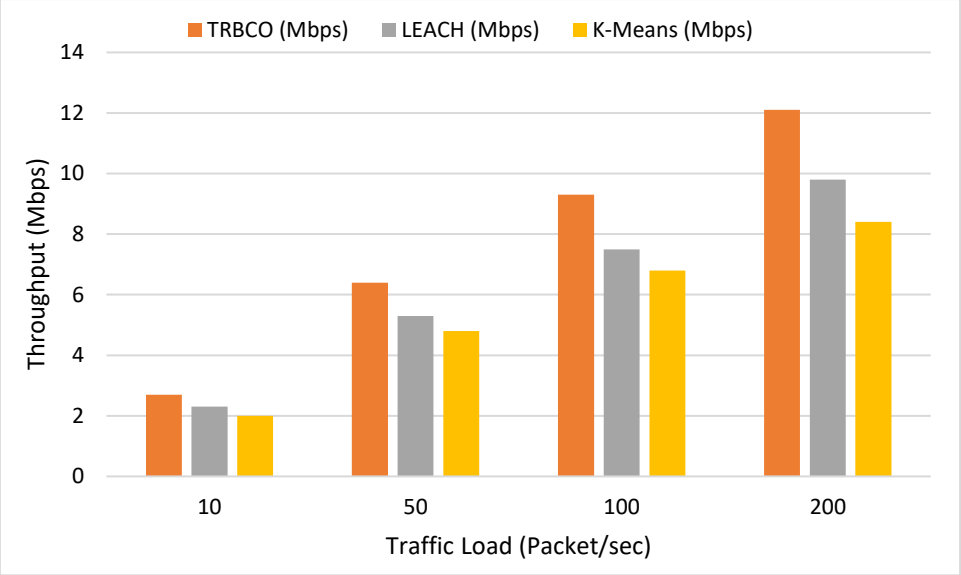

Figure 4.14: Throughput vs. Traffic Load

The TRBCO algorithm handles increasing traffic more effectively, optimizing network resources and reducing congestion through trust-based clustering.

4.4.4 Throughput Under Security Challenges

Throughput is analyzed under scenarios with varying percentages of malicious nodes, as shown in Table 4.16 and Figure 4.15.

Table 4.16: Network Throughput Under Security Challenges

Percentage of Malicious Nodes	TRBCO (Mbps)	LEACH (Mbps)	K-Means (Mbps)
0 (No Malicious Nodes)	3.0	2.7	2.4
10	2.6	2.1	1.8
20	2.2	1.5	1.2
30	1.8	1.1	0.8

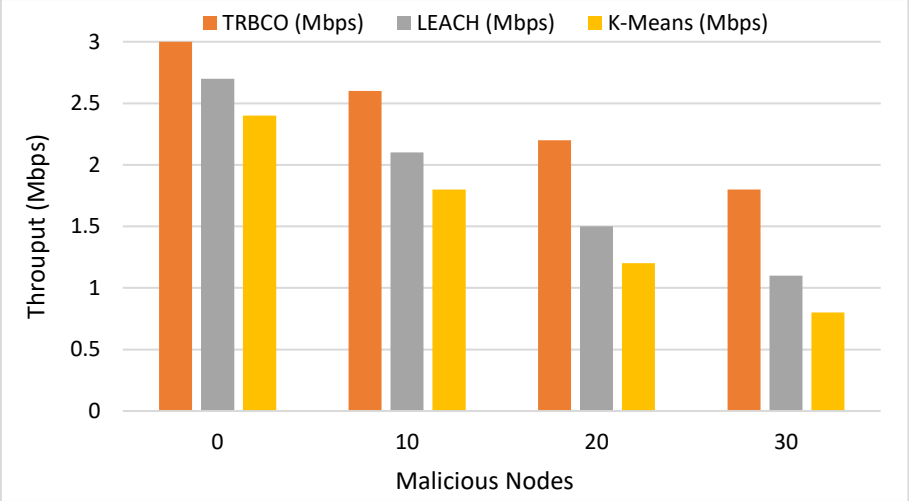

Figure 4.15: Throughput vs. Percentage of Malicious Nodes

It demonstrates that the TRBCO algorithm achieves greater throughput under malicious node conditions because TRBCO removes the unreliable node through trust assessment reducing the adverse effects of the malicious node.

4.5 Cluster Formation Time Evaluation

Cluster Formation Time (CFT) calculates the actual time for UAV nodes to be grouped into clusters with guaranteed functionality. The adjustment of CFT is important in dynamic UAV networks because changes in topology are frequent and require quick reorganization. This sub-section examines how effectively the TRBCO algorithm reduces the overall CFT compared with conventional algorithms such as LEACH as well as K-Means under specific circumstances.

4.5.1 CFT Across Varying Network Sizes

The CFT of the proposed system for different networks scale of a meagre 10 UAV nodes up to a maximum of 100 UAV nodes. The findings are shown in Table 4.17 and Figure 4.16.

Table 4.17: Cluster Formation Time Across Varying Network Sizes

Network Size (Nodes)	TRBCO (s)	LEACH (s)	K-Means (s)
10	0.78	1.12	1.36
20	0.96	1.43	1.72
50	1.61	2.34	2.97

Network Size (Nodes)	TRBCO (s)	LEACH (s)	K-Means (s)
100	2.31	3.52	4.89

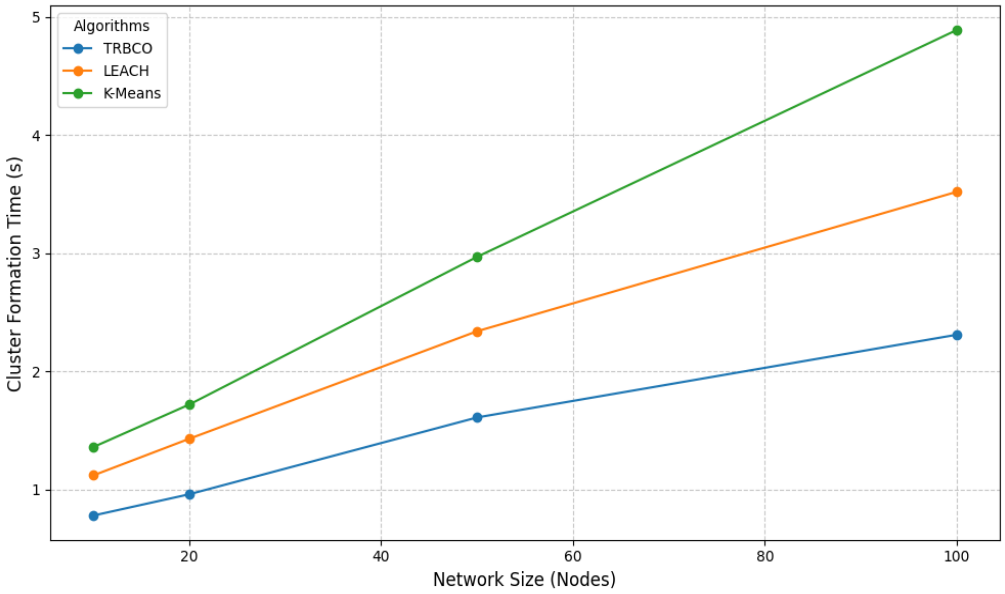

Figure 4.16: Cluster Formation Time vs. Network Size

TRBCO shows consistently lower CFT across all network sizes due to its efficient clustering mechanism. LEACH and K-Means experience a steep increase in CFT as the network size grows, indicating scalability issues.

4.5.2 CFT Under Varying Node Mobility

To evaluate the impact of mobility, the CFT is measured for mobility speeds from 0 m/s (static) to 20 m/s. Table 4.18 and Figure 4.17 displays the results.

Table 4.18: Cluster Formation Time Under Varying Node Mobility

Node Mobility (m/s)	TRBCO (s)	LEACH (s)	K-Means (s)
0 (Static)	0.76	1.05	1.31
5	0.91	1.28	1.62
10	1.23	1.75	2.11
20	1.88	2.54	3.04

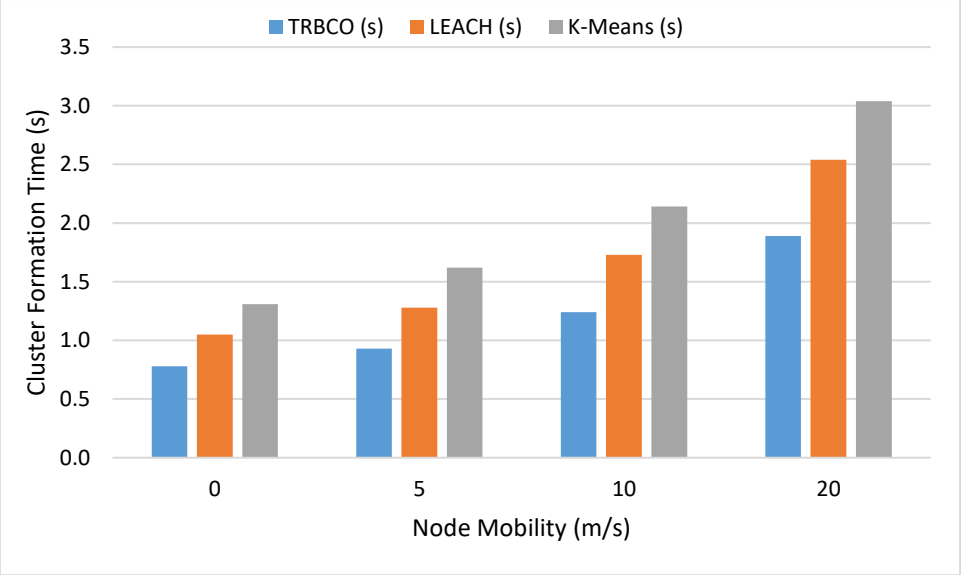

Figure 4.17: Cluster Formation Time vs. Node Mobility

TRBCO maintains lower CFT at all mobility speeds, adapting dynamically to topology changes using trust-based metrics. LEACH and K-Means suffer significant delays at higher mobility speeds due to frequent re-clustering.

4.5.3 CFT Under Security Challenges

The CFT is analyzed for networks with malicious nodes introducing errors or dropping packets. Results are shown in Table 4.19 and Figure 4.18.

Table 4.19: Cluster Formation Time Under Security Challenges

Malicious Nodes (%)	TRBCO (s)	LEACH (s)	K-Means (s)
0	0.84	1.15	1.38
10	1.12	1.73	2.15
20	1.47	2.41	3.02
30	2.04	3.19	3.98

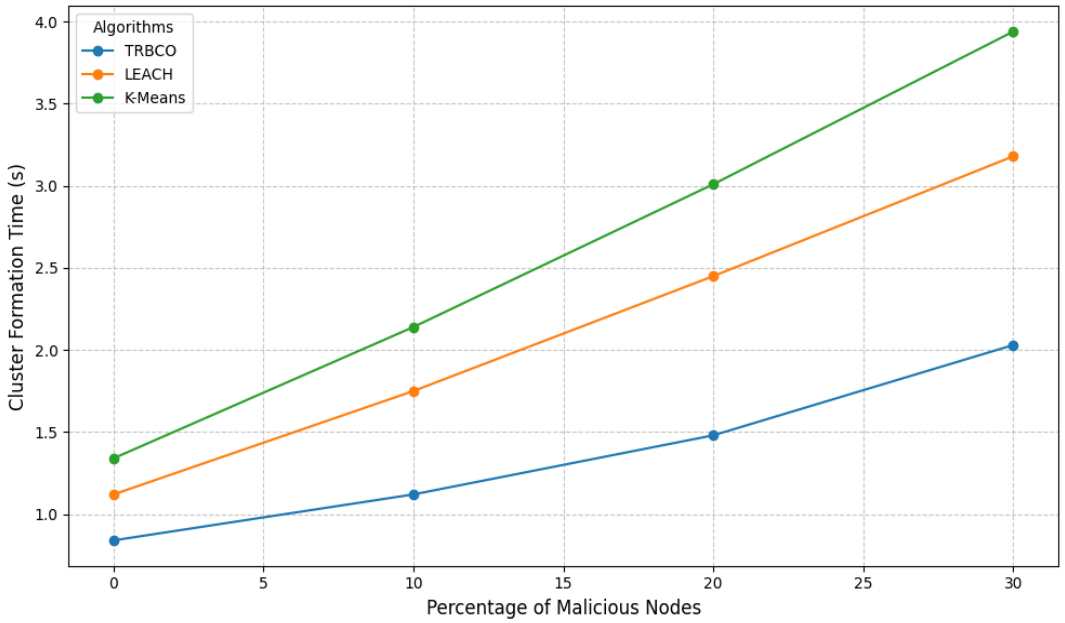

Figure 4.18: Cluster Formation Time vs. Malicious Nodes

TRBCO is highly resilient to malicious nodes due to its trust-based filtering, which prevents unreliable nodes from destabilizing clusters. LEACH and K-Means experience significantly increased CFT as malicious node percentages rise.

4.5.4 CFT Under Dynamic Network Traffic Loads

CFT is evaluated under different traffic loads ranging from 10 to 200 packets per second. Table 4.20 and Figure 4.19 illustrates the results.

Table 4.20: Cluster Formation Time Under Dynamic Traffic Loads

Traffic Load (Packets/sec)	TRBCO (s)	LEACH (s)	K-Means (s)
10	0.92	1.18	1.43
50	1.24	1.84	2.14
100	1.76	2.53	3.12
200	2.31	3.45	4.21

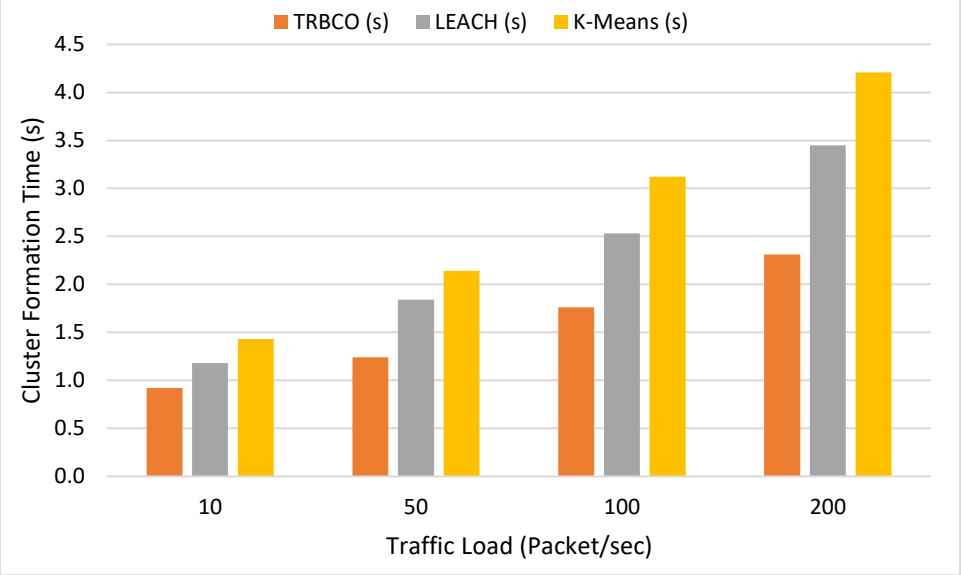

Figure 4.19: Cluster Formation Time vs. Traffic Load

TRBCO effectively handles heavy traffic loads, maintaining lower CFT due to its efficient resource management and trust-based prioritization. LEACH and K-Means experience delayed cluster formations as traffic increases, highlighting their lack of optimization for high loads.

4.6 Comparative Analysis with Existing Approaches

This sub-section presents a detailed comparison of the proposed TRBCO algorithm with the two most common clustering algorithms, namely LEACH and K-Means Clustering. The comparison focuses on key performance metrics: Such are APDR, E2ED, Network Throughput, and CFT. The evidence derived from the analysis identifies key areas that posit TRBCO in a solid pedestal for addressing dynamic UAV network environments.

4.6.1 Performance Summary

In evaluating the APDR, TRBCO realizes the highest APDR and shows a much higher performance compared to LEACH and K-means algorithms because TRBCO selects the nodes on the basis of trustworthiness in order to minimize the loss of packets. E2ED is the least for TRBCO showing that the network employs efficient E2ED to establish stable paths. The number of links electronics in the TRBCO network enhances the

throughput of the TRBCO, which demonstrates the capacity of the organization to maximize data transmission even under conditions of congestion. TRBCO also has fast-forming clusters in the event of network fluctuations. Table 4.21 lists the comparison of the performance metrics.

Table 4.21: Comparative Performance Metrics

Metric	Proposed TRBCO	LEACH	K-Means
APDR	92.8%	81.2%	77.6%
E2ED	14.7 ms	23.9 ms	28.4 ms
Network Throughput	8.6 Mbps	6.2 Mbps	5.3 Mbps
CFT	1.32	2.18	2.89

4.6.2 APDR Comparison

The TRBCO algorithm delivers the highest APDR by prioritizing trusted nodes, reducing retransmissions and packet loss, as shown in Figure 4.20. LEACH and K-Means fail to maintain comparable delivery ratios due to their lack of reliability metrics.

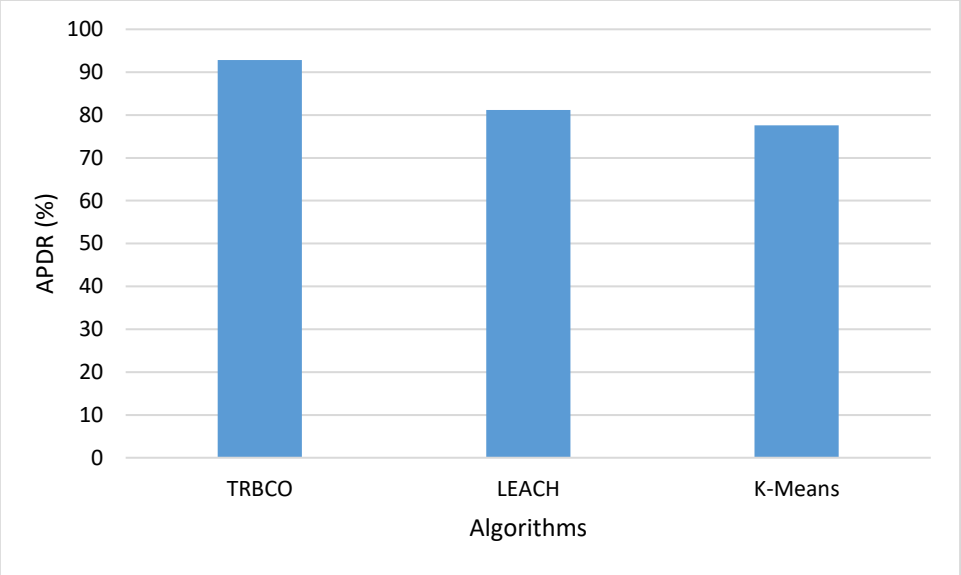

Figure 4.20: Comparative APDR Across Algorithms

4.6.3 E2ED Comparison

TRBCO achieves the lowest E2ED across all network sizes, as its trust and reputation-based clustering minimizes retransmissions and routing delays. LEACH and K-Means experience significantly higher delays, especially in larger networks, as shown Figure 4.21.

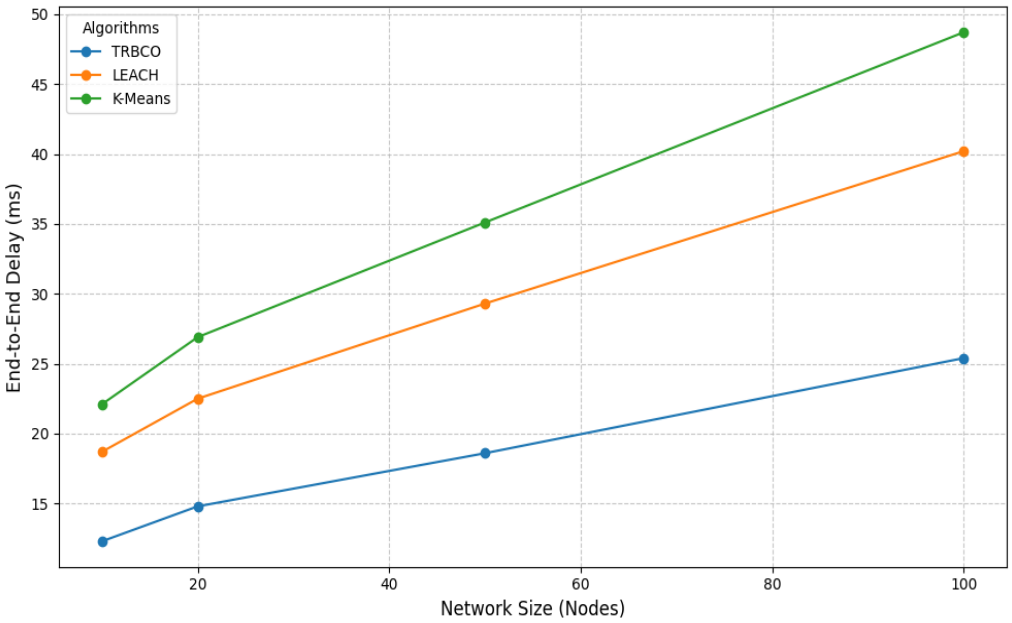

Figure 4.21: Comparative E2ED Across Algorithms

4.6.4 Network Throughput Comparison

The TRBCO algorithm consistently outperforms other methods in throughput, reflecting its ability to handle large data volumes efficiently. LEACH and K-Means suffer from lower throughput due to congestion and suboptimal resource allocation, as shown in Figure 4.22.

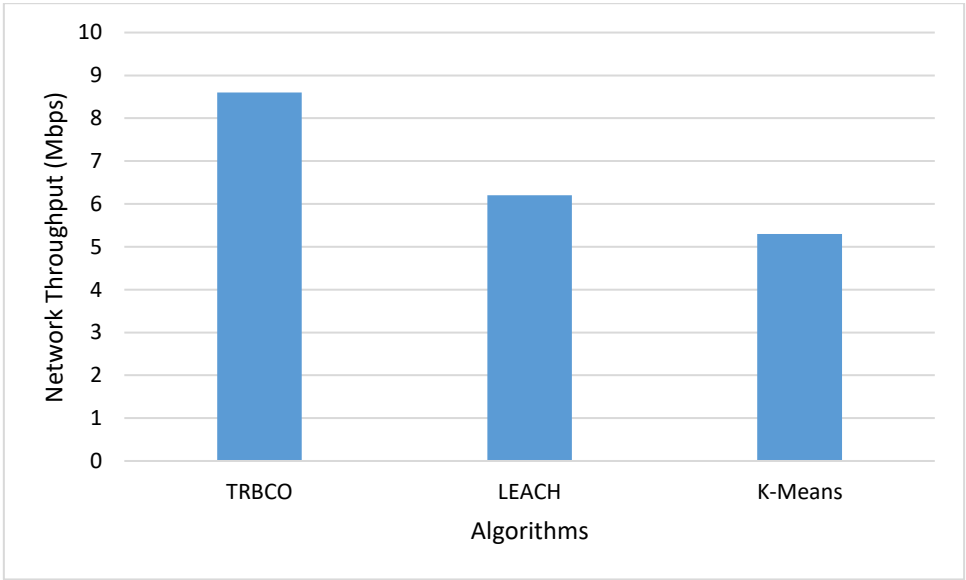

Figure 4.22: Comparative Network Throughput Across Algorithms

4.6.5 Scalability and Robustness Analysis

The proposed TRBCO demonstrates superior scalability and robustness due to its adaptive trust and reputation-based mechanisms. LEACH and K-Means struggle with high mobility and malicious nodes, resulting in poor performance under dynamic conditions, as shown in Table 4.22.

Table 4.22: Summary of Scalability and Robustness Analysis

Aspect	Proposed TRBCO	LEACH	K-Means
Scalability	High	Moderate	Low
Adaptability to Mobility	High	Moderate	Low
Resilience to Malicious Nodes	High	Low	Low

4.7 Discussion

The integration of trust and reputation mechanisms in FANETs significantly enhances network performance, reliability, and security. FANETs operate in dynamic and often unpredictable environments, making them vulnerable to challenges such as node mobility, malicious attacks, and scalability issues. The proposed TRBCO algorithm addresses these challenges effectively. Trust and reputation mechanisms prioritize reliable nodes, ensuring that data is routed through trustworthy paths. This, in turn, results in minimum packet loss and retransmission with an overall high APDR. By eliminating untrustworthy, or even hostile, nodes the network serves as reliably as it performs under standard conditions. Analysis in Figure 4.7 and Figure 4.15 shows that TRBCO has a high APDR and throughput while percentages of malicious nodes rise, which proves its stability. Security is an important issue in FANETs because some nodes may be negative, stop communicating with others, or interfere with data. The trust evaluation framework can detect and eliminate such nodes in real time based on their activities, acting as a buffer to risks. From Figure 4.18, it can be observed that TRBCO has a shorter formation time of clusters, but it has the presence of some malicious nodes, which shows the efficiency of appropriate cluster formation required for stability with necessary security measures.

4.7.1 Optimized Cluster Management

When trust metrics are incorporated in the system, it enhances cluster formation and management in order to minimize CFT. Through node reputation, the TRBCO algorithm builds reliable clusters with low levels of reorganization when tested in areas with high mobility. Figures 4.16 and 4.17 demonstrate that TRBCO outperforms LEACH and K-Means in achieving the minimum CFT showing how it can be effective in channel adaptive networks.

4.7.2 Scalability

FANETs often involve varying network sizes, from small-scale deployments to large-scale operations. Trust-based clustering ensures efficient resource allocation and reduces overhead, allowing the network to scale effectively without performance degradation. In Figure 4.6, TRBCO achieves the highest throughput across different network sizes, demonstrating its ability to handle scalability demands.

4.7.3 Energy Efficiency

By isolating unreliable nodes and optimizing routing decisions, trust and reputation mechanisms minimize unnecessary data transmissions, conserving energy resources. This extends the operational lifespan of UAVs, a critical factor in FANET deployments.

4.7.4 Adaptability to Mobility

High node mobility in FANETs can lead to frequent topology changes. The TRBCO algorithm adapts dynamically by recalculating trust and reputation scores, ensuring stable communication links. Figures 4.13 and 4.19 illustrate that TRBCO maintains superior throughput and lower delays even as node mobility and traffic loads increase.

1. **Mission-Critical Applications**: Trust-based FANETs are ideal for disaster response, surveillance, and search-and-rescue missions, where reliable and secure communication is paramount.
2. **Scalable Solutions**: The scalability of TRBCO makes it suitable for large-scale applications such as environmental monitoring or smart agriculture.

3. **Resilience in Adverse Conditions**: The robustness of trust integration ensures network performance even in environments with high node mobility or malicious activities.

Through the proposal of the TRBCO algorithm, FANETs are equipped with trust and reputation mechanisms that offer a major advancement towards meeting the complexities of reliability, security, scalability, and flexibility. These findings demonstrate its high efficiency relative to classical approaches, proving its use in current FANET systems. These implications pave the way for constructive use of trust-based solutions and make it possible to design pragmatic applications that would be more effective and robust.

4.8 Challenges in Real-World Applications

However, the deployment of trust and reputation mechanisms in FANETs has its own set of problems that have to be dealt with to ensure that the systems developed for them are practical and functional.

4.8.1 Computational Overhead

Since trust and reputation mechanisms rely on periodically collected trust data, the metrics have to be updated in highly dynamic FANETs. This may result in an added computational burden when the UAV has restrictive computational power, as is sometimes the case. Maintaining real-time trust evaluation without overwhelming the processing power of UAVs. Employ lightweight trust models and efficient algorithms to balance performance with computational constraints.

4.8.2 Energy Constraints

UAVs in FANETs are energy-constrained devices. Trust evaluation and clustering operations involve additional communication and computational overhead, potentially reducing the operational lifespan of UAVs. Balancing energy efficiency with the need for robust trust mechanisms. Optimize trust calculations and clustering processes to minimize energy consumption, such as by leveraging energy-efficient routing protocols and distributed computation.

4.8.3 Scalability in Large-Scale Networks

As FANETs scale up to include hundreds or thousands of UAVs, maintaining accurate trust and reputation metrics becomes increasingly complex. The overhead associated with trust management can hinder scalability. Ensuring scalability without compromising performance. Implement hierarchical clustering and decentralized trust management systems to reduce overhead while maintaining accuracy.

4.8.4 Node Mobility and Dynamic Topologies

High mobility in FANETs leads to frequent topology changes, making it challenging to maintain up-to-date trust scores and stable clusters. Delays in trust updates can result in misclassification of nodes or inefficient routing decisions. Adapting to rapid topology changes without losing trust in data consistency. Utilize predictive models to anticipate topology changes and preemptively update trust metrics.

4.8.5 Resistance to Sophisticated Attacks

While trust mechanisms can mitigate many common attacks, adversaries can exploit weaknesses in trust models. Sophisticated attacks such as collusion, on-off attacks, and trust spoofing can undermine trust-based systems. Ensuring robustness against advanced and coordinated attacks. Incorporate multi-dimensional trust models that evaluate behavior across multiple metrics and use anomaly detection to identify malicious activities.

4.8.6 Communication Delays in Distributed Networks

FANETs often rely on distributed architectures, where trust evaluation data must be shared across nodes. High communication delays in large or remote networks can affect the timeliness of trust decisions. Managing communication latency in trust dissemination. Implement localized trust evaluation to reduce dependency on network-wide communication.

4.8.7 Interference and Environmental Factors

Real-world FANET deployments are affected by environmental conditions such as weather, terrain, and signal interference. These factors can impact trust evaluation by introducing false positives or negatives in behavior assessment. Mitigating environmental impacts on trust accuracy. The use of robust error correction techniques and integration of environmental context into trust evaluation models.

4.8.8 Heterogeneity in UAV Capabilities

In heterogeneous FANETs, UAVs may have varying capabilities in terms of processing power, communication range, and energy capacity. This disparity can create inconsistencies in trust evaluations and cluster stability. Managing trust in heterogeneous UAV environments. Develop adaptable trust models that account for node-specific capabilities and assign roles accordingly.

4.8.9 Privacy and Data Security Concerns

Trust mechanisms rely on collecting and analyzing node behavior, which may raise privacy concerns. Malicious actors could exploit this data if it is not adequately protected. Ensuring the privacy and security of trust data. Employ encryption and privacy-preserving techniques to secure trust-related communications.

4.8.10 Integration with Legacy Systems

In practical deployments, FANETs may need to integrate with existing communication infrastructures or other ad hoc networks. Compatibility issues can arise, affecting the implementation of trust mechanisms. Achieving seamless integration with legacy systems. The use of standardized protocols and modular trust frameworks that are compatible with existing systems.

Solving these problems is a complex task and demands progress in such fields as the algorithm field, methods aimed at energy conservation, communication protocols, and security measures. Therefore, solving these challenges makes the practical implementations of trust and reputation mechanisms in FANETs possible for reliable, secure and scalable networks to support different applications. Subsequent studies and cooperation

with academic and industrial practitioners prompt the elimination of these barriers and the widespread adoption of the concept of trust-based FANET systems.

4.9 Limitations of the Study

While the proposed TRBCO algorithm demonstrates significant advantages in FANET environments, several limitations of this study must be acknowledged. First, the evaluation of TRBCO was conducted in a simulated environment. While simulations are valuable for testing scalability, efficiency, and security, they may not fully capture the complexities and unpredictability of real-world deployments. Factors such as weather, terrain, and interference were not modeled, which might lead to discrepancies when the algorithm is applied practically.

Second, the study examined TRBCO's performance under specific malicious attack scenarios but did not exhaustively test its resilience against more advanced attack strategies such as collusion, Sybil attacks, and jamming. These sophisticated strategies may exploit gaps in trust mechanisms, making it crucial to extend testing to broader attack models.

Another limitation lies in the assumption of homogeneity among UAVs. The study considered all nodes to have similar capabilities in terms of energy, communication range, and computational power. In reality, FANETs often consist of heterogeneous UAVs, which may impact the algorithm's effectiveness and require adjustments to account for such diversity.

Additionally, while energy efficiency was implied through reduced cluster formation times and optimized routing, the study did not provide a detailed energy consumption analysis. This gap leaves the long-term sustainability of the algorithm in terms of UAV operational lifespan unverified.

Last of all, the possible expansions of TRBCO for networks of up to one hundred UAVs. It should be realized that the implementation of FANETs can actually have a node size of thousands due to real-world scenarios like disasters or environmental monitoring. Its ability to work under such massive deployments remains unknown and thus calls for more research.

Chapter 5

Conclusion and Future Work

5.1 Summary and Conclusion

The study describes the context, design, and assessment of the newly proposed TRBCO algorithm aimed at responding to essential FANETs' problems in terms of dependability, security, and expansiveness. As stated, underlay networks such as FANETs have dynamic topologies and constrained resources, hence the need for reliable communication management. The implementation of trust and reputation measurements in the TRBCO algorithm provides the following solution for the above-mentioned challenges: a dynamic assessment of node activity and the best formation of clusters.

The achievement of the present study proves that the results anomalous to TRBCO are better than traditional clustering algorithms like LEACH and K-Means in terms of specified performance parameters. As a result of the selective focus on nodes with high trust scores, TRBCO delivers better APDR at the cost of slightly high E2ED, and an overall improvement in network throughput is obtained from the experiments. These improvements highlight the need to include trust and reputation in clustering in order to make FANETs more effective and efficient.

Another important strength of TRBCO is the ability to operate in a highly changeable network setting. The algorithm also has low control overhead; it can manage nodes with high mobility and ever-changing topologies by providing relatively stable clusters and low re-clustering frequency. This is quite important for real-world applications of FANET within sectors such as disaster response, surveillance, and smart agriculture, where network conditions are dynamic and fickle.

An equally important feature of this work is to focus on security. The key challenge for TRBCO is to select nodes with low trust scores as malicious or unreliable nodes and block their adverse actions. This proactive approach increases the network's locality against risks, for example, data corruption, packet dropping and denial of service attacks.

Nonetheless, the study has some limitations, calling for performance evaluation using simulations and with no detailed energy consumption. These shortcomings should be understood as certain prerequisites for the continuation of the work in testing the efficiency of this algorithm in practical conditions and improving its energy characteristics to adapt it for a long duration of UAV functioning.

Therefore, the design of the TRBCO explains a feasible algorithm for clustering FANET securely where issues of reliability, scalability, and adaptability are entrenched. The enhanced performance compared to conventional algorithms confirms its feasibility for practical use. Subsequent research in this area should aim at rectifying detected shortcomings, such as experimentation on a real-world setting, higher attack resistance, and power efficiency enhanced models for improving the applicability of trust based clustering mechanisms for FANETs. Thus, this research forms a base for the design of improved FANET solutions with the capability for efficient and dependable communication in complex conditions.

5.2 Recommendations for Future Research

For the purpose of advancing future studies, these limitations should be considered while the real-world applicability of the TRBCO algorithm should be further extended. One of the promising directions for further development of the study is the integration and experimentation of TRBCO in practical contexts. Challenges associated with effective test scenes include crowd density, farmland, and weather conditions that probe the algorithm's real-world applicability.

It is also a subject of future research to consider the endurance of TRBCO to advanced attack tactics. The algorithm could be further optimized to protect against intelligent threats such as collusion, Sybil attack or jamming. The integration of the procedures of anomaly detection and multi-dimensional trust models can improve its capacity to address such threats successfully.

Optimization of energy efficiency is also a formidable direction that requires additional research. Through specific examination of the energy parameters within various states of the network and the design of energy-aware algorithms for trust calculation and routing, the overall lifetime of UAVs can be prolonged. Moreover, integrating TRBCO with

readily-known, but in fact, heterogeneous UAV capabilities requires adaptation of the algorithm to cover the variations within real-world UAV deployments.

If TRBCO is to be used in large-scale networks, then it is necessary to conduct further experiments to validate the applicability of TRBCO to such a context. Both hierarchical clustering and decentralized trust evaluation could be combined in a way to provide scalability of large scale deployments without compromising on the resultant performance and accuracy.

Another research direction identified here is the integration of privacy-preserving approaches. Trust mechanisms are data-driven and, specifically, work based on node behavior data. Various risks originate from the fact that privacy concerns may be raised. One must look at tools such as encryption, AI federated learning, and zero-knowledge proof for the possibility of securing the trust evaluation while preserving the privacy of the data.

Multi-objective optimization can also enhance the adaptability of TRBCO by balancing competing objectives such as trust, energy efficiency, and network performance. This approach would allow the algorithm to adapt to different mission requirements, ensuring optimal operation in varying scenarios.

Finally, future research should explore cross-layer design integration. By incorporating trust-based mechanisms into the MAC, routing, and physical layers, the coordination between these layers can be improved, leading to enhanced overall network performance. Addressing these recommendations will strengthen the practical utility of trust-based clustering in FANETs, making it a robust solution for modern UAV applications.

References

[1] M. Ahmad, A. Salam, and I. Wahid, "A survey on Trust and Reputation-Based Clustering Algorithms in Mobile Ad-hoc Networks," *Journal of Information Communication Technologies and Robotic Applications*, pp. 59-72, 2018.

[2] K. Singh and A. K. Verma, "A fuzzy-based trust model for flying ad hoc networks (FANETs)," *International Journal of Communication Systems*, vol. 31, p. e3517, 2018.

[3] M. Y. Arafat and S. Moh, "A survey on cluster-based routing protocols for unmanned aerial vehicle networks," *IEEE Access*, vol. 7, pp. 498-516, 2019.

[4] A. Mehmood, J. L. Mauri, M. Noman, and H. Song, "Improvement of the wireless sensor network lifetime using LEACH with vice-cluster head," *Ad Hoc & Sensor Wireless Networks*, vol. 28, pp. 1-17, 2015.

[5] A. Bujari, C. T. Calafate, J.-C. Cano, P. Manzoni, C. E. Palazzi, and D. Ronzani, "Flying ad-hoc network application scenarios and mobility models," *International Journal of Distributed Sensor Networks*, vol. 13, p. 1550147717738192, 2017.

[6] Y.-H. Ho, Y.-R. Chen, and L.-J. Chen, "Krypto: assisting search and rescue operations using Wi-Fi signal with UAV," in *Proceedings of the First Workshop on Micro Aerial Vehicle Networks, Systems, and Applications for Civilian Use*, 2015, pp. 3-8.

[7] S. Waharte and N. Trigoni, "Supporting search and rescue operations with UAVs," in *2010 International Conference on Emerging Security Technologies*, 2010, pp. 142-147.

[8] J. Scherer, S. Yahyanejad, S. Hayat, E. Yanmaz, T. Andre, A. Khan, *et al.*, "An autonomous multi-UAV system for search and rescue," in *Proceedings of the First Workshop on Micro Aerial Vehicle Networks, Systems, and Applications for Civilian Use*, 2015, pp. 33-38.

[9] K. A. Ghamry and Y. Zhang, "Fault-tolerant cooperative control of multiple UAVs for forest fire detection and tracking mission," in *2016 3rd conference on control and fault-tolerant systems (SysTol)*, 2016, pp. 133-138.

[10] L. Merino, F. Caballero, J. R. Martínez-de Dios, J. Ferruz, and A. Ollero, "A cooperative perception system for multiple UAVs: Application to automatic detection of forest fires," *Journal of Field Robotics*, vol. 23, pp. 165-184, 2006.

[11] T. Samad, J. S. Bay, and D. Godbole, "Network-centric systems for military operations in urban terrain: The role of UAVs," *Proceedings of the IEEE*, vol. 95, pp. 92-107, 2007.

[12] P.-M. Olsson, J. Kvarnström, P. Doherty, O. Burdakov, and K. Holmberg, "Generating UAV communication networks for monitoring and surveillance," in *2010 11th*

International Conference on Control Automation Robotics & Vision, 2010, pp. 1070-1077.

[13] R. Reshma, T. Ramesh, and P. Sathishkumar, "Security situational aware intelligent road traffic monitoring using UAVs," in *2016 international conference on VLSI systems, architectures, technology and applications (VLSI-SATA)*, 2016, pp. 1-6.

[14] J. Torres-Sánchez, F. López-Granados, A. I. De Castro, and J. M. Peña-Barragán, "Configuration and specifications of an unmanned aerial vehicle (UAV) for early site specific weed management," *PloS one*, vol. 8, p. e58210, 2013.

[15] X. Li, Y. Zhao, J. Zhang, and Y. Dong, "A hybrid PSO algorithm based flight path optimization for multiple agricultural UAVs," in *2016 IEEE 28th international conference on tools with artificial intelligence (ICTAI)*, 2016, pp. 691-697.

[16] H. Chao, M. Baumann, A. Jensen, Y. Chen, Y. Cao, W. Ren, *et al.*, "Band-reconfigurable multi-UAV-based cooperative remote sensing for real-time water management and distributed irrigation control," *IFAC Proceedings Volumes*, vol. 41, pp. 11744-11749, 2008.

[17] O. Alvear, C. T. Calafate, E. Hernández, J.-C. Cano, and P. Manzoni, "Mobile pollution data sensing using UAVs," in *Proceedings of the 13th International Conference on Advances in Mobile Computing and Multimedia*, 2015, pp. 393-397.

[18] M. Erdelj and E. Natalizio, "UAV-assisted disaster management: Applications and open issues," in *2016 international conference on computing, networking and communications (ICNC)*, 2016, pp. 1-5.

[19] V. Kumar, D. Rus, and S. Singh, "Robot and sensor networks for first responders," *IEEE Pervasive computing*, vol. 3, pp. 24-33, 2004.

[20] P. J. Mosterman, D. E. Sanabria, E. Bilgin, K. Zhang, and J. Zander, "A heterogeneous fleet of vehicles for automated humanitarian missions," *Computing in Science & Engineering*, vol. 16, p. 90, 2014.

[21] B. Grocholsky, J. Keller, V. Kumar, and G. Pappas, "Cooperative air and ground surveillance," *IEEE Robotics & Automation Magazine*, vol. 13, pp. 16-25, 2006.

[22] S. A. H. Mohsan, M. A. Khan, F. Noor, I. Ullah, and M. H. Alsharif, "Towards the unmanned aerial vehicles (UAVs): A comprehensive review," *Drones*, vol. 6, p. 147, 2022.

[23] F. Pasandideh, T. D. E. Silva, A. A. S. d. Silva, and E. Pignaton de Freitas, "Topology management for flying ad hoc networks based on particle swarm optimization and software-defined networking," *Wireless Networks*, pp. 1-16, 2022.

[24] F. Pasandideh, J. P. J. da Costa, R. Kunst, N. Islam, W. Hardjawana, and E. Pignaton de Freitas, "A review of flying ad hoc networks: Key characteristics, applications, and wireless technologies," *Remote Sensing*, vol. 14, p. 4459, 2022.

[25] I. H. Beloev, "A review on current and emerging application possibilities for unmanned aerial vehicles," *Acta technologica agriculturae,* vol. 19, pp. 70-76, 2016.

[26] A. Rovira-Sugranes, A. Razi, F. Afghah, and J. Chakareski, "A review of AI-enabled routing protocols for UAV networks: Trends, challenges, and future outlook," *Ad Hoc Networks,* vol. 130, p. 102790, 2022.

[27] Z. Ullah, F. Al-Turjman, L. Mostarda, and R. Gagliardi, "Applications of artificial intelligence and machine learning in smart cities," *Computer Communications,* vol. 154, pp. 313-323, 2020.

[28] R. Udroiu, A. M. Deaconu, and C.-Ş. Nanau, "Data delivery in a disaster or quarantined area divided into triangles using DTN-based algorithms for unmanned aerial vehicles," *Sensors,* vol. 21, p. 3572, 2021.

[29] K. K. Nguyen, T. Q. Duong, T. Do-Duy, H. Claussen, and L. Hanzo, "3D UAV trajectory and data collection optimisation via deep reinforcement learning," *IEEE Transactions on Communications,* vol. 70, pp. 2358-2371, 2022.

[30] T. Alladi, V. Chamola, N. Sahu, and M. Guizani, "Applications of blockchain in unmanned aerial vehicles: A review," *Vehicular Communications,* vol. 23, p. 100249, 2020.

[31] M. Huang, A. Liu, N. N. Xiong, and J. Wu, "A UAV-assisted ubiquitous trust communication system in 5G and beyond networks," *IEEE Journal on Selected Areas in Communications,* vol. 39, pp. 3444-3458, 2021.

[32] F. Mohammed, I. Jawhar, N. Mohamed, and A. Idries, "Towards trusted and efficient UAV-based communication," in *2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS)*, 2016, pp. 388-393.

[33] R. Kumar, B. Sharma, and S. Athithan, "TBMR: trust based multi-hop routing for secure communication in flying ad-hoc networks," *Wireless Networks,* pp. 1-17, 2023.

[34] Y. Wang, Z. Su, T. H. Luan, R. Li, and K. Zhang, "Federated learning with fair incentives and robust aggregation for UAV-aided crowdsensing," *IEEE Transactions on Network Science and Engineering,* vol. 9, pp. 3179-3196, 2021.

[35] O. O. Olufemi and O. K. Oluwasesan, "An efficient authentication and key agreement scheme for security-aware unmanned aerial vehicles assisted data harvesting in Internet of Things," *Internet of Things,* vol. 23, p. 100862, 2023.

[36] Y. Pang and R. Liu, "Trust-Aware Emergency Response for A Resilient Human-Swarm Cooperative System," in *2021 IEEE International Symposium on Safety, Security, and Rescue Robotics (SSRR)*, 2021, pp. 15-20.

[37] E. A. Refaee and S. Shamsudheen, "Trust-and energy-aware cluster head selection in a UAV-based wireless sensor network using Fit-FCM," *The Journal of Supercomputing*, pp. 1-16, 2022.

[38] A. Shahraki, A. Taherkordi, Ø. Haugen, and F. Eliassen, "A survey and future directions on clustering: From WSNs to IoT and modern networking paradigms," *IEEE Transactions on Network and Service Management*, vol. 18, pp. 2242-2274, 2020.

[39] N. Mittal, U. Singh, R. Salgotra, and B. S. Sohi, "A boolean spider monkey optimization based energy efficient clustering approach for WSNs," *Wireless Networks*, vol. 24, pp. 2093-2109, 2018.

[40] S. S. Sefati, S. Halunga, and R. Z. Farkhady, "Cluster selection for load balancing in flying ad hoc networks using an optimal low-energy adaptive clustering hierarchy based on optimization approach," *Aircraft Engineering and Aerospace Technology*, vol. 94, pp. 1344-1356, 2022.

[41] G. Jayakumar and G. Gopinath, "Ad hoc mobile wireless networks routing protocols–a review," *Journal of Computer science*, vol. 3, pp. 574-582, 2007.

[42] M. Ayyub, A. Oracevic, R. Hussain, A. A. Khan, and Z. Zhang, "A comprehensive survey on clustering in vehicular networks: Current solutions and future challenges," *Ad Hoc Networks*, vol. 124, p. 102729, 2022.

[43] M. Fouladlou and A. Khademzadeh, "An energy efficient clustering algorithm for wireless sensor devices in internet of things," in *2017 Artificial Intelligence and Robotics (IRANOPEN)*, 2017, pp. 39-44.

[44] C. Gherbi, Z. Aliouat, and M. Benmohammed, "An adaptive clustering approach to dynamic load balancing and energy efficiency in wireless sensor networks," *Energy*, vol. 114, pp. 647-662, 2016.

[45] V. S. Devi and N. P. Hegde, "Multipath security aware routing protocol for MANET based on trust enhanced cluster mechanism for lossless multimedia data transfer," *Wireless Personal Communications*, vol. 100, pp. 923-940, 2018.

[46] A. B. McDonald and T. F. Znati, "A mobility-based framework for adaptive clustering in wireless ad hoc networks," *IEEE Journal on Selected Areas in communications*, vol. 17, pp. 1466-1487, 1999.

[47] J. Wang, Z. Yan, H. Wang, T. Li, and W. Pedrycz, "A survey on trust models in heterogeneous networks," *IEEE Communications Surveys & Tutorials*, 2022.

[48] R. Hussain, J. Lee, and S. Zeadally, "Trust in VANET: A survey of current solutions and future research opportunities," *IEEE transactions on intelligent transportation systems*, vol. 22, pp. 2553-2571, 2020.

[49] L. Abualigah, A. Diabat, P. Sumari, and A. H. Gandomi, "Applications, deployments, and integration of internet of drones (iod): a review," *IEEE Sensors Journal*, vol. 21, pp. 25532-25546, 2021.

[50] H. Wang, H. Zhao, J. Zhang, D. Ma, J. Li, and J. Wei, "Survey on unmanned aerial vehicle networks: A cyber physical system perspective," *IEEE Communications Surveys & Tutorials*, vol. 22, pp. 1027-1070, 2019.

[51] J. Zhou and Z. Wang, "Security Clustering Algorithm Based on Integrated Trust Value for Unmanned Aerial Vehicles Network," *KSII Transactions on Internet and Information Systems (TIIS)*, vol. 14, pp. 1773-1795, 2020.

[52] W. Osamy, A. M. Khedr, D. Vijayan, and A. Salim, "TACTIRSO: trust aware clustering technique based on improved rat swarm optimizer for WSN-enabled intelligent transportation system," *The Journal of Supercomputing*, vol. 79, pp. 5962-6016, 2023.

[53] I. Al Ridhawi, O. Bouachir, M. Aloqaily, and A. Boukerche, "Design guidelines for cooperative UAV-supported services and applications," *ACM Computing Surveys (CSUR)*, vol. 54, pp. 1-35, 2021.

[54] W. Fang, C. Zhang, Z. Shi, Q. Zhao, and L. Shan, "BTRES: Beta-based trust and reputation evaluation system for wireless sensor networks," *Journal of Network and Computer Applications*, vol. 59, pp. 88-94, 2016.

[55] Y. Ouyang, W. Liu, Q. Yang, X. Mao, and F. Li, "Trust based task offloading scheme in UAV-enhanced edge computing network," *Peer-to-Peer Networking and Applications*, vol. 14, pp. 3268-3290, 2021.