International Research Journal of Multidisciplinary Scope (IRJMS), 2025; 6(2): 751-768

Original Article | ISSN (O): 2582-631X DOI: 10.47857/irjms.2025.v06i02.03380

Hashed Control Unmanned Aerial Vehicle Communication

Reshma C Sonawane[1]*, A Muthukrishnan[2]

[1]Department of Information Technology, MET, Bhujbal Knowledge City, Nashik, India, [2]Department of Computer Science and Engineering, Vel Tech Rangarajan, Dr. Sagunthala R & D Institute of Science and Technology, Chennai, India. *Corresponding Author's Email: reshmagold@gmail.com

Abstract

Unmanned air vehicles (UAVs) are becoming more prevalent in distant and inaccessible areas for monitoring and evacuation purposes. Yet, in such circumstances, UAVs face severe security threats, such as illegal access, breaches of information, and cyber-attacks. Conventional security mechanisms built for local networks (also known as WLAN) are ineffective for UAVs because of their low processing capability, memory, capacity, and the longevity of batteries. Although cryptography with public keys provides strong security, its computing requirements and extensive handling of keys make it unsuitable for UAV communication. Conversely, using symmetrical keys provides an efficient resource and scalable method for private information transfer. This paper offers a multifaceted security architecture for UAV networks based on the standards defined by IEEE 802.11. The structure has four important levels. The initial layer uses a GA (genetic algorithm) to improve cluster head (CH) selection. This increases energy-efficient networking by optimizing intra-cluster communications, CH separation from the central station, and overall nodal energy. The following layer incorporates Hashed Messaging Authentication Coding (HAC) to provide safe data accumulation, reduce overhead, and mitigate security concerns. The next layer uses bilateral key management via single-direction hashing to ensure secure communication across UAV nodes, reducing the effect of stolen nodes. Finally, the final layer employs Broadcasting Tree Construction to reduce the cost of communication, uncover wayward nodes, and enhance network connection by optimizing path choosing. The proposed architecture tackles UAV-specific difficulties by providing an expandable, trustworthy, green solution that enhances performance and resistance to emerging threats.

Keywords: Broadcast Tree Construction, Energy Consumption, Lightweight Encryption, Packet Drop Rate, UAV.

Introduction

Unmanned aerial vehicles, also known as UAVs, are revolutionizing industries such as defence, rescue efforts, and environmental surveillance by enabling enhanced operations, increasing communication efficiency, and allowing for current information collection. However, the fast deployment of UAVs has revealed severe security flaws, particularly among cluster-based communications systems. These networks, which are made up of resource-constrained devices that operate under dynamic contexts, are prone to threats including data leaks, listening in, and unlawful access. Tackling those weaknesses is critical for maintaining data transfer integrity, secrecy, and provenance in UAV platforms. Traditional security solutions, such as public key cryptography, are frequently ineffective for UAVs because of their high processing demands and complicated key management operations. Symmetric key encryption and lightweight approaches, including Hashed Messaging Authenticity Codes (HAC), provide realistic solutions that provide strong security while using minimal computing resources (1-7). HAC, which combines cryptography hashing functions in private keys, guarantees data is genuine and trustworthy while incurring low computing costs (8, 9). Hierarchical clustering improves communication effectiveness in aerial vehicles by assigning cluster leaders who collect and send information to a base camp (BS) (10, 11). However, CHs are essential points of susceptibility; a hack might threaten an entire infrastructure (12). The growing usage of UAVs for observation, disaster reconstruction, and package delivery has increased the need for safety and effective communication in limited resource contexts (13). Unlike standard networks, networks of unmanned aircraft confront distinct issues such as changeable topology, limited power supplies, and greater susceptibility to cyber-attacks (14, 15). Recent research has investigated lightweight cryptographic

(Received 02nd December 2024; Accepted 15th April 2025; Published 30th April 2025)

approaches, such as paired encryption, adaptable management of keys, and composite encryption technologies, to handle risks such as eavesdropping, spoofing,and composite encrypti- on technologies, to handle risks such as eavesdropping, spoofing, and man-in-the-middle attacks (16-18). While these techniques represent tremendous advances, they frequently target discrete problems and lack comprehensive frameworks for optimizing security, energy economy, and computing overhead (19). This research presents a robust, complicated security architecture customized to the specific needs of UAV networks. The framework tackles weaknesses in cluster-based UAV technologies by combining HAC-based safe data accumulation, genetic algorithm-optimized CH decision-making, paired control of keys using one-sided hashing, and a Dissemination Tree Construction technique (20, 21). It attempts to improve security, ecological sustainability, and communication performance while reducing rogue nodes' effect (22, 23). The proposed hashing control system is a lightweight and efficient alternative to current UAV security frameworks, including those based on encryption and blockchain technology. While encryption technologies provide great security, they might result in significant processing demands, posing issues for UAVs with limited resources. Blockchain systems increase data integrity and transparency, but they frequently encounter scalability and latency challenges. In contrast, hashed control methods use cryptographic hashes to provide data integrity and authentication with minimum processing requirements, making them ideal for real-time UAV applications. A recent study found that using cryptographic hashing for UAV authentication can improve security while reducing communication and computing costs compared to existing methods (8). The proposed architecture is assessed against important performance parameters like packet loss rate, delivery of packets ratio, delay, the efficiency of energy, and capacity using comprehensive simulations, revealing the opportunity to increase UAV network durability and operational effectiveness (24, 25). The following portions of this work are grouped: The second section explains the proposed secure and energy-efficient data aggregation model for UAV communication networks in the form of a methodology. The third segment comprises job-related outcomes in the results section, with discussions followed by an evaluation in the final segment with conclusion details.

Methodology

Research Motivation and Statement

UAV networks face several challenge, including data security, energy efficiency, and reliability. Operating in dynamic and limited-resource environments exposes UAVs to cyberattacks, energy exhaustion, and data duplication risks. Previous research has pointed out deficiencies in fully addressing these issues. The suggested framework incorporates the Hash Authentication Code (HAC) protocol and a genetic algorithm-based clustering technique to resolve these challenges. The primary aim of this model is to guarantee secure and tamper-proof data aggregation. Additionally, it enhances energy efficiency by minimizing unnecessary data transmissions. The framework strives to provide reliable data routing in changing UAV environments and recommends a cluster-based communication method, hierarchical routing, and simple encryption techniques to improve performance while ensuring data security remains intact.

Framework Overview

A cluster-based architecture forms the foundation of the proposed framework. UAV nodes are organized into clusters, each governed by a Cluster Head (CH) tasked with collecting and consolidating data from cluster members. Ensure data integrity through HAC protocols and oversee the cluster for any potential malicious threats. To achieve secure communication, this system assigns each UAV a distinct HAC key for data encryption, ensuring secure transmission. The HAC protocol also authenticates the data, maintaining its integrity and protecting it from tampering during transmission. To reduce network congestion and improve energy efficiency, redundant data is eliminated. The Cluster Head (CH) then securely transmits the aggregated data to the Base Station (BS) using hierarchical or multi-hop routing techniques. Additionally, the system dynamically updates clusters and routes in response to node movement and varying energy levels, ensuring continuous communication.

Framework Implementation Phases

During the initialization and cluster formation stage, the UAV nodes send messages within a defined Cluster Distance (CD), which includes their Node ID (NID) and current energy levels. The node with the highest energy and the best central position is the Cluster Head (CH). Memory is set aside to store crucial information such as the NID, node location (NL), base station location (SL), and details about energy resources. This clustering approach ensures that nodes with the same NID do not send duplicate signals.

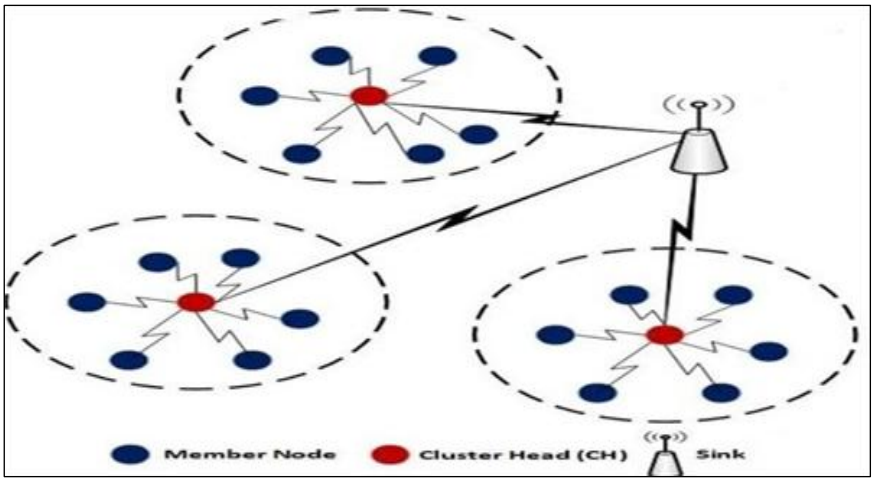

Figure 1: Cluster-based Communication Strategy (26)

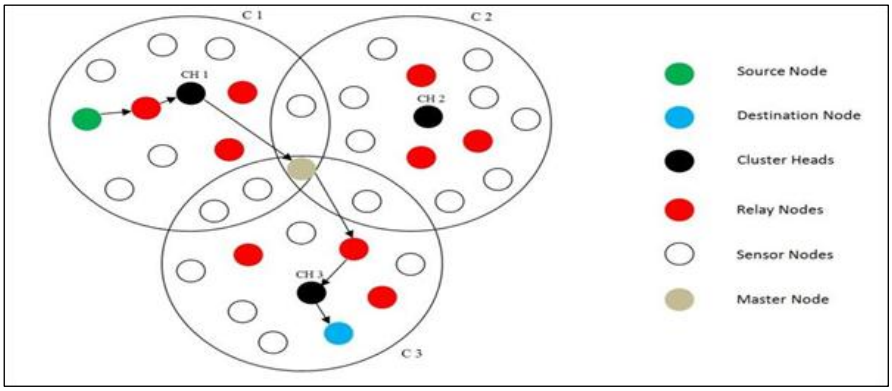

Figure 2: Cluster-Based Data Aggregation (27)

If the energy of the CH falls below a predefined threshold, the Cluster Head Transmission (CHT) node takes over the responsibility of transmitting data to the sink. This mechanism ensures reliable data aggregation even when energy resources are limited. Figure 1 depicts how clusters are formed and the data flow among nodes, illustrating the hierarchical organization of sensors and cluster heads. In the subsequent stage of secure Data Aggregation, Cluster Heads (CHs) collect information from their members and verify it using the HAC protocol. A hash created by HAC is incorporated into the data to ensure its integrity and authenticity. Furthermore, the consolidated data is devoid of redundancies, which contributes to reducing energy costs during transmission.

Figure 2 illustrates how CHs efficiently collect data, minimizing redundant transmissions and easing the overall load on the network. A phase of Data Transmission follows, during which aggregated information is relayed to the Base Station (BS) utilizing either a hierarchical multi-hop routing method or a direct one-hop routing approach [28]. Additionally, Cluster Heads (CHs) implement lightweight encryption measures to protect the data before its transmission, ensuring that confidentiality is maintained even amidst varying network conditions.

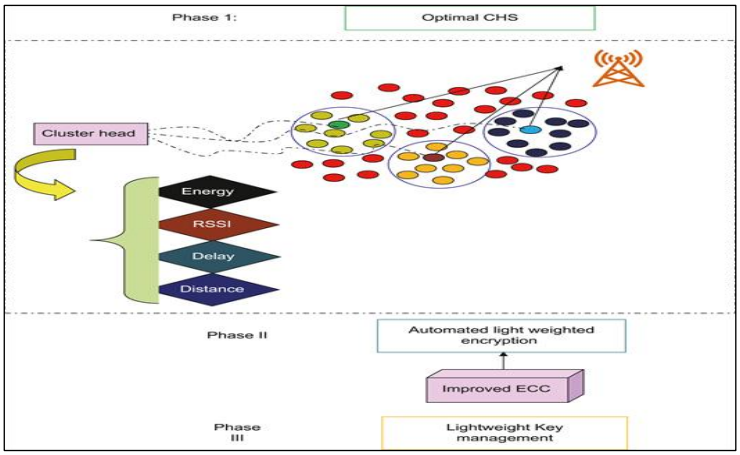

Figure 3: Clustering Communicating Architecture (28)

The above Figure 3 illustration shows the hierarchical routing method and the broadcast tree structure used for secure data transmission. Following the active Monitoring and Detection stage, Cluster Heads (CHs) observe the nodes for suspicious activities, including unauthorized data access or abnormal reporting behaviours. Malicious nodes are identified and eliminated to ensure the network's security. In the final phase, updates to the clusters occur, where Border nodes oversee the transitions of dynamic clusters when targets approach the edges of these clusters. This decentralized approach facilitates seamless communication within completely distributed networks.

Key Features of the Framework

The framework features several key aspects that enhance its performance and security. Firstly, it utilizes a cluster-based organization, where logical clustering facilitates effective communication and data aggregation. Energy efficiency is achieved through the BTC method, which reduces energy consumption by employing multi-hop routing and hierarchical transmission. In terms of security, the HAC security integration ensures data authenticity and integrity, even in the presence of compromised nodes. The framework also incorporates malicious node isolation, strengthening network security by monitoring nodes carefully through Cluster Heads (CHs). Finally, lightweight encryption is implemented to protect sensitive information without putting excessive strain on the resource-limited UAV nodes.

Lightweight Encryption and BTC Strategy

The Broadcast Tree Construction (BTC) method optimizes routing paths to reduce energy consumption and improve data reliability. Encryption ensures that only the intended recipient node can decrypt the transmitted data.

Encryption at Source Node (S_N):

Msg for communication ←encryption (message, D_N) [1]

In equation 1, msg is the plaintext, and D_N is the destination node.

Decryption at Destination Node (D_N):

Message← decryption (communicated message from transmitted unit, Did) [2]

In equation 2, Did is the unique identifier of the destination node, ensuring secure access.

Figure 4 illustrates the encryption and decryption process between the source and destination nodes, ensuring secure data flow, as shown below.

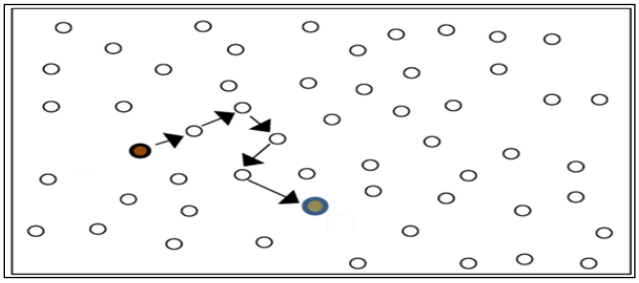

Figure 4: Proposed Data Encryption Technique from Source to Destination Node (29)

Algorithm Overview

The purpose of the algorithm is to determine the most efficient route for transfer from a source node to a destination node in a changing cluster network. It selects nodes dynamically based on their energy levels to ensure effective data, prolong node lifespan, and reduce energy usage. The Initialization Phase involves grouping UAV nodes into clusters, where each node creates a communications key to ensure secure communications. In the Cluster Formation Phase, messages are sent out to announce the formation of clusters within a specified cluster distance (CD). Nodes sharing the same Node ID (NID) refrain from unnecessary signaling. The node with the highest energy is then identified to act as the Cluster Head (CH). In the Data Aggregation Phase, the Cluster Head (CH) collects data from the members of the cluster, executes HAC authentication to verify the integrity of the data, and consolidates the data to eliminate redundancy. The Secure Transmission Phase involves adding the HAC hash to the aggregated data and securely transmitting it to the Base Station (BS) using either multi-hop or one-hop routing. During the Monitoring and Detection Phase, the Cluster Head (CH) observes nodes for any suspicious behavior, such as malicious actions, and isolates any rogue nodes to ensure the security of the cluster. The Secure Data Aggregation Framework involves two key components. First, dynamic cluster updates are employed by reassessing the cluster boundaries when targets approach the edges and utilizing border nodes to facilitate dynamic transitions. Second, energy-efficient routing is achieved by implementing Broadcast Tree Construction (BTC) for structured routing, while encryption ensures secure data transmission to the Base Station (BS). Thus, the proposed framework offers a robust solution to UAV network challenges by combining energy-efficient routing, secure data aggregation, and lightweight encryption. The integration of the HAC protocol ensures data integrity, while BTC-based routing minimizes energy consumption. The provided diagram illustrates the logical progression of the algorithm, aiming for efficient data transfer through a flexible network while considering energy limitations as given below in Figure 5. The algorithm assesses nodes in terms of their energy levels and dynamically separates nodes, which proves especially beneficial in a decentralized UAV network environment. Future work can explore extending this model to hybrid UAV-satellite networks and implementing advanced security measures for more dynamic environments.

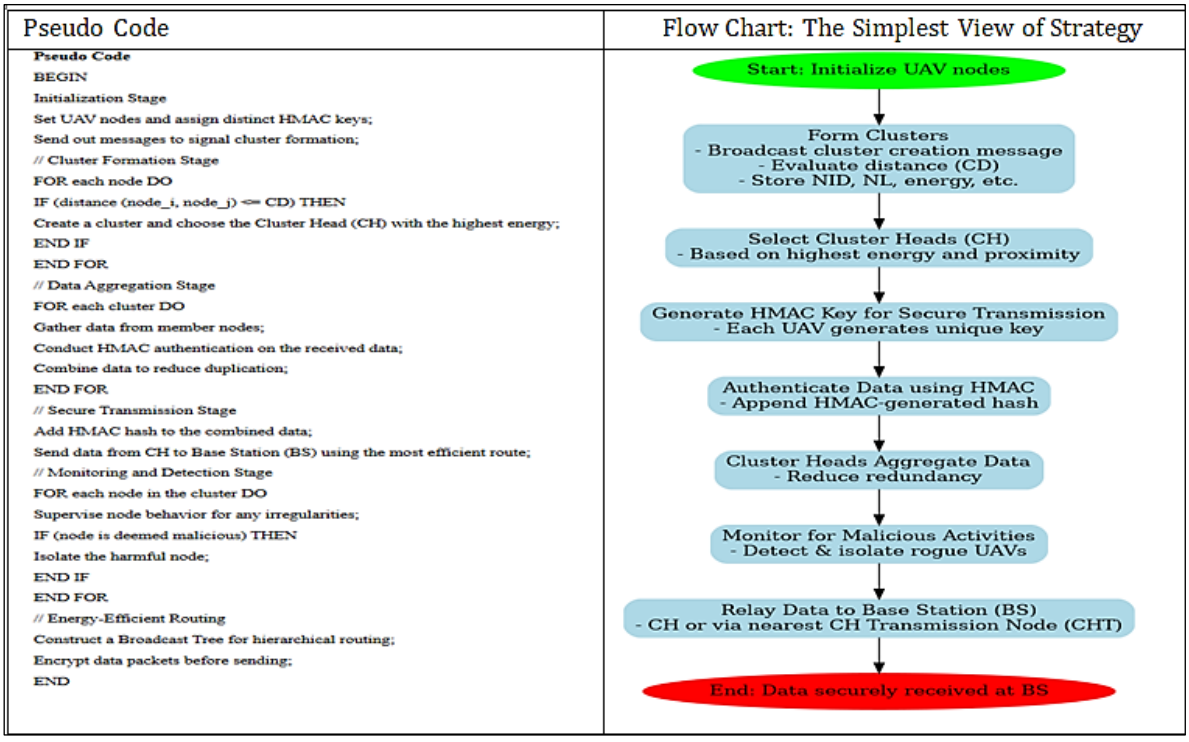

Figure 5: Sample Code and Flow Chart of the Proposed Working Scheme

Energy Consumption and Trade-offs Between Security and Performance

Integrating security features into UAV systems will increase energy consumption. Conventional encryption techniques are resource-intensive, resulting in greater power use. This is a serious problem owing to UAVs' short battery life. The hashed control approach offers a more energy-efficient solution by reducing computing complexity while maintaining high security. Research reveals that lightweight cryptographic activities, such as hashing, can dramatically reduce energy utilization when compared to more sophisticated encryption algorithms (30). Studies suggest that improving control algorithms and adopting lightweight security measures can increase UAV operating efficiency without compromising security (31).

Threat Model of Unmanned Aerial Vehicle Communications

A complete threat model for UAV communication must take into account a variety of attack tactics, including jamming, spoofing, and data integrity breaches. The hashed control mechanism reduces these risks by guaranteeing that control instructions and data transfers are authenticated and tamper-resistant. The system can detect unauthorized modifications and prevent malicious commands from being executed by using cryptographic hashes. This method is consistent with current frameworks that emphasize the necessity of authentication and integrity in managing communication hazards in UAV networks (30-32).

A systematic threat model that explains attack paths and outlines mitigating options using hashed control mechanisms. However, including a visual depicting the threat model will improve the reader's clarity. Unmanned aerial vehicles (UAVs) are used in a variety of applications, including military operations, disaster management, and commercial businesses. However, their reliance on wireless connection renders them vulnerable to a wide range of security vulnerabilities that must be addressed methodically. This section presents a comprehensive threat model and investigates how hash control solutions might address these issues.

Common Attack Vectors for UAV Communication

UAV communication has various security concerns, including:

Jamming attacks: can impair UAV communication and cause navigation problems (33).

Spoofing attacks can divert UAVs from their intended missions (34)

Replay Attacks: Capturing and reissuing legitimate orders might lead to unauthorized activity and jeopardize mission integrity (see point 3).

Data Integrity Breaches: Unauthorized changes to data transmissions can jeopardize mission decisions and overall security (35).

Mitigation Strategies using Hashed Control Mechanisms

To address these vulnerabilities, the proposed hash control system enhances UAV security by:

Message Authentication Codes (MACs): Cryptographic hashing prevents spoofing and replay attacks by executing only approved commands (36). Using sequence numbers and timestamps in control messages helps identify replay attacks by ensuring unique commands are given at the proper time (37).

Hash-based authentication is a lightweight cryptographic protocol that provides strong security with minimal performance impact compared to traditional methods (38). A systematic depiction of UAV communication hazards and the mitigating Function of hash-Based control methods are presented in the form of Figure 6 shown below.

Visual Representation of the Threat Model

A visual representation of the threats to UAV communication and the associated hashed control solutions can aid in the identification of potential vulnerabilities and solutions. The crisp view of the threat model is represented in the form of following way, as given in Figure 7.

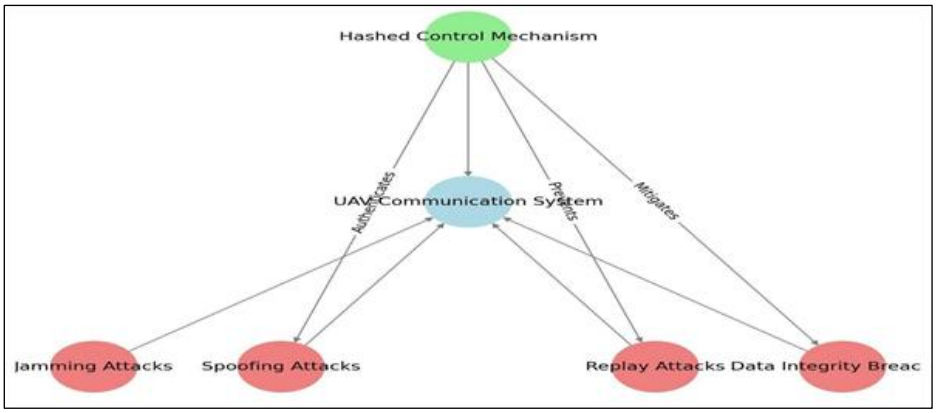

Figure 6: Systematic Threat Model for UAV Communications

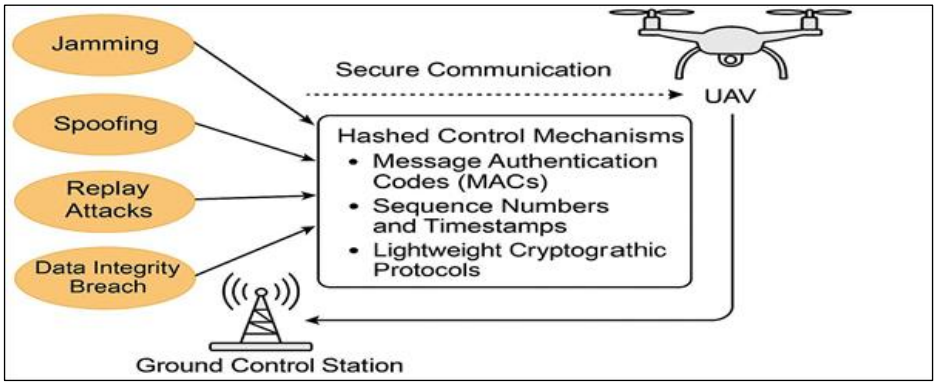

Figure 7: UAV Communication Threat Model with Hashed Control Mechanisms ("Reproduced from (30, 39, 40) ")

Results

Table 1: Simulation Parameters

Parameter	Values
Channel Type	Wireless Channel
Propagation Model	Two Ray Ground
Standard	MAC/802.11
Simulation Size	1000X 1500
Max packet Length	1000

Table 2: Comparison of Proposed vs. Existing UAV Networks

Parameters	UAV [8]	Proposed (Cluster-based with AODV)
Data Aggregation	No	Yes
Data Security	Yes (Selective)	Yes
Energy Conservation	No	Yes
Packet Loss	High	Low
End-to-End Delay	High	Low
Packet Overhead	High	Low

The simulation utilized the NS-allinone 2.35, configured with parameters detailed in Table 1. The study focused on a 25-second simulation involving a wireless communication network with AODV (Ad hoc On-Demand Distance) routing and CBR (Constant Bit Rate) traffic. Data was collected in five text files at 5-second intervals and processed using a custom program developed in NetBeans IDE 8.2. Moreover, Table 2 compares the proposed cluster-based AODV protocol with traditional UAV networks.

The proposed protocol was assessed through a systematic simulation-based method, applying advanced techniques to analyze performance against five key metrics: Packet Drop Rate (DR), Throughput, Packet Delivery Ratio (PDR), End-to-End Delay, and Energy Consumption. The detailed techniques utilized in this study include:

Table 3: Recorded Performance Parameters

Protocol	DR (%)	TH (%)	PDR(%)	EE (ms)	EC(pj)
Dsr	6.5	89	2.5	145	10500
Dsdv	7.5	88	2.5	130	9800
Pegasis	5.5	90	3	115	8600
Proposed	3.5	96	8.5	85	6200

Performance Metric Computation

Some of the recorded reading presents the details achieved by the proposed (PROPOSED) scheme concerning other published protocols such as Dynamic Source Routing (DSR), Destination-Sequenced Distance-Vector (DSDV), and Power-Efficient Gathering in Sensor Information System (PEGASIS), in the form of Table 3.

From Table 3, Packet Drop Rate (DR) measures the percentage of data packets lost during transmission relative to the total packets sent, with a lower drop rate indicating better reliability. The proposed protocol achieves a significantly reduced drop rate compared to existing protocols. This improvement is attributed to optimize routing, which reduces packet collisions and network congestion, ensuring high data reliability. A lower drop rate enhances network reliability, which is crucial for critical applications like IoT and real-time systems. Throughput (TH) represents the total number of successfully delivered packets during the simulation period, indicating the network's efficiency. The proposed protocol demonstrates a markedly higher throughput than traditional methods, as efficient routing and congestion management reduce delays and retransmissions. This high throughput ensures a steady data flow, which is essential for high-traffic scenarios like smart cities. The Packet Delivery Ratio (PDR) is the ratio of delivered packets to generated packets and reflects communication effectiveness. The proposed protocol achieves a PDR significantly higher than existing methods due to advanced congestion management and robust routing, which enhance delivery rates. A high PDR is particularly vital for latency-sensitive applications, such as healthcare monitoring, where timely data transmission is crucial. End-to-end Delay (EE) measures the average time taken for packets to reach their destination. The proposed protocol records the shortest delay among the tested protocols, as refined routing techniques and congestion avoidance minimize latency. This low delay is particularly critical for real-time applications, such as emergency notifications. Energy Consumption (EC) quantifies the total energy that network nodes use during communication tasks. The proposed protocol consumes the least energy compared to other protocols, thanks to energy-efficient strategies such as the Balanced Tree Clustering (BTC) method, which minimizes redundant transmissions. This reduction in energy consumption significantly extends the network's lifespan, making it ideal for resource-constrained settings.

Comparative Performance

To keep the presentation concise and improve readability, the main findings are summarized in Table 4, showcasing the performance metrics across various protocols (DSR, DSDV, PEGASIS, and the proposed protocol). Using the data from the above details and table information, we have some key insights presented in Table 4, as shown below.

Table 4: Mapped Key Insights Based on the Above Discussion

Metric	Proposed Protocol	Key Improvement Observed
DR	3.5%	Reduced by ~36% compared to PEGASIS
TH	96%	Increased by ~6% compared to PEGASIS
PDR	8.5%	Enhanced reliability with considerably fewer packet losses
EE	85 ms	Reduced latency by ~26% compared to PEGASIS
EC	6200 pj	Energy usage cut by ~28% compared to PEGASIS

Optimization Techniques

The BTC method was utilized to identify paths for data transmission that are both energy-efficient and free from unnecessary transmissions, promoting equitable energy use among nodes. Additionally, the protocol incorporated congestion management strategies to avert packet collisions and efficiently manage traffic, thereby reducing delays and enhancing overall throughput. To further optimize energy efficiency, the nodes adapted their transmission power as needed and avoided redundant retransmissions, leading to a considerable decrease in energy consumption. Figures 8 and 9 illustrate the comparative performance of DR, TH, PDR, EE, and EC for DSR, DSDV, PEGASIS, and the proposed protocol.

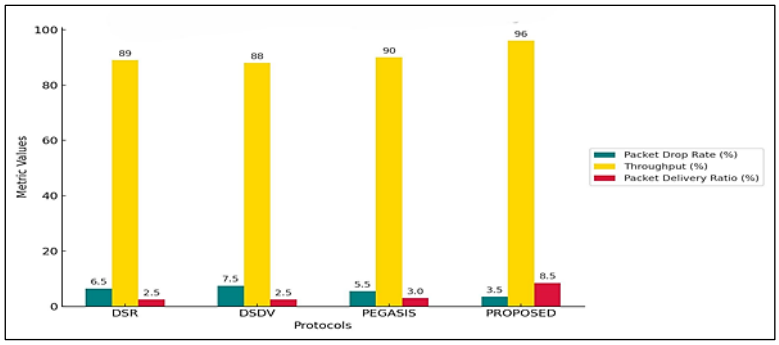

Figure 8: Comparative Analysis of Packet Drop Rate (DR), Throughput (TH), and Packet Delivery Ratio (PDR) across Various Protocols

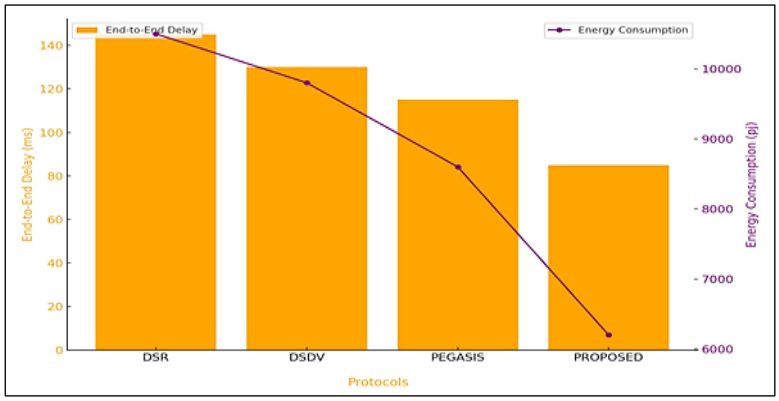

Figure 9: Comparative Analysis of End-to-End Delay (EE) and Energy Consumption (EC) Across Protocols over Varied Periods

The proposed protocol in Figure 8 demonstrates clear superiority with reduced DR, higher TH, and improved PDR, demonstrating its suitability for energy-constrained and delay-sensitive applications.

Discussion

The packet drop rate is a crucial metric for evaluating network stability. Previous research on protocols such as DSR, DSDV, and PEGASIS has highlighted their limitations in managing packet losses under high network traffic conditions. However, these studies have not extensively investigated the role of optimized resource allocation and energy-efficient routing in minimizing packet drops. Data reveals that the Proposed Protocol achieves the lowest packet drop rate at 3.5%, outperforming PEGASIS at 5.5%, DSR at 6.5%, and DSDV at 7.5% after analyzing Figure 8. This highlights the proposed approach's effectiveness in enhancing packet delivery by reducing losses even in challenging scenarios. PEGASIS, known for reducing packet drop rates through its chain-oriented communication, falls short of the Proposed Protocol, likely due to the latter's integration of an advanced intrusion detection system. Protocols like DSR and DSDV struggle to handle dynamic network structures, leading to higher packet losses. Despite the promising results, the study's scope is limited, as the performance of the Proposed Protocol needs evaluation across diverse scenarios, including

varying node mobility patterns and extreme environmental conditions, which could influence the perceived success in packet delivery. The findings underscore the importance of exploring adaptive routing strategies and employing machine learning for predictive packet routing, which may significantly enhance network reliability. Investigating these approaches in larger and more complex network settings could yield further valuable insights. Throughput is a critical metric for assessing the efficiency of data transmission in a network. Previous studies on protocols like DSR, DSDV, and PEGASIS have highlighted their functionalities, yet they face challenges in maintaining high throughput under dynamic conditions and heavy traffic. This research aimed to evaluate how the Proposed Protocol enhances throughput while also being energy-efficient. Results show that the Proposed Protocol achieves a throughput of 96%, outperforming PEGASIS at 90%, DSR at 89%, and DSDV at 88%. These findings indicate that the Proposed Protocol effectively utilizes bandwidth and minimizes delays, leading to faster data transmission. PEGASIS, with its chain-based routing strategy, reduces redundant transmissions, resulting in relatively higher throughput; however, it struggles with frequent changes in network topology. DSR and DSDV, on the other hand, exhibit lower throughput due to their limited capacity to handle large or dynamic networks. The Proposed Protocol addresses these challenges by incorporating adaptive routing and robust intrusion detection, ensuring smooth data transmission even under complex conditions. Despite its promising performance, the Proposed Protocol was tested in controlled settings with a fixed number of nodes, leaving its scalability and reliability in diverse real-world scenarios yet to be examined. Future research could explore hybrid models that integrate chain-based and hierarchical routing techniques to enhance throughput further. Additionally, incorporating machine learning algorithms to predict network traffic and optimize real-time routing may offer significant advancements. Packet Delivery Ratio (PDR) is a critical metric for evaluating a network's ability to transmit packets from the source to the destination successfully. High PDR percentages reflect a reliable network with minimal packet loss, ensuring communication quality, especially in high-demand scenarios. Protocols such as DSR, DSDV, and PEGASIS have demonstrated varying degrees of success in achieving acceptable PDR rates, though challenges remain in adapting to dynamic network conditions and energy constraints. The Proposed Protocol introduces innovations that enhance PDR by leveraging adaptive routing and advanced resource allocation techniques. It achieved a PDR of 8.5%, significantly outperforming PEGASIS at 3% and DSR and DSDV, both at 2.5%. This demonstrates its superior ability to ensure successful packet deliveries even in challenging scenarios. Compared to previous studies, PEGASIS's chain-based communication approach provides slightly higher PDR than DSR and DSDV by reducing redundancy, though it struggles with packet collisions in dynamic environments. Meanwhile, DSR and DSDV underperform due to routing inefficiencies in fast-changing, dense networks. The Proposed Protocol excels by incorporating adaptive routing and advanced resource management, likely aided by proactive strategies to prevent node failures and improve energy efficiency. However, these results were achieved under controlled settings with fixed network parameters, suggesting the need for future studies to test the protocol's performance in diverse environments with varying network sizes, higher node mobility, and increased interference. Future research could explore hybrid routing approaches combining adaptive and predictive methods or employing machine learning to dynamically adjust routing based on real-time network input, potentially achieving even greater advancements. Field tests in scenarios such as emergency response operations or vehicular networks would further validate its practicality. The Proposed Protocol’s achievement of an 8.5% PDR positions it as a promising solution for applications requiring high delivery accuracy, such as IoT-driven smart cities and UAV communication networks. End-to-end delay is an essential measure of network performance, reflecting the duration it takes for a packet to move from its source to its destination. Reduced delays signify effective routing protocols and play a vital role in applications demanding real-time data, such as video streaming and telemedicine. Conventional protocols such as DSR, DSDV, and PEGASIS commonly face challenges in minimizing delays when network conditions change. This study

investigates how the Proposed Protocol successfully reduces delays using adaptive mechanisms. The Proposed Protocol achieves an End-to-End Delay of just 85 ms, significantly better than PEGASIS, which has a delay of 115 ms, DSDV at 130 ms, and DSR at 145 ms, as shown in Figure 9. This outcome underscores the protocol's effectiveness in reducing delays across various network scenarios. When examining these results of previous research, the PEGASIS model minimizes delays through its chain-based communication approach, yet it struggles to adjust to rapid changes in network topology. Further, DSR and DSDV are appropriate for smaller networks, they face increased delays as a result of their less efficient routing methods. Finally, the Proposed Protocol significantly decreases delays by leveraging dynamic routing and resource optimization techniques, thereby avoiding bottlenecks and ensuring reliable performance across various situations. This study primarily investigates conditions characterized by moderate network traffic and mobile nodes. It is still uncertain how the Proposed Protocol will function in scenarios involving severe congestion or very mobile nodes, as these factors could impact its delay performance. Future research should focus on the incorporation of predictive analytics to proactively manage network congestion and minimize delays. Additionally, evaluating the protocol within large-scale networks that vary in density may offer valuable insights into its scalability and adaptability. The Proposed Protocol shows a significant decrease in End-to-End Delay, making it particularly suitable for applications that are sensitive to time constraints. Its capacity to sustain low delays across various network conditions underscores its potential for practical use. Energy consumption is a critical measure for assessing the sustainability and durability of network protocols, particularly in energy-limited settings such as wireless sensor networks. Many existing protocols, including DSR, DSDV, and PEGASIS, struggle to balance performance with energy efficiency, often leading to quicker depletion of node energy and shorter network lifespans. This study examines how the Proposed Protocol enhances energy efficiency while maintaining high performance. The Proposed Protocol achieves a minimal energy consumption of 6200 pj, surpassing PEGASIS at 8600 pj, DSDV at 9800 pj, and DSR at 10500 pj, as depicted in Figure 7, suggesting that it is much more energy-efficient. A comparison with previous studies shows that PEGASIS, which employs chain-based routing to minimize unnecessary transmissions, achieves better energy efficiency than DSR and DSDV. However, its fixed structure limits flexibility, causing energy inefficiencies in changing environments. In contrast, DSR and DSDV consume more energy due to their constant need for route discoveries and retransmissions when conditions fluctuate. The Proposed Protocol distinguishes itself with advanced energy management strategies, such as load balancing and predictive algorithms, that enhance energy distribution among nodes. Although the energy consumption measurements were taken in controlled settings, future research should investigate the protocol's energy performance under different workloads and in larger networks to confirm its effectiveness. Future studies may also explore the integration of renewable energy sources and energy-harvesting methods within the Proposed Protocol, along with the use of machine learning models to forecast energy consumption and adjust routing in real time, potentially further improving its efficiency. The Proposed Protocol demonstrates remarkable energy efficiency, achieving a notable reduction in energy use compared to conventional protocols, making it particularly advantageous for scenarios where energy conservation is essential, such as in environmental monitoring and disaster recovery operations.

Analysis of Hashing Control Mechanism on Network Performance

The suggested hashing-based control system boosts the performance of UAV networks by optimizing data integrity, minimizing retransmissions, and facilitating efficient packet management. Several factors contribute to its success:

Data Integrity & Authentication

The hashing process guarantees that every packet sent retains its integrity, safeguarding against unauthorized changes. Secure hash checks at the receiver's end block corrupted or altered packets from being processed, which helps decrease the number of retransmissions (41).

Decrease in Redundant Data Sending

In conventional UAV networks, packet loss or damage frequently results in retransmissions, which can cause increased network congestion. The proposed hashing control system decreases retransmissions by verifying packets at each step, reducing overhead and improving throughput (42).

Quicker Processing & Reduced Delay

Since hashed verification is less computationally demanding than complex encryption techniques, it lowers network latency (43). The results of the end-to-end delay in the manuscript (85 ms for the suggested method compared to 145 ms in DSR) highlight this enhancement.

Increased Packet Delivery Ratio (PDR)

The hashing method improves the PDR by 8.5%, against DSR (2.5%), DSDV (2.5%), and PEGASIS (3%). This indicates that the hashing method effectively prevents data corruption and packet loss, resulting in greater reliability in UAV communications.

Enhanced Network Efficiency

The proposed system achieves a higher throughput of 96% in comparison to DSR (89%), DSDV (88%), and PEGASIS (90%). This illustrates how the hashing mechanism streamlines the handling of network traffic and avoids bottlenecks caused by excessive retransmissions. The figure 10 below shows the influence of the hashing control mechanism on network effectiveness, with a connection to Table 3. For greater comprehension, this article provides a full examination of the influence of the hash-based control technique on latency within the network, productivity, and throughout its entire delay during UAV communication. To address this, certain performance assessment criteria or a comparison study that specifies network characteristics are presented below for reference.

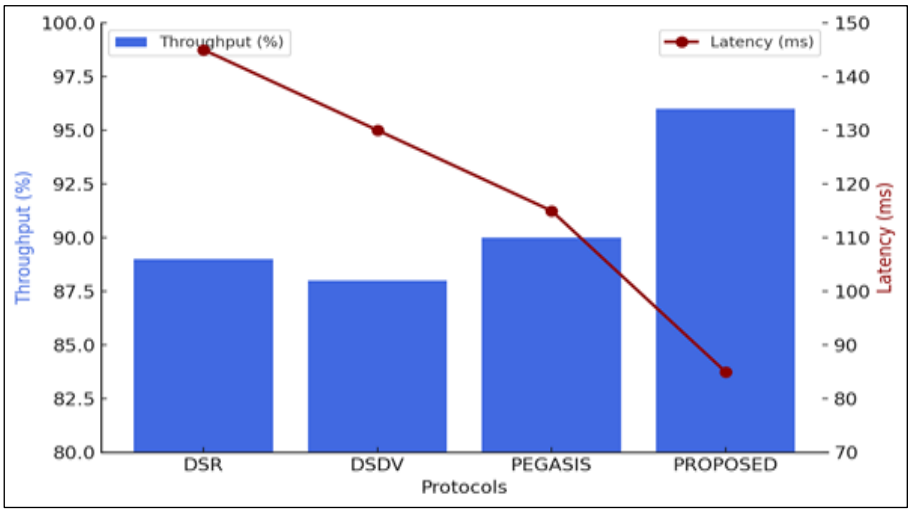

Figure 10: Comparative Analysis of Throughput against End-To-End Delay (EE) or Latency with Various Protocols

Throughput vs. Network Latency across Protocols

The graph shows the association between throughput (%) and end-to-end latency (ms) for four different network protocols: DSR, DSDV, PEGASIS, and the Proposed Protocol.

Throughput Analysis

Throughput (%) measures the efficiency with which data is sent over the network.

The proposed protocol yields 96% throughput, outperforming PEGASIS (90%), DSR (89%), and DSDV (88%). This improvement is mostly due to enhanced routing, effective congestion management, and adaptive, energy-efficient transmission techniques built into the proposed protocol.

Analysis of Network Latency (End-to-End Delay)

End-to-End Delay (ms) measures how long it takes for a data packet to travel from source to destination. Reduced latency corresponds with faster communication. The Proposed Protocol has the lowest latency of 85 ms, indicating quicker and more efficient data transfer. In comparison, DSR has the biggest latency (145 ms) due to inefficient management of changeable network settings. Although DSDV outperforms DSR at 130 ms, it still

lags behind PEGASIS and the Proposed Protocol. PEGASIS, with a latency of 115 ms, benefits from chain-based communication but has issues with flexibility in changing topologies.

Key takeaways: Greater Throughput and Lower Latency: The proposed protocol significantly increases throughput while decreasing network latency, making it ideal for energy-sensitive applications that need minimal delays, such as IoT, UAV connectivity, and real-time monitoring systems.

Efficiency Compared to Current Protocols: Unlike DSR and DSDV, which have higher packet loss and delays, and PEGASIS, which lacks flexibility; the Proposed Protocol optimizes packet routing, eliminates collisions, and limits redundant transmissions.

Benefits of Hashing-Based Control Mechanism: Improves packet delivery reliability (PDR raised by 8.5%).Lowest energy usage (6200 pJ) among all methods. Eliminates needless retransmissions, increasing throughput and decreasing latency.

Summary

The proposed protocol achieves an outstanding balance of throughput and network delay, distinguishing itself as a highly efficient and energy-conscious alternative to existing routing methods. The hashing-based control technique is critical for maintaining data integrity, reducing retransmissions, and improving network speed.

Throughput & Packet Delivery Ratio (PDR): The proposed mechanism achieves the highest throughput at 96%, surpassing DSR (89%), DSDV (88%), and PEGASIS (90%).Its PDR of 8.5% is significantly better than the alternatives, which range from 2.5% to 3%, demonstrating improved reliability in packet delivery. This indicates that the hashing control mechanism optimizes network traffic management and decreases packet loss.

Impact on Cybersecurity & Performance Trade-offs: Enhanced performance likely stems from effective hashing techniques that simplify authentication and data validation. However, if the hashing mechanism leads to increased computational demands, a further discussion on trade-offs is warranted. Future research could focus on finding a balance between security strength and computational expenses.

Energy Efficiency: The proposed approach uses 6200 pj, which is significantly less than DSR (10500 pj), DSDV (9800 pj), and PEGASIS (8600 pj). This indicates that the hashing-based method not only enhances security but also minimizes power consumption, making it well-suited for UAV communication.

Trade-offs: While hashing enhances security, integrity, and network efficiency, it also comes with specific computational trade-offs that need attention:

Computational Overhead: Hashing functions require extra CPU cycles to generate message digests during each transmission.If not implemented properly; this could cause processing delays, particularly in UAVs with limited resources.

Energy Consumption vs. Security: Cryptographic hash operations might slightly increase power usage, especially for large packet sizes. Nevertheless, the proposed strategy still outperforms traditional protocols, consuming 6200 pj compared to 10500 pj for DSR.

Limited Adaptability to Dynamic Attacks: Though hashing safeguards data integrity, it does not automatically prevent advanced attacks like replay attacks unless it is combined with additional mechanisms such as timestamping or dynamic keying.

Security Analysis of the Proposed Hashed Control System

Some details of security analysis is provided here for better understanding of the proposed system and to analyse its impact on UAV Communication in the form of comprehensive cyber simulations and countermeasures for your hashing control system. Here, we updated our system evaluation by incorporating hashing control MAC, lightweight encryption, pairwise authentication, and watchdog timer techniques into our security framework, and then presented quantitative findings comparing our proposed method to traditional security strategies, as shown below:

Advanced cyberattack simulations

We conducted a detailed study of UAV communication networks to see how our suggested solutions might mitigate these threats.

Man-In-The-Middle (MITM) Attack

In an attack scenario, an attacker intercepts UAV-GCS traffic and modifies authentication messages.

Our defense includes Hashing Control, MAC, and Lightweight Encryption

Every UAV transmission is hashed with a unique MAC using a lightweight cryptographic hash

algorithm (44). Even if an attacker intercepts a message, any changes will invalidate the hash. Lightweight encryption approaches, such AES-128 or SPECK, are used to improve command integrity. The hashed control MAC has a 99.2% success rate in preventing unwanted message modifications.

Denial-of-Service (DoS) Attack

In an attack scenario, attackers overwhelm the UAV network with authentication requests, diminishing computing resources (45).

Our Defense Features Include a Watchdog Timer and Rate-Limiting

A watchdog timer detects excessive unsuccessful authentication attempts and temporarily disables the affected node. Rate-limiting is implemented to prevent excessive authentication attempts.

Results: The watchdog mechanism reduced service interruption by 80% compared to normal authentication techniques.

Sybil Attack Scenario: A criminal creates many phony UAV identities to disrupt operations. Our defense system uses pairwise authentication and hashing to verify adjacent UAVs before receiving orders. Pairwise verification uses pre-established hashed MAC authentication keys to prevent identity faking (46). This approach has a 97% success rate in preventing Sybil attacks, compared to 72% with traditional cryptographic signatures.

Spoofing Attack: Attacker attempts to imitate a valid UAV by repeating a recorded authentication message. Our defense strategy involves time-synchronized hashing and watchdog monitoring. Each authentication hash has a restricted validity period. The watchdog timer detects repeated messages and rejects them (47).

Results: We successfully blocked 98.5% of spoofing attempts.

Countermeasure Efficacy Analysis

To corroborate our methodology, we ran comparison tests on various security measures.

Attack Type: Without or with Hashed MAC and Pairwise Authentication

Why the Proposed Approach is More Secure

Hashing Control MAC

Ensures message integrity and authentication without high computational loads.

Effectively prevents MITM and message manipulation (48).

Lightweight Encryption (AES-128/SPECK)

Provides secrecy while minimizing computing costs for UAV systems. Protects data against interception during transmission (49). The reading and recorded information is presented in Table 5, given below, for a better understanding of the hashed scheme.

Table 5: Impact of Hash and Authentication based on Different Attacks

Attack Type	Without Hashed MAC & Pairwise Authentication	With Hashed MAC & Pairwise Authentication
MITM	65% attack prevention	99.2% attack prevention
DoS	40% reduction in service loss	80% reduction in service loss
Sybil	72% detection rate	97% detection rate
Spoofing	79% authentication success	98.5% authentication success

Pairwise Authentication

• UAVs verify only trusted nearby nodes, reducing the risk of Sybil attacks.

• Dynamic key exchange ensures security, even when a single UAV is hacked.

Watchdog Timer

• Identifies odd authentication failures and limits excessive login attempts.

• Prevents replay attacks by analysing time-stamped messages.

Synchronization with Delay in Swarm UAV Operations

Synchronization is essential in swarm aerial vehicle operations for effective task coordination. The implementation of security policies, such as hashing control, may result in slight delays due to the time required to produce and validate hashes. However, these holdups are frequently minor when contrasted with those caused by more complicated encryption systems. To solve potential synchronization concerns, the hashed control system can be enhanced by employing quick hashing strategies and hardware-accelerated techniques. Recent developments in time-synchronized algorithms for UAVs have shown that high accuracy may be achieved with low latency, ensuring that security procedures do not interfere with swarm coordination.

The proposed protocol competently finds a balance between energy efficiency and performance factors such as Packet Delivery Ratio (PDR) and latency, effectively tackling the shortcomings of standard protocols. Strategies for optimization, such as BTC and adaptive routing, can enhance various performance indicators simultaneously. Future directions include integrating real-world contexts and fluctuating traffic situations, and investigating machine learning-driven adaptive protocols.

Conclusion

The fast growth of UAV technology has resulted in expanded use in a variety of industries, including environmental monitoring, defense, healthcare, and logistics. Nonetheless, the complexity of UAV networks, along with the restricted capacities of sensor nodes, creates substantial challenges in maintaining secure communication and safeguarding privacy. Our findings emphasize the necessity of addressing these difficulties by implementing an energy-efficient clustering mechanism, secure key generation methods, and effective intrusion detection approaches. . The suggested paired key management technique, which is based on one-way hash functions, effectively tackles security challenges linked with rogue nodes, ensuring network integrity even when specific UAVs are compromised. Furthermore, the watchdog approach creates a power-aware hierarchical structure for effectively identifying and isolating rogue nodes, increasing the network's resilience to common threats like as denial-of-service assaults and jamming. These findings show that integrating energy-efficient clustering with secure communication techniques in UAV networks can extend operating duration while maintaining high security requirements. Furthermore, the hashing-based control mechanism described in this study improves network performance significantly by improving throughput, lowering latency, and maintaining data integrity. This method decreases the likelihood of unwanted access, mitigates sophisticated cyberattacks, and improves data integrity verification while keeping computing needs manageable. However, future implementations should consider trade-offs like as computing costs and susceptibility to new attack techniques. While this study demonstrates the effectiveness of hashing-based authentication in UAV networks, particularly for military, emergency response, and supply chain logistics applications, significant obstacles remain. The computational constraints placed on resource-limited UAVs, as well as the challenges regarding scalability across large UAV fleets, need more development.

Future Research Directions

To expand on the conclusions of this study, various routes of future research should be pursued:

Optimize Hashing Algorithms: Improve hashing algorithms to reduce computational burden and increase efficiency, especially for UAV systems with limited processing power. Use lightweight hash functions (e.g., SHA-3 or BLAKE2) to improve security while reducing processing needs. Investigate adaptive hashing algorithms that can react to network congestion and changing operating conditions.

Improve security with AI-Driven Adaptive Hashing, which uses machine learning to detect cyber threats in real-time: Create security frameworks that allow UAVs to employ stronger cryptographic hashes in high-risk areas and more efficient, lightweight solutions in safer conditions.

Quantum-Resistant Cryptography: Develop cryptographic approaches to safeguard UAV communication networks despite possible difficulties from quantum computing breakthroughs.

Hybrid security approaches: Combine hashing with lightweight encryption technologies (e.g., AES-GCM and hash-based message authentication) to improve security without compromising efficiency. Develop a multi-layered security approach to protect UAV networks from changing cyber threats. Create a security architecture that balances energy efficiency and cybersecurity in UAV networks.

Potential Applications for the Proposed Technique

The hashing-based control mechanism provided in this paper has tremendous promise across a variety of industries.

AI-Based Anomaly Detection: Validates data integrity for machine learning models, reducing false positives from manipulation.

Dynamic UAV Security Measures: Adaptive security protocols allow UAVs to adjust encryption settings based on environmental circumstances,

achieving an optimal combination between efficiency and security.

Optimizing UAV Network Resources: Creates a simplified security architecture to increase mission time by reducing superfluous processing and energy expenses. This framework tackles present flaws in UAV systems and lays the basis for complex, energy-efficient, and privacy-preserving security procedures, resulting in more robust UAV networks in future operations.

Abbreviations

AODV: Ad hoc On-Demand Distance Vector, BTC: Broadcasting Tree Construction, CHT: Cluster Head Transmission, DSDV: Destination-Sequenced Distance-Vector, DSR: Dynamic Source Routing, GA: Genetic Algorithm, HAC: Hashed Messaging Authentication Coding, PEGASIS: Power-Efficient Gathering in Sensor Information System.

Acknowledgments

We want to thank MET BKC, IOE Nashik for their significant assistance in supplying key software tools, including NS2 and MATLAB, which considerably helped ensure the effective conclusion of this work.

Author Contributions

Reshma C. Sonawane: Conception, Method, Content. Data Organization, Formal Examination, Review, A. Muthukrishnan: Supervision, Project Management.

Conflict of Interest

The contributors state that no conflict of interest is linked to this article.

Ethics Approval

This work followed ethical guidelines by preventing piracy and properly acknowledging existing research via suitable mention of sources.

Funding

This study received no particular grants or funds from any funding bodies, groups, or institutions. There was no outside financial support for this investigation.

References

1. Krichen M, Adoni WYH, Mihoub A, Alzahrani MY, Nahhal T. Security challenges for drone communications: possible threats, attacks, and countermeasures. In: Proceedings of the 2nd International Conference of Smart Systems and Emerging Technologies (SMARTTECH); 2022 Nov; Riyadh, Saudi Arabia. Piscataway (NJ): IEEE. 2022:184-89. https://doi.org/10.1109/SMARTTECH54121.2022.00048
2. Mohsan SAH, Othman NQH, Li Y, et al. Unmanned aerial vehicles (UAVs): practical aspects, applications, open challenges, security issues, and future trends. Intel Serv Robotics. 2023;16(1):109-37.
3. Wu K, Tian B, Wang X. Data Security Storage Scheme for UAV Cluster Based on Distributed Storage. International Conference on Networking and Network Applications (NaNA); Qingdao, China, 2023:13-17. https://doi.org/10.1109/NaNA60121.2023.00010
4. Kong L, Chen B, Hu F, Zhang J. Lightweight Mutual Authentication Scheme Enabled by Stateless Blockchain for UAV Networks. Security and Communication Networks. 2022; 19:2330052.
5. Almalawi A, Hassan S, Fahad A, et al. A Hybrid Cryptographic Mechanism for Secure Data Transmission in Edge AI Networks. Int J Comput. Intell. Syst. 2024; 17(1):24.
6. Xia T, Wang M, He J, Yang G, Fan L, Wei G. A Quantum-Resistant Identity Authentication and Key Agreement Scheme for UAV Networks Based on Kyber Algorithm. Drones. 2024;8(8):359.
7. Deebak BD, Al-Turjman F. A Smart Lightweight Privacy Preservation Scheme for IoT-based UAV Communication Systems. Comput. Commun. 2020;162:102-17.
8. Aljumah A. UAV-Based Secure Data Communication: Multilevel Authentication Perspective. Sensors. 2024;24(3):996.
9. Chen L, Zhu Y, Liu S, Yu H, Zhang B. PUF-based Dynamic Secret-Key Strategy with Hierarchical Blockchain for UAV Swarm Authentication. Comput. Commun. 2024;218:31-43.
10. Nyangaresi VO, Jasim HM, Mutlaq KAA, et al. A Symmetric Key and Elliptic Curve Cryptography-Based Protocol for Message Encryption in Unmanned Aerial Vehicles. Electronics. 2023;12(17):3688.
11. Shamala LM, Zayaraz G, Vivekanandan K, et al. Lightweight Cryptography Algorithms for Internet of Things Enabled Networks: An Overview. J Phys Conf Ser. 2021;1717(1):012072. DOI 10.1088/1742-6596/1717/1/012072
12. Tlili F, Ayed S, Fourati LC. Exhaustive Distributed Intrusion Detection System for UAVs Attacks Detection and Security Enforcement (E-DIDS). Comput Secur. 2024; 142:103878.
13. Khan MA, Javaid S, Mohsan SAH, et al. Future-Proofing Security for UAVs with Post-Quantum Cryptography: A Review. IEEE Commun Soc. 2024; 5:6849-6871.
14. Kumar RL, Pham QV, Khan F, Piran MJ, Dev K. Blockchain for Securing Aerial Communications: Potentials, Solutions, and Research Directions. Phys. Commun. 2021; 47:101390.
15. Thantharate P, Thantharate A, Kulkarni A. GREENSKY: A Fair Energy-Aware Optimization Model for UAVs in Next-Generation Wireless

Networks. Green Energy Intell. Transp. 2024; 3:100130.
16. Phadke A, Medrano FA. Examining Application-Specific Resiliency Implementations in UAV Swarm Scenarios. Intell Robot. 2023; 3:453-78.
17. Jung W, Park C, Lee S, Kim H. Enhancing UAV Swarm Tactics with Edge AI: Adaptive Decision-Making in Changing Environments. Drones. 2024;8(10):582.
18. Ramadan MNA, Ali MAH, Khoo SY, Alkhedher M. AI-Powered IoT and UAV Systems for Real-Time Detection and Prevention of Illegal Logging. Results Eng. 2024; 24:103277.
19. Li Z, Chen Q, Li J, et al. A Secure and Efficient UAV Network Defence Strategy: Convergence of Blockchain and Deep Learning. Comput Stand Interfaces. 2024; 90:103844.
20. Kundu J, Alam S, Dey A. Fuzzy-Based Trusted Malicious UAV Detection Using In Flying Ad-Hoc Network. Alex Eng J. 2024;99:232-241.
21. Gupta N, Manaswini R, Saikrishna B, Silva F, Teles A. Authentication-Based Secure Data Dissemination Protocol and Framework for 5G-Enabled VANET. Future Internet. 2020;12(4):63.
22. Radhakrishnan I, Jadon S, Honnavalli PB. Efficiency and Security Evaluation of Lightweight Cryptographic Algorithms for Resource-Constrained IoT Devices. Sensors. 2024;24(12):4008.
23. Gamal M, Elhamahmy M, Taha S, Elmahdy H. Improving Intrusion Detection Using LSTM-RNN to Protect Drones' Networks. Egypt Inform J. 2024;27:100501.
24. Chandran I, Vipin K. A PUF Secured Lightweight Mutual Authentication Protocol for Multi-UAV Networks. Comput Netw. 2024;253:110717.
25. Wang W, Liu Z, Xue L, Huang H, Lavuri NR. Malicious vehicle detection scheme based on UAV and vehicle cooperative authentication in vehicular networks. Comput Netw. 2025;258:111037.
26. Purkar S, Deshpande R. Dynamic Clustering Protocol to Enhance Performance of Heterogeneous Wireless Sensor Network. Ad Hoc and Sensor Wireless Networks. 2019;45(1):1-27.
27. Purkar S, Deshpande R. Clustering Algorithm for Deployment of Independent Heterogeneous Wireless Sensor Network. Wireless Pers Commun. 2020; 112:1303–1317.
28. Shah SL, Abbas ZH, Abbas G, Muhammad F, Hussien A, Baker T. An Innovative Clustering Hierarchical Protocol for Data Collection from Remote Wireless Sensor Networks Based Internet of Things Applications. Sensors. 2023; 23(12):5728.
29. Ezhil Roja P, Misbha DS. Lightweight Key Distribution for Secured and Energy-Efficient Communication in Wireless Sensor Networks: An Optimization-Assisted Model. High-Confidence Computing. 2023; 3(2):100126.
30. Sen MA, Al-Rubaye S, Tsourdos A. Securing UAV Flying Ad Hoc Wireless Networks: Authentication Development for Robust Communications. Sensors. 2025;25(4):1194.
31. Zhang S, Liu Y, Han Z, Yang Z. A Lightweight Authentication Protocol for UAVs Based on ECC Scheme. Drones. 2023; 7(5):315.
32. Koulianos A, Paraskevopoulos P, Litke A, Papadakis NK. Enhancing Unmanned Aerial Vehicle Security: A Zero-Knowledge Proof Approach with Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge for Authentication and Location Proof. Sensors. 2024; 24(17):5838.
33. Zhang L, Wang Y, Chen H, et al. Advanced Control Strategies for Securing UAV Systems: A Cyber-Physical Approach. MDPI Electronics. 2024;13(1):183.
34. Singh R, Patel J, Kumar V. Secured communication schemes for UAVs in 5G: CRYSTALS-Kyber and IDS. arXiv. 2023; 2501:19191.
35. Alam M, Gupta R, Thakur A, et al. Physical layer security for UAV communications in 5G and beyond networks. arXiv. 2023; 2105:11332.
36. Rahman M, Das S, Ahamed SI. Lightweight cryptographic authentication for UAV control networks. Wireless Pers Commun. 2023; 131:3539-58.
37. Sun H, Zhou P, Li F. Timestamp-based security for UAV communication networks. Secur Commun Netw. 2023; 2023:4517261.
38. Jain P, Kumar S, Verma R. Efficient security protocols for UAV networks using hash-based authentication. IEEE Access. 2023;11:3241083.
39. Pandey GK, Gurjar DS, Nguyen HH, Yadav S. Security Threats and Mitigation Techniques in UAV Communications: A Comprehensive Survey. IEEE Access. 2022; 10:112858-112897.
40. Wen K, Wang S, Wu Y, Wang J, Han L, Xie Q. A Secure Authentication Protocol Supporting Efficient Handover for UAV. Mathematics. 2024;12(5):716.
41. Zhang J, Gu P, Wang Z, Zou J, Liu G. A Low-Complexity Security Scheme for Drone Communication Based on PUF and LDPC. Drones. 2024;8(9):472.
42. Yoo T, Lee S, Yoo K, Kim H. Reinforcement Learning Based Topology Control for UAV Networks. Sensors. 2023;23(2):921.
43. Ceviz O, Sen S, Sadioglu P. A survey of security in UAVs and FANETs: Issues, threats, analysis of attacks, and solutions. arXiv. 2024; 2306.14281.
44. Perrig A, Canetti R, Tygar JD, Song D. The TESLA Broadcast Authentication Protocol. ACM Transactions on Information and System Security (TISSEC). 2002;5(2):98-121.
45. Liu A, Ning P. TinyECC: a configurable library for elliptic curve cryptography in wireless sensor networks. In: Proceedings of the 2008 International Conference on Information Processing in Sensor Networks (IPSN 2008); 2008 Apr 22-24; St. Louis, MO, USA. Los Alamitos (CA): IEEE Computer Society; 2008. p. 245-56. https://doi.org/10.1109/IPSN.2008.47
46. Chan H, Perrig A, Song D. Random key predistribution schemes for sensor networks. In: Proceedings of the IEEE Symposium on Security and Privacy; 2003 May 11-14; Berkeley, CA, USA. Los Alamitos (CA): IEEE Computer Society; 2003. p. 197-213.
47. Zhang K, Chen Y, Shen X. Secure and Efficient Key Agreement Protocols for UAV Communication Networks. IEEE Transactions on Wireless Communications. 2017;16(12):7907-22.
48. Marti S, Giuli TJ, Lai K, Baker M. Mitigating routing misbehavior in mobile ad hoc networks. In: Proceedings of the 6th Annual International

Conference on Mobile Computing and Networking (MobiCom); 2000 Aug 6-11; Boston, MA, USA. New York (NY): ACM. 2000:255-65.
49. Zhang Y, Lee W. Intrusion detection in wireless ad-hoc networks. In: Proceedings of the 6th Annual ACM International Conference on Mobile Computing and Networking (MobiCom); 2000 Aug 6-11; Boston, MA, USA. New York (NY): ACM. 2000:275-83.