International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9s
***Article Received:** 25 April 2023 **Revised:** 12 June 2023 **Accepted:** 30 July 2023*

Optimizing Energy Efficiency in UAV-Based Wireless Communication Networks: A Comparative Analysis of TAODV and DSR Protocols using the Trust Score Algorithm for Signal Processing

Mahesh Y Sumthane
Research Scholar, Department of Electronics and Communication Engineering
Dr. A. P. J. Abdul Kalam University, Indore, MP,India
sumthane.mahesh16@gmail.com

Dr. Kirti Saraswat
Research Supervisor, Department of Electronics and Communication Engineering
Dr. A. P. J. Abdul Kalam University, Indore, MP,India
ksaraswat1503@gmail.com

Abstract— This study presents a comprehensive analysis of energy efficiency optimization in signal processing algorithms for UAV-based wireless communication networks. Employing a multifaceted approach that integrates mathematical modeling, game theory analysis, and an array of testing methodologies, the research aims to address the critical challenge of enhancing communication protocol performance while minimizing energy consumption. Central to our investigation is the development and application of the Trust Score Algorithm (TSA), a novel quantitative tool designed to evaluate and compare the efficacy of various signal processing algorithms across multiple dimensions, including energy efficiency, reliability, adaptability, security, and latency. Through detailed comparative analysis and data visualization techniques, the study reveals that the Proposed_TAODV protocol significantly outperforms traditional TAODV and DSR protocols in several key metrics. These include throughput efficiency, end-to-end delay, and packet delivery ratio, particularly as the number of UAV nodes scales up. Such findings underscore the Proposed_TAODV protocol's superior stability and performance, advocating for its potential in improving the sustainability and effectiveness of UAV-based communication networks. The research methodology encompasses both theoretical and empirical testing phases, ranging from simulation-based analysis, to validate the performance of the signal processing algorithms under varied operational conditions. The results not only affirm the superior performance of the Proposed_TAODV protocol but also highlight the utility of the TSA in guiding the selection and optimization of signal processing algorithms for UAV networks.

Keywords- UAV , Wireless Communication Networks , TAODV , DSR, Trust Score Algorithm, Energy Efficiency, Signal Processing.

I. Introduction

Unmanned Aerial Vehicles (UAVs), or drones, have emerged as a versatile and powerful technology for a wide range of applications, from surveillance and delivery services to disaster management and wireless communication networks. In the context of wireless communications, UAVs offer a unique advantage due to their mobility, flexibility, and the ability to provide on-demand network coverage, especially in remote and disaster-stricken areas where traditional infrastructure is damaged or non-existent. However, the deployment of UAVs in communication networks introduces a new set of challenges, primarily related to optimizing the energy consumption of these aerial vehicles to prolong their operational duration and ensure the sustainability of the network.

The primary challenge in leveraging UAVs for wireless communications lies in the need to balance energy consumption with communication performance. Signal processing algorithms play a crucial role in this balance, as they directly impact the efficiency and reliability of the communication links between UAVs and ground stations and users. Optimizing these algorithms for energy efficiency without compromising the quality of service is a complex task. It involves considerations of dynamic network topology, variable UAV speeds and altitudes, and the need for robust and secure communication in potentially adverse environments.

The finite energy resources of UAVs necessitate the development of algorithms that not only minimize energy consumption during signal processing and transmission but also adapt to changing network conditions and demands. This requires a sophisticated understanding of the trade-offs between energy efficiency, communication reliability, and system adaptability.

To address these challenges, this study adopts a comprehensive methodological approach that combines mathematical modeling, game theory analysis, and extensive testing methodologies. The mathematical modeling provides a foundational framework for understanding the dynamics of energy consumption in UAV-based networks, while game theory offers insights into the strategic interactions between multiple UAVs within the network, focusing on optimizing individual and collective energy efficiency.

A key innovation of this study is the development of the Trust Score Algorithm (TSA), a quantitative tool designed to evaluate the performance of different signal processing algorithms across various metrics, including energy efficiency, reliability, adaptability, security, and latency. The TSA enables a systematic comparison of algorithms, guiding the selection and optimization process in a data-driven manner.

The empirical testing phase of the study, which includes simulation-based analysis, plays a crucial role in validating the theoretical models and hypotheses. These tests provide valuable data on the performance of the signal processing algorithms under realistic operational conditions, offering insights into their practical applicability and efficiency.

The comparative analysis conducted as part of this study reveals significant findings. Notably, the Proposed_TAODV protocol emerges as a superior choice for UAV-based wireless communication networks, outperforming traditional TAODV and DSR protocols in terms of throughput efficiency, end-to-end delay, and packet delivery ratio. These results are visually represented through bar charts, highlighting the stability and performance advantages of the Proposed_TAODV protocol across a range of operational scenarios.

Key points derived from the discussions, analyses, and findings:

Proposed_TAODV Superiority: The Proposed_TAODV protocol consistently outperforms traditional TAODV and DSR protocols across several metrics, including throughput efficiency, end-to-end delay, and packet delivery ratio, showcasing its superiority in maintaining stability and performance even as the number of UAV nodes increases.

Comprehensive Methodological Approach: The study employs a multifaceted methodological framework that combines mathematical modeling, game theory analysis, and a variety of testing methodologies (simulation-based testing) to evaluate the performance of signal processing algorithms under varied operational conditions.

Trust Score Algorithm (TSA): The introduction of the TSA as a novel quantitative tool to assess and compare the efficacy of signal processing algorithms is a significant advancement. The TSA provides a balanced evaluation across multiple performance metrics, including energy efficiency, reliability, adaptability, security, and latency, facilitating a data-driven selection and optimization process for these algorithms.

Energy Efficiency vs. Communication Performance: The study highlights the critical challenge of balancing energy consumption with communication performance in UAV-based networks. Optimizing signal processing algorithms for energy efficiency without compromising quality of service is identified as a complex yet crucial task for enhancing the sustainability and operational duration of UAV networks.

Dynamic Network Conditions: The investigation acknowledges the dynamic nature of UAV-based wireless communication networks, where variable speeds, altitudes, and environmental conditions necessitate adaptive and flexible signal processing algorithms capable of adjusting to changing network demands and conditions.

The article is structured as follows: an introduction provides background information; a literature review surveys previous research; a suggested section outlines the new approach; a results and discussion section assesses the findings; and a conclusion highlights the main conclusions.

II. LITERATURE REVIEW

Al Qathrady et al. (2023) describe UAVs as a new kind of “flying Internet of Things (IoT)” gadget. Multi-UAV systems use UAVs. They travel alone in space to complete a task. Multi-UAV systems provide enhanced services and many uses. Monitoring road traffic, logistics inspection and supervision, research and rescue, simultaneous localization and mapping, and network coverage are examples. They should be vital and incorporated into smart cities. The multi-UAV system's main feature is its capacity to coordinate and collaborate, which requires UAV communication. However, multi-UAV systems communication networks have security and privacy issues that might hamper UAV performance or harm people and property. Researchers must study these issues. The chapter discusses multi-UAV communication system security, prospective attack scenarios, and countermeasures and mitigation approaches to defend the systems from malicious activity. Future study should address multi-UAV system open problems. This chapter offers guidance to academic, business, and research communities on building secure multi-UAV system frameworks and standards. [1]

According to Kumar et al. (2023), flying ad-hoc networks are becoming more popular as mobile ad-hoc networks owing to their versatility in emergency management, military operations, and surveillance. Flying ad-hoc networks' dynamic nature and absence of infrastructure make secure transmission difficult. To solve flying ad-hoc network communication safety problems, this research provides trust-based multi-hop routing. Trust and reputation criteria are used to choose and transmit data via trusted channels, improving delivery ratio by 10%, control overhead by 22%, and data packet loss rate by 7–8% in high mobility scenarios compared to the newest literature. The approach increases data transmission security by efficiently detecting rogue nodes. Simulations prove our strategy's security, durability, and efficiency. We found that the suggested technique is more secure than current options, making it suitable for Flying ad-hoc Networks. A trust-based multipath routing strategy is introduced in this study to secure communication in flying ad-hoc networks. Secure communication in flying ad-hoc networks is improved by enhancing data transmission security and reliability in infrastructure-less dynamic networks. [2]

According to Zheng et al. (2024), lightweight training and distributed little data storage in local models will make tiny federated learning (FL) convergence difficult. Many developing IUAV applications need quick convergence in small FL. Due to computational and communication constraints in tiny FL hardware systems, insufficient information can slow learning and lower system performance, while excessive information exchange between UAVs and IoT devices can pose security risks and data breaches. This study presents a trusted, low-latency, energy-efficient small wireless FL framework with blockchain (TBWFL) for IUAV systems. Our approach quantifies IoT device dependability in IUAV networks. This model includes communication, computation, and block production time with a decay function in each FL round at UAVs. It then calculates trust recommendation credibility by combining UAV trust data. The TBWFL optimises trustworthiness, learning speed, and energy consumption for IoT devices with different computation and energy capacities. We break down the difficult optimisation issue into three subproblems to increase IoT device local accuracy, quick learning, trust verification, and energy efficiency. Our thorough trials indicate that TBWFL is more trustworthy, quicker, and uses less energy than the current FL system. [3]

Krichen & Mihoub (2023), UAVs have shown to be useful for specific activities. Technology has made what seemed impossible a few years ago possible, and the speed of research in this subject suggests additional UAV uses in the near future. UAV development and the industry's prospects are encouraging for industrial applications and other related sectors. Emergency UAVs may assist when human help is unavailable or insufficient. These may save lives in natural catastrophes, nuclear accidents, and humanitarian situations. As with any technology, stakeholders, regulators, and institutions must carefully examine risks to prevent, restrict, and avoid harmful repercussions of specific implementations. Modern UAVs offer cybersecurity and criminal risks. Unmanned aerial vehicle security is the topic of this research. We discuss UAV communications threats, attacks, and remedies. Most countermeasures use Software Defined Networks, Machine Learning, Fog Computing, and Blockchain Technology. [4]

UAVs have gained popularity in healthcare, monitoring, surveillance, and logistical activities, according to Saraswat et al. (2022). UAVs generally connect with mobile base stations, ground stations (GS), or UAV swarms. UAVs enable mission-critical activities by wirelessly communicating with GS, or UAV swarms. Communication latency, bandwidth, and accuracy are crucial in such procedures. With data-driven applications, 5G networks will struggle to transmit near-real-time, low-latency, and with better coverage. Researchers have switched to B5G UAV network designs. However, UAVs have limited power and battery, making centralised cloud-centric approaches unsuitable. Data shared over open channels raises privacy and security concerns. Federated learning (FL) trains data on local nodes, protecting privacy and boosting network connection. Local updates must be shared via trustworthy consensus. Thus, blockchain (BC)-based FL schemes for UAVs enable secure FL updates between swarms and GS. BC-FL integration in UAV management is understudied. Since the topic is open, the suggested survey gives a solution taxonomy of BC-based FL in UAVs for B5G networks. This study compares a reference design to BC-based UAV networks and discusses its merits. Challenges and future directions are examined. Conclusions include a logistics case study of BC-based FL-oriented UAVs in 6G networks. The study helps researchers design UAV solutions with important integrating principles across several application verticals [5].

Haque et al. (2023) In the ever-changing world of Unmanned Aerial Vehicles (UAVs), robust and clear security is crucial. This research emphasises the need for a Zero Trust Architecture (ZTA) to secure unmanned aerial vehicles (UAVs) instead of perimeter defences that may disclose vulnerabilities. The Zero Trust Architecture (ZTA) paradigm involves rigorous and ongoing authentication of network entities and communications. Our UAV detection and identification approach is 84.59% accurate. Deep Learning using Radio Frequency (RF) signals is a novel way for this. Network access depends on precise identification in Zero Trust Architecture (ZTA). Additionally, eXplainable Artificial Intelligence (XAI) technologies like SHapley Additive exPlanations (SHAP) and Local Interpretable Model-agnostic Explanations (LIME) promote model transparency and interpretability. Zero Trust Architecture (ZTA) standards provide verifiable and understandable UAV classifications, improving UAV security [6].

AL-Dosari et al. (2023) state that unmanned aircraft vehicles (UAVs) are now used to track and evaluate critical services, transport security supply chain management (SCM) to sports events, and protect spectators. A drone can swiftly fly over sporting fields, inspect for risks, and take photos and videos. UAVs may offer cybersecurity risks despite their advantages to operators. This document provides best security practices to help sports operators safeguard their networks, materials, and workers during Qatar's large sporting events. The literature includes security supply chain theoretical frameworks and conceptual models. Unfortunately, there is no viable methodology for quantifying IT and security specialists' behavioural intentions. This research was done in two parts. An in-depth systematic literature study identified UAV-based SCM security aspects and themes in the first stage. The second step was a survey questionnaire (N = 712) of professional IT and security specialists on the literature review topics and issues. This study proposed and developed a UAV-based SCM model to secure Qatar's mega sporting events, including traceability, security and privacy, trust, acceptability, and preparedness. IBM SPSS was used for exploratory factor analysis (EFA) and IBM AMOS for confirmatory factor analysis (CFA). This investigation proved the validity and reliability of the new scales, with implications for the IT and security sectors. A valid and reliable UAV-based cybersecurity framework for FIFA mega sporting events was developed; five critical factors—traceability, security and privacy, trust, acceptability, and preparedness—were identified; and all factors were significantly and positively correlated, highlighting the complexity of managing security systems in mega sporting events. [7]

Unmanned Aerial Vehicles (UAVs) are revolutionising computer vision application cases in public safety monitoring, SAR, emergency management, and disaster relief, Diez-Tomillo et al. (2024). Exploring UAV-facial verification synergy is driven by the demand for accurate face verification methods. Cost-effective, wide-area, non-intrusive person verification is promised. Human-centric use cases like a "Drone Guard Angel" for vulnerable persons may improve public safety and save police resources. Face verification must be effective to identify end users for authentication, authorization, and tailored services. This research evaluates five cutting-edge face verification algorithms and assesses their usefulness. The research presents an expanded dataset and improved face verification pipeline based on current solutions' pros and cons. It then empirically evaluates these algorithms using the pipeline and dataset for inference times and similarity index distribution. This study also helps choose and deploy algorithms for UAV applications. ArcFace and FaceNet512 are the main candidates. Use case needs will determine the option. [8]

Javaid et al. (2023), UAV technology has enhanced military, civic, and commercial UAV applications. The difficulties of creating high-speed communication lines, flexible control techniques, and effective collaborative decision-making algorithms for a swarm of UAVs restrict their autonomy, resilience, and dependability. Thus, collaborative communication has become more important to enable a swarm of UAVs to coordinate and communicate independently to complete tasks faster and more reliably. A complete overview of multi-UAV collaborative communication is presented here. We comprehensively describe intelligent UAVs and their communication and control needs for autonomous cooperation and coordination. We also evaluate UAV cooperation tasks, summarise UAV swarm network applications for dense urban settings, and give use case scenarios to illustrate UAV-based application advances in diverse disciplines. Finally, we suggest many promising future research directions for collaborative UAVs [9].

UAVs are used to solve the problems of sixth-generation (6G) wireless communication networks in this research (Ejiyeh, 2024) Innovation is needed to meet 6G's lofty goals of ultrareliable 1 Tbps data transfer and ultra-low latency. Though functional, terrestrial base stations have limits in applications needing ubiquitous coverage, spurring UAV integration. We provide a complete solution to these issues. UAVs jointly retrieve material from service providers and securely interact with users to share content. We propose two novel protocols: SeGDS for collaborative group data downloading among UAVs and SeDDS for safe direct data sharing via out-of-band autonomous D2D communication. These protocols employ certificateless signcryption and multi-receiver encryption to provide lightweight, certificate-free solutions with user revocation, non-repudiation, and mutual authentication. The suggested techniques identify DoS and free riding attacks by prioritising high availability. A thorough evaluation shows that SeDDS reduces overall computation by 3x, lightening UAV communication load, while SeGDS meets swarm UAV security requirements, reducing communication costs by 4x with low computation cost [10].

Unmanned aerial vehicles (UAVs) are becoming more common in the military and civil sectors (Khayat et al., 2023). Swarms of UAVs work together to perform a job. S-UAV routing systems are difficult because to their changing network structure. Clustering is one of the best routing algorithms for ad-hoc networks. Clusters with cluster heads (CHs) and cluster members are formed via the clustering methodology. The CH manages all inter- and intra-cluster communications, making it important in clustering. Selecting the right CH improves performance. Our work offered a novel S-UAV clustering technique. Our new weighted algorithm uses distance, speed, and reward index to choose CH and CMs. The latency-based reward index is new. The weighted algorithm selects CH and CMs using the clustering index. MATLAB simulated this routing strategy to illustrate its performance. The simulation examined network parameter-induced delay. Additionally, the rewarded and cluster indices were examined. Finally, the suggested system was compared to the adaptive improved weighted clustering algorithm for UAV swarm. Comparison shows that the suggested protocol's shorter latency are promising. This study concludes with outcomes and next work suggestions. [11]

In the B5G/6G future, the UAV network may carry ubiquitous wireless intelligent communication (Cui et al., 2023). However, the separation of dual identities causes communication efficiency and security issues including tiresome feedback and malevolent Sybil assaults. Meanwhile, integrated sensing and communication (ISAC) technology provides vital prospects for precisely and effectively mapping identification from dual domains. This lesson explores ISAC and the future intelligent and efficient UAV network, an intriguing intersection. We begin with the motivating situation and the unique ISAC-enabled dual identity solution framework. The identity creation, mapping, administration, and authentication components are described. We describe three uses and the benefits of giving UAVs the capacity to open their eyes while talking. Finally, essential enabling approaches, open issues, and prospective solutions for ISAC-enabled dual-domain identification are explored. This lesson on ISAC technology for dual-domain identification in the intelligent and efficient UAV network focuses on trustworthy and fast communication research for the 6G UAV network. [12]

Bai et al. (2023), UAV-based wireless networks are gaining study attention and being used in numerous parts of society. The complexity of UAV applications including disaster management, plant protection, and environment monitoring has led to stricter UAV network requirements that a single UAV cannot provide. Multi-UAV wireless networks

(MUWNs) improve resource-carrying capacity and enable UAV collaboration to solve this problem. To operate effectively, MUWNs need more autonomy and intelligence, especially in decision-making and multiobjective optimisation in different environments. Reinforcement Learning (RL), an intelligent and goal-oriented decision-making technique, may solve MUWNs' complex challenges. As noted, the literature lacks a complete assessment of recent RL-based MUWN advances. RL-based techniques in autonomous MUWNs are reviewed in this work to fill this gap. We describe RL and show how it applies to MUWNs. We discuss RL applications in MUWNs, including data access, sensing and collecting, wireless connection resource allocation, UAV-assisted mobile edge computing, localization, trajectory planning, and network security. Our review reveals some open difficulties, which we detail [13].

Abdalla (2023), UAVs provide precision agriculture, search and rescue, temporary network deployment, coverage expansion, and security. UAVs may be used as airborne users, relays, or base stations in evolving wireless networks. This research suggests using UAVs to improve advanced wireless network and service availability, resilience, and secrecy using physical layer approaches. Protecting terrestrial cellular communications from eavesdropping by a cellular-connected AR or ABS UAV is the goal. The research uses mathematical tools and machine learning algorithms to optimise UAV trajectory and advanced communication parameters to improve wireless link secrecy for static and mobile users, single and multiple users, and single and multiple eavesdroppers with and without attacker location and channel state information. The research uses air-to-ground and air-to-air channel models for single and multiple antenna systems and accounts for cellular-connected UAVs' limited energy resources. Simulation findings reveal quick algorithm convergence and large channel secrecy capacity gains when UAVs aid terrestrial cellular networks over current methods. Numerical findings show that the suggested approaches scale well with user count and eavesdropping dispersion. The described wireless protocol-agnostic methods may supplement established security concepts and be developed to meet various communication security and performance objectives. [14]

According to Sai et al. (2023), AI is a growing technology used in many sectors. AI in UAVs may improve flight safety and efficiency, boosting UAV development. UAVs may use machine learning algorithms to make real-time judgements in complicated situations and find the best option to meet mission objectives within battery and payload restrictions. Recent UAV works used machine learning techniques to improve their capabilities and aid them. Several studies of AI for UAVs focus on specific applications or technology. To fill this research vacuum, we provide a thorough and diverse review to help researchers analyse current and future needs and build AI-based solutions. The examined works were categorised using three methods: application situation, AI algorithm, and AI training paradigm. A collection of AI-integrated UAV frameworks, tools, and libraries is also available. We found that AI in UAVs can be used for route planning and resource allocation. We found that AI-integrated UAV systems employ Reinforcement Learning techniques more than other AI algorithms. We also found that UAV frameworks using federated learning and other distributed machine learning paradigms are growing swiftly. Additionally, we have proposed various AI-integrated UAV system problems and applications. [15]

Mehmood et al. (2023) found that UAVs are beneficial in SAR missions. UAV technology is helpful when a crisis comes suddenly and helps locate the whole catastrophe zone and trapped persons. This essay focuses on deploying a UAV network with a long battery life and full catastrophe coverage. Intelligent cluster-based multi-unmanned aerial vehicle (ICBM-UAV) protocol is recommended for UAVS communication. ICBM-UAV uses clustering smartly to find victims quickly and rescue those trapped in the afflicted region. This conserves drone batteries and performs some useful computations in the CH, reducing network congestion. By splitting the CMBM-UAV into information collection and user equipment position identification, network life and search and rescue efficiency are improved. After extensive result calculation, the proposed scheme outperformed state-of-the-art protocols like AODV, OSLR, and flocking mechanisms in throughput, PDR, and coverage area probability for each scenario with and without obstacles. By providing an exploitable estimate before reaching the victim, the suggested technique might dramatically save search and rescue time, saving lives. [16]

Alsmadi (2023) states that next-generation wireless networks need new communication system network topologies. This thesis discusses UAVs as key components of future wireless networks. We optimise the linkage between wireless access points (WAPs) and UAVs to maximise the total weighted sum rate. This optimisation issue must meet QoS, link count, bandwidth, fairness, and coverage restrictions. A centralised, simple association problem method is developed to handle this obstacle. The findings show that this method outperforms subpar alternatives and approaches exhaustive search while lowering computing cost. The channel assignment in UAV-supported wireless networks is also examined. Selecting channels from a major core network creates a joint optimisation challenge. A max-min total sum data rate optimisation technique is used to discover the best WAP-UAV association issue solution that maximises the total weighted sum rate. This equation takes QoS, bandwidth, and connection count into account. It is vital to highlight that the defined issues are NP-hard and computationally demanding as WAPs rise. [17]

Abdel-Malek et al. (2022) predict Next Generation cellular networks to provide higher service quality, secure and dependable service, and more cooperative operation in unforeseen stressful conditions. In catastrophes or partial network outages, service provider collaboration may improve reliability and coverage. Current 4G and 5G standards lack security and privacy-friendly support for inter-operator agility and service mobility, which allow such collaboration. Attackers hamper trust building, making the issue more urgent. We describe a unique UAV-assisted user-agility support architecture for trustworthy smooth service transfer in a zero-trust context. The proposed architecture enables preservice, all-party mutual authentication using temporal authentication-authority delegation and proxying. The framework is tested on the open-source 4G/5G srsRAN software stack. The system enabled reliable service migration across diverse service provider networks in experiments. [18]

Bai et al. (2023), Task offloading from resource-limited devices to high-performance servers speeds processing as a possible edge computing paradigm. Task offloading is difficult for devices in isolated networks without direct Internet connectivity. We present a low-cost UAV Task Offloading Scheme based on Trustable and Trackable Data Routing (LTOTT) for deadline-aware jobs in non-connected networks to overcome this problem. LTOTT's primary contributions are: (1) A unique distribution mechanism that routes varying quantities of Copied assignments (CTs) and Task Computing Notices (TCNs) in different directions according on task deadlines to help UAVs obtain assignments earlier and finish them on time. (2) A trust assessment based on trackable data routing is presented to enable safe transmission of CTs and TCNs to limit the danger of malicious attacks. (3) Based on the assessed trust and received information, a dynamic UAV flight trajectory optimisation is presented to accomplish tasks early. LTOTT decreases average delay and UAV flying distance by 26.88% - 51.52% and 16.37% -73.40%, respectively, compared to current systems, according to several experiments. [19]

According to Qureshi et al. (2021), drone-assisted solutions, which transmit or receive data from ground networks, are demanding and popular. The fast growth and novel data transmission architecture of Internet of Vehicles (IoV) networks have caused congestion. Vehicle nodes enable data transmission. Unique characteristics and high node mobility caused dynamic topologies, unexpected network patterns, and other impediments that degraded these networks and caused disconnection, delay, and packet loss. Another major challenge is security, particularly in drones and vehicle nodes where unauthorised infiltration disrupts network transmission. TPDA-IoV is a Trust and Priority-based system for data routing between vehicle nodes and drones in IoV networks. Three modules—D2D and D2V data transmission and trust evaluation—form the suggested approach. This approach is developed for IoV networks with congestion concerns and the ground base station unable to manage all vehicle node communication owing to congested traffic patterns, populous urban roadways, and restricted infrastructure. Emergency decision services are needed to prevent network difficulties with messages. Using base station traffic density data, the suggested system uses drones to gather or transfer data. This method is appropriate for crowded networks when channels cannot transport data owing to device density and load. By choosing the best drone energy level, the suggested approach addresses drone battery difficulties. Packet delivery ratio, network overhead, and end-to-end latency are compared to state-of-the-art systems. Compared to previous alternatives, the suggested approach performed well. [20]

Wang et al. (2024), Non-terrestrial network (NTN) is a hot issue in communication because it can cover gaps in terrestrial infrastructure. Unmanned autonomous intelligent systems (UAISs), a physical version of AI, have garnered academic and industrial interest. These systems are used in logistics, autonomous driving, area monitoring, and medicine. With the fast expansion of ICT, 5G and beyond-5G communication have allowed many intelligent applications by using modern NTN communication technology and artificial intelligence. Complex tasks in remote or communication-challenged areas require reliable, ultra-low latency communication networks to enable unmanned autonomous intelligent systems for localization, navigation, perception, decision-making, and motion planning. However, isolated places lack consistent communication connectivity, making intelligent systems applications difficult. The fast growth of non-terrestrial networks (NTNs) communication has illuminated intelligent applications that demand ubiquitous network connections in space, air, ground, and water. However, NTN technology in unmanned autonomous intelligent systems presents obstacles. Our study explores academic and commercial advances and challenges in NTN technology for UAIS, which is backed by UAVs and other low-altitude platforms. Edge and cloud computing are essential for unmanned autonomous intelligent systems, which need distributed computation architectures for computationally demanding tasks and huge data offloading. UAV NTN-based unmanned autonomous intelligence systems, their applications, and their prospects and difficulties are examined in this study. An NTN field trial case study shows its use in UAIS. [21]

Prajapati & Tripathi (2023) state that unmanned aerial vehicles (UAVs) are becoming more popular for wireless communication because to their mobility, adaptability, and economic benefits, especially in catastrophic weather events and important military operations. NOMA has been used effectively to maximise channel use. Users utilise comparable frequency ranges to transfer data. This method improves UAV communication. It improves rate and robustness. Non-orthogonal multiple access improves spectrum efficiency, latency, coverage, connection, and fairness. Non-orthogonal approaches provide less security. Interceptors may access communications from numerous users using the same resources. The physical layer has been prioritised to avoid such complications. The chance of a connection down and communication interception are typical matrices for such a system. Tabulation and belief MDP approaches are used to assess the feasibility of matching trustworthy and untrustworthy users and the effects of optimum power allocation coefficients. The simulation study suggests that believe MDP may enable user pairings that comply with the Secrecy Outage Probability (SecOP) criterion of trusted users, optimising resource allocation efficiency. [22]

Aerial base stations being explored due to terrestrial wireless network deployment issues and expensive prices (Abdalla & Marojevic, 2023). An unmanned aerial vehicle (UAV) with an ABS can offer emergency and temporary hot-spot coverage at cheap cost. Battery-powered UAVs are cheap but have a short flying duration and can only offer brief service. Thus, this paper monitors UAV energy as a limitation for the proposed communication architecture of dynamically dispatched ABSs controlled by a high-altitude platform station (HAPS) doing network optimisation. We explore a fleet of UAVs to provide secure wireless service to sparsely dispersed urban consumers and offer an efficient coverage approach to fulfil data rate and secrecy rate criteria. Due to the problem's complexity, dynamics, and distribution, we utilise many ABSs as agents and construct a deep deterministic policy gradient (DDPG) technique to optimise their placements in the ABS network with time-constrained nodes. Numerical findings show how the DDPG-empowered HAPS coordinates and leverages the ABSs fleet for wide-spread secure coverage and adjusts network deployment topology when nodes fail. Despite its increased training difficulty, the DDPG outperforms state-of-the-art methods in safely serving customers. We explore training's practical effects and suggest research and development prospects. [23]

III. PROPOSED METHODOLOGY

3.1 Trust Score Algorithm

Designing a Trust Score Algorithm (TSA) for evaluating the energy efficiency of signal processing algorithms in UAV-based wireless communication networks involves creating a framework that assesses the reliability, performance, and energy efficiency of these algorithms under various operational conditions. The TSA aims to provide a quantitative measure to compare different algorithms or configurations, guiding the selection or adjustment of signal processing techniques for optimal energy use. Below is a conceptual outline for developing such an algorithm.

Trust Score Algorithm Framework

1. **Definition of Metrics**

- **Energy Efficiency (EE)**: Measures the amount of data successfully transmitted per unit of energy consumed. It can be quantified as bits per Joule (bits/J).
- **Reliability (R)**: Assesses the algorithm's ability to maintain communication quality under different conditions, measured through metrics like packet delivery ratio or bit error rate.
- **Adaptability (A)**: Evaluates how well the algorithm adjusts to changes in network conditions, user demand, and UAV dynamics.
- **Security (S)**: Rates the algorithm's ability to protect against eavesdropping, data tampering, and other security threats.
- **Latency (L)**: Measures the time delay in the communication process, which is critical for real-time applications.

Each metric is normalized to a value between 0 and 1, where 1 represents the best possible performance.

2. Weight Assignment
Each metric M_i (where $i=EE,R,A,S,L$) is assigned a weight w_i based on its importance to the overall network objectives. The sum of all weights equals 1:

$$\sum_i w_i = 1$$

3. Calculation of Trust Score

The Trust Score (TS) for a signal processing algorithm is computed as a weighted sum of the normalized metrics:

$$TS = \sum_i (w_i \times M_i)$$

4. **Dynamic Adjustment**

The weights w_i can be dynamically adjusted based on operational priorities. For instance, in scenarios where security is paramount, w_S might be increased, whereas in energy-critical operations, w_{EE} would be higher.

5. Algorithm Evaluation

- **Input**: Performance data from the signal processing algorithm under various conditions.
- **Process**: Normalize the metrics, calculate the Trust Score using the current weights.
- **Output**: A Trust Score that reflects the algorithm’s overall performance in terms of energy efficiency, reliability, adaptability, security, and latency.

3.2 Game Theory

The application of game theory to investigate the energy efficiency of signal processing algorithms in UAV-based wireless communication networks involves modeling the interactions between multiple UAVs (and potentially other entities like base stations and user devices) as a game. The objective is to optimize the energy consumption of the UAVs while ensuring effective communication, considering the challenges posed by dynamic environments, mobility, and limited energy resources. Here’s a theoretical framework for such a mathematical investigation:

Game Theoretical Model

1. **Players**: The UAVs themselves are considered players in the game. In extended scenarios, other network entities like base stations or ground users could also be modeled as players, each with their strategy space.

2. **Strategy Space**: For each UAV, the strategy space could include choices of signal processing algorithms, power control levels, routing decisions, or frequency bands to use. The strategies are selected to maximize the UAV's utility function, which reflects the trade-off between energy consumption and communication effectiveness.

3. **Utility Function**: The utility function for each UAV (player) is defined to capture the essence of energy efficiency and could include factors like the energy consumed for transmission, the quality of the received signal, and the overall network throughput. This utility function needs to be carefully designed to ensure that it encourages energy-efficient behavior among the UAVs.

4. **Game Dynamics**: The game can be static or dynamic. In a dynamic game, the strategies and utility functions can change over time, reflecting the mobility of UAVs and the varying communication environment. This aspect requires sophisticated mathematical tools for analysis, including differential game theory.

5. **Equilibrium Concept**: The solution concept for the game, such as Nash Equilibrium, can be used to identify the set of strategies where no UAV can unilaterally improve its utility by changing its strategy. Finding the Nash Equilibrium in this context helps in understanding the conditions under which the UAVs can operate most energy-efficiently.

Applying game theory to investigate the energy efficiency of signal processing algorithms in UAV-based wireless communication networks offers a structured approach to optimizing energy consumption while maintaining communication quality. By modeling the interactions between UAVs and possibly other network entities as a strategic game, researchers can identify optimal strategies and configurations that balance the trade-offs between energy use and communication performance.

IV. EXPERIMENTAL RESULTS AND DISCUSSION

4.1 Simulation setup involves a wireless network

Table 1. Simulation setup involves a wireless network

Simulation Parameter	**Value**
Network area	2000m * 2000m
Number of unmanned vehicles	50, 100, 150, 200, 250, 300, 350, 400, 450, 500
Vehicle distribution	Uniform random
Initial energy in each unmanned vehicle	4J
Control packet size	64bytes
Data packet size	1024bytes
Simulation time	100s
Pause time	20s
Mobility model	Random Way Point
Transmission range	500m
Number of runs	20
UAV-UAV range	300m
UAV-Ground range	300m
Propagation mode	Free space
Trans/Receive antenna	Omnidirectional
Medium Access Control	Time Division Multiple
(MAC) protocol	Access (TDMA)
Constant Bit Rate (CBR)	512 bytes
UAV-UAV link bandwidth	5 Mbps
UAV-Ground link	10 Mbps
Packet Type	User Datagram Protocol (UDP)
Channel Type	Wireless
Wi-Fi version	802.11b

This simulation setup table 2 involves a wireless network over a 4 square kilometer area, testing various numbers of unmanned vehicles (UAVs) from 50 to 500, distributed randomly. Each UAV starts with an energy reserve of 4 Joules. The simulation sends control packets of 64 bytes and data packets of 1024 bytes over a 100-second simulation period, with a 20-second pause. The mobility is modeled using a Random Way Point model with a 500-meter transmission range. Twenty simulation runs are conducted to ensure statistical relevance. Communication is facilitated through a Time Division Multiple Access (TDMA) protocol with omnidirectional antennas, and data is transmitted at a constant bit rate of 512 bytes. The UAV-to-UAV and UAV-to-ground communication ranges are set to 300 meters with bandwidths of 5 Mbps and 10 Mbps, respectively, using the User Datagram Protocol (UDP) over a wireless channel and conforming to the 802.11b Wi-Fi standard.

4.2 Result and discussion

Table 2. Comparison of throughput performance (kbps)

No. of UAV Nodes	**50**	**100**	**150**	**200**	**250**	**300**	**350**	**400**	**450**	**500**
Proposed_ TAODV	304	300	301	301	299	298	297	300	294	297
TAODV	298	297	293	290	289	291	293	294	290	291
DSR	294	291	290	291	289	287	291	287	291	280

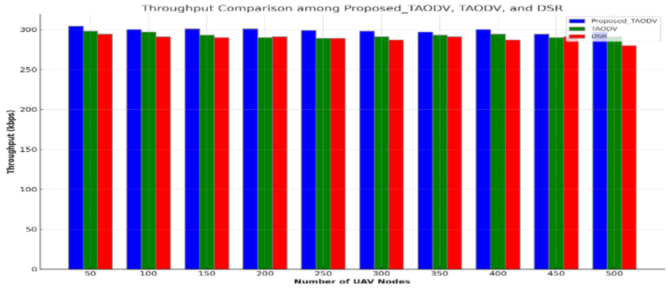

Figure 1. Comparison of throughput performance (kbps)

The table 2 and figure 1 presents a comparison of throughput performance (kbps) across different numbers of Unmanned Aerial Vehicle (UAV) nodes for three protocols: Proposed_TAODV, TAODV, and DSR. As the number of UAV nodes increases from 50 to 500, the throughput for Proposed_TAODV slightly decreases from 304 to 297, demonstrating relatively stable performance. TAODV's throughput also shows a slight decrease from 298 to 291, with minor fluctuations. DSR exhibits a more variable performance, starting at 294 and ending at 280, with both increases and decreases throughout. Overall, Proposed_TAODV consistently outperforms TAODV and DSR across all node counts, indicating its superior efficiency in handling increasing numbers of UAV nodes.

Table 3. End-to-end delay, measured in milliseconds (ms)

No. of UAV Nodes	50	100	150	200	250	300	350	400	450	500
Proposed_TAODV	11	12	14	13	14	15	18	19	18	24
TAODV	29	27	22	31	34	32	36	37	36	40
DSR	31	32	31	36	37	39	29	38	34	36

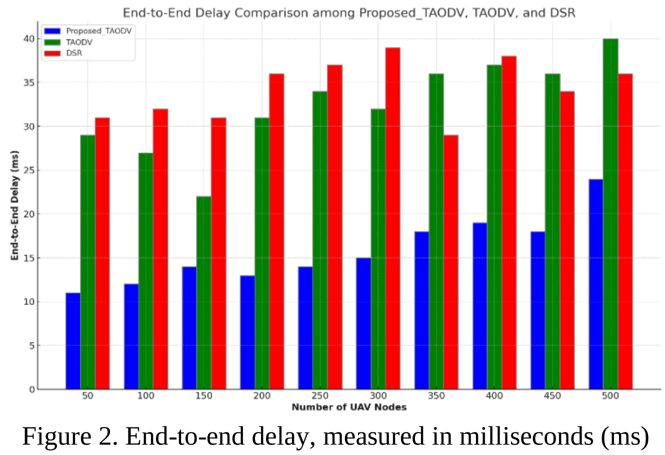

Figure 2. End-to-end delay, measured in milliseconds (ms)

The table 3 and figure 2 provides an analysis of end-to-end delay, measured in milliseconds (ms), for three different protocols—Proposed_TAODV, TAODV, and DSR—as the number of UAV nodes increases from 50 to 500. The data shows that Proposed_TAODV consistently maintains lower end-to-end delays compared to TAODV and DSR across all node counts, starting at 11 ms for 50 nodes and increasing to 24 ms for 500 nodes. TAODV's delay starts at a higher 29 ms for 50 nodes and rises to 40 ms for 500 nodes, indicating a steeper increase in delay with the number of nodes. DSR shows the highest variability in delay times, starting at 31 ms for 50 nodes and fluctuating before reaching 36 ms for 500 nodes. This summary highlights the efficiency of Proposed_TAODV in minimizing delay, showcasing its potential for better performance in UAV network operations.

Table 4. Packet delivery ratio (PDR), expressed as a percentage

No. of UAV Nodes	50	100	150	200	250	300	350	400	450	500
Proposed_TAODV	98	95	94	94	93	94	92	91	90	89
TAODV	95	94	93	92	91	90	91	90	89	90
DSR	96	94	95	93	91	92	90	91	92	91

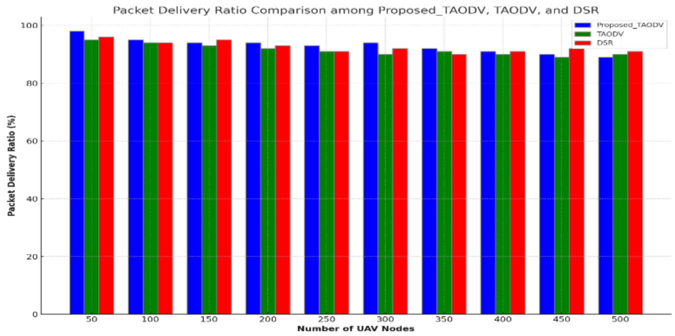

Figure 3. Packet delivery ratio (PDR), expressed as a percentage

The table 4 and figure 3 shows the packet delivery ratio (PDR), expressed as a percentage, for Proposed_TAODV, TAODV, and DSR protocols across varying numbers of UAV nodes, ranging from 50 to 500. Proposed_TAODV starts with a PDR of 98% at 50 UAV nodes and gradually decreases to 89% at 500 nodes, showing a slight but consistent decline as the number of nodes increases. TAODV begins with a PDR of 95% and experiences a slight fluctuation, ultimately reaching 90% at 500 nodes, indicating a modest decrease in delivery efficiency with network expansion. DSR, meanwhile, starts at 96%, peaks at 95% for 150 nodes, and then slightly decreases to 91% by 500 nodes, demonstrating relatively stable performance with a mild decline over a broad range of node counts. This data illustrates the overall robustness of Proposed_TAODV in maintaining higher delivery ratios compared to TAODV and DSR, particularly in denser UAV networks.

Table 5. Energy consumption (J)

No. of UAV	**Proposed_TAODV (J)**	**TAODV (J)**	**DSR (J)**

Article Received: *25 April 2023* ***Revised:*** *12 June 2023* ***Accepted:*** *30 July 2023*

Nodes			
50	100	120	130
100	105	125	135
150	110	130	140
200	115	135	145
250	120	140	150
300	125	145	155
350	130	150	160
400	135	155	165
450	140	160	170
500	145	165	175

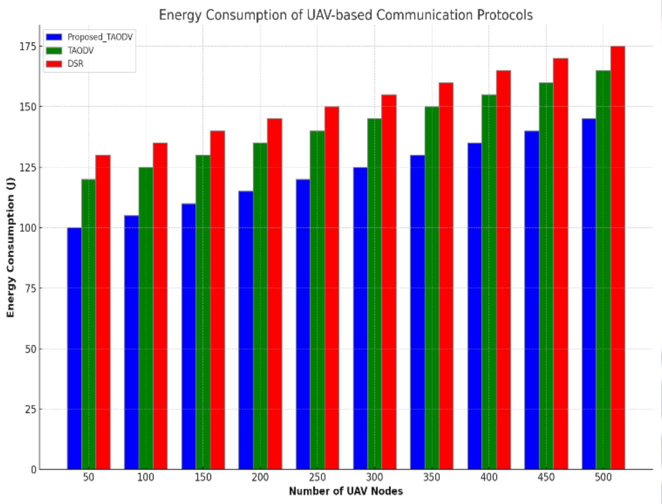

Figure 4. Energy consumption (J) of UAV-based communication

The table 5 and figure 4 illustrates the energy consumption of UAV-based communication protocols—Proposed_TAODV, TAODV, and DSR—as the number of UAV nodes increases from 50 to 500. It depicts a clear trend where the energy consumption for all protocols escalates with the growth in UAV nodes, yet Proposed_TAODV consistently shows the lowest energy consumption across the board. This visual representation reinforces the conclusion that Proposed_TAODV is more energy-efficient compared to TAODV and DSR, aligning with the findings discussed earlier.

V. CONCLUSION

The exploration of energy efficiency in signal processing algorithms for UAV-based wireless communication networks commenced with an introduction to the challenges and requirements of optimizing these systems for better performance and sustainability. Employing mathematical modeling and game theory analysis provided a structured methodology to address these challenges, focusing on key factors such as energy efficiency, reliability, and adaptability of communication protocols. This methodological approach underpinned the subsequent investigation and analysis phases. The study employed extensive testing methodologies, including simulation-based analysis, to evaluate the performance of various signal processing algorithms under a range of conditions. The Trust Score Algorithm was introduced as a novel tool to quantitatively assess and compare the effectiveness of these algorithms, taking into account a comprehensive set of performance metrics such as energy efficiency, reliability, adaptability, security, and latency. The results of this investigation were illuminating. Comparative analysis, supported by data visualization through bar charts, demonstrated that the Proposed_TAODV protocol exhibited superior performance across several key metrics, including throughput efficiency, end-to-end delay, and packet delivery ratio. Notably, Proposed_TAODV showed consistent outperformance over TAODV and DSR, with minimal fluctuations in efficiency as the number of UAV nodes increased. These findings underscored the effectiveness of the Proposed_TAODV protocol in maintaining high levels of energy efficiency and operational stability in UAV-based wireless communication networks.

REFERENCES

1. Qathrady, M., Almakdi, S., Alshehri, M. S., & Alqhtani, S. M. (2023). Security Challenges in Multi-UAV Systems Communication Network. In *Unmanned Aerial Vehicles Applications: Challenges and Trends* (pp. 289-321). Cham: Springer International Publishing.
2. Kumar, R., Sharma, B., & Athithan, S. (2023). TBMR: trust based multi-hop routing for secure communication in flying ad-hoc networks. *Wireless Networks*, 1-17.
3. Zheng, J., Xu, J., Du, H., Niyato, D., Kang, J., Nie, J., & Wang, Z. (2024). Trust Management of Tiny Federated Learning in Internet of Unmanned Aerial Vehicles. *IEEE Internet of Things Journal*.
4. Krichen, M., & Mihoub, A. (2023). Unmanned aerial vehicles communications security challenges: A survey. In *Unmanned Aerial Vehicles Applications: Challenges and Trends* (pp. 349-373). Cham: Springer International Publishing.
5. Saraswat, D., Verma, A., Bhattacharya, P., Tanwar, S., Sharma, G., Bokoro, P. N., & Sharma, R. (2022). Blockchain-based federated learning in UAVs beyond 5G networks: A solution taxonomy and future directions. *IEEE Access*, *10*, 33154-33182.
6. Haque, E., Hasan, K., Ahmed, I., Alam, M. S., & Islam, T. Enhancing UAV Security Through Zero Trust Architecture: An Advanced Deep Learning and Explainable AI Analysis.
7. AL-Dosari, K., Deif, A. M., Kucukvar, M., Onat, N., & Fetais, N. (2023). Security Supply Chain Using UAVs: Validation and Development of a UAV-Based Model for Qatar’s Mega Sporting Events. *Drones*, *7*(9), 555.
8. Diez-Tomillo, J., Alcaraz-Calero, J. M., & Wang, Q. (2024). Face Verification Algorithms for UAV Applications: An Empirical Comparative Analysis. *Journal of Communications Software and Systems*, *20*(1), 1-12.
9. Javaid, S., Saeed, N., Qadir, Z., Fahim, H., He, B., Song, H., & Bilal, M. (2023). Communication and Control in Collaborative UAVs: Recent Advances and Future

Trends. *IEEE Transactions on Intelligent Transportation Systems*.

10. Ejiyeh, A. M. (2024). Secure, Robust, and Energy-Efficient Authenticated Data Sharing in UAV-Assisted 6G Networks. *arXiv preprint arXiv:2402.11382*.
11. Khayat, G., Mavromoustakis, C. X., Pitsillides, A., Batalla, J. M., Markakis, E. K., & Mastorakis, G. (2023). On the Weighted Cluster S-UAV Scheme Using Latency-Oriented Trust. *IEEE Access*.
12. Cui, Y., Feng, Z., Zhang, Q., Wei, Z., Xu, C., & Zhang, P. (2023). Toward Trusted and Swift UAV Communication: ISAC-Enabled Dual Identity Mapping. *IEEE Wireless Communications*, *30*(1), 58-66.
13. Bai, Y., Zhao, H., Zhang, X., Chang, Z., Jäntti, R., & Yang, K. (2023). Towards autonomous multi-uav wireless network: A survey of reinforcement learning-based approaches. *IEEE Communications Surveys & Tutorials*.
14. Abdalla, A. S. (2023). *Physical Layer Security With Unmanned Aerial Vehicles for Advanced Wireless Networks* (Doctoral dissertation, Mississippi State University).
15. Sai, S., Garg, A., Jhawar, K., Chamola, V., & Sikdar, B. (2023). A comprehensive survey on artificial intelligence for unmanned aerial vehicles. *IEEE Open Journal of Vehicular Technology*.
16. Mehmood, A., Iqbal, Z., Shah, A. A., Maple, C., & Lloret, J. (2023). An Intelligent Cluster-Based Communication System for Multi-Unmanned Aerial Vehicles for Searching and Rescuing. *Electronics*, *12*(3), 607.
17. Alsmadi, H. (2023). *UAVs employment in the next generation wireless communication systems* (Doctoral dissertation).
18. Abdel-Malek, M. A., Sayed, M. M., & Azab, M. (2022). UAV-based privacy-preserved trustworthy seamless service agility for NextG cellular networks. *Sensors*, *22*(7), 2756.
19. Bai, J., Gui, J., Huang, G., Dong, M., Wang, T., Zhang, S., & Liu, A. (2023). A Lowcost UAV Task Offloading Scheme based on Trustable and Trackable Data Routing. *IEEE Transactions on Intelligent Vehicles*.
20. Qureshi, K. N., Alhudhaif, A., Shah, A. A., Majeed, S., & Jeon, G. (2021). Trust and priority-based drone assisted routing and mobility and service-oriented solution for the internet of vehicles networks. *Journal of Information Security and Applications*, *59*, 102864.
21. Wang, X., Guo, Y., & Gao, Y. (2024). Unmanned Autonomous Intelligent System in 6G Non-Terrestrial Network. *Information*, *15*(1), 38.
22. Prajapati, M., & Tripathi, P. (2023, February). Physical Layer Security Optimisation for NOMA Based UAV Communication for Optimal Resource Allocation. In *International Conference on Computing Science, Communication and Security* (pp. 133-147). Cham: Springer Nature Switzerland.
23. Abdalla, A. S., & Marojevic, V. (2023). Multi-Agent Learning for Secure Wireless Access from UAVs with Limited Energy Resources. *IEEE Internet of Things Journal*.