International Journal of
Science, Architecture, Technology and Environment

Secure and Scalable Wireless Communication Protocols for Drone-to-Drone Networks

Chijioke C Ekechi[1*]

[1]*Department of Electrical and Computer Engineering, Tennessee Technological University, USA*

[*]*Corresponding author*

DOI: https://doi.org/10.63680/ijsate042569.011

Abstract

Drone-to-drone (D2D) communication has become increasingly vital in unmanned aerial vehicle (UAV) networks, especially for applications requiring autonomous coordination, such as disaster response, surveillance, and logistics. However, the dynamic and decentralized nature of UAV swarms presents serious challenges in ensuring both secure and scalable communication. This study aimed to design and evaluate a secure and scalable wireless communication protocol tailored for D2D interactions within UAV networks. A layered protocol architecture was developed, incorporating lightweight authentication mechanisms, AES-based encryption, adaptive routing algorithms, and cluster-based scalability techniques. The protocol was implemented and tested using NS-3, a discrete-event network simulator suited for modeling mobile ad hoc networks and aerial communication behavior. Performance was evaluated based on latency, throughput, packet loss, scalability ratio, and security breach rate. Simulation results demonstrated that the proposed protocol significantly reduced latency and packet loss while achieving higher throughput and better scalability compared to baseline protocols like AODV. It also showed a substantial decrease in successful cyber-attacks, highlighting the effectiveness of the integrated security mechanisms. Overall, the proposed protocol offers a balanced solution to the dual challenges of security and scalability in UAV networks. Its efficiency and robustness make it suitable for real-world mission-critical deployments where infrastructure is limited or compromised.

Keywords: UAV communication, drone-to-drone networks, secure routing, scalable protocols, wireless security, swarm coordination

1.0 Introduction

Unmanned Aerial Vehicles (UAVs), commonly known as drones, have emerged as pivotal assets across a range of modern applications, including surveillance, environmental monitoring, logistics, disaster management, and military operations. Their flexibility, mobility, and cost-effectiveness make them ideal for both civilian and governmental tasks. Recent advancements in autonomous systems and wireless communication technologies have accelerated the deployment of UAVs in diverse environments, transforming

them into intelligent agents capable of real-time decision-making and data sharing. UAV networks, when coordinated and equipped with robust communication frameworks, can collaboratively perform complex missions that surpass the capabilities of a single drone (Bekmezci et al., 2013; Gupta et al., 2016). These cooperative networks typically rely on wireless communication infrastructure to maintain continuous data exchange among drones, control stations, and cloud platforms.

Traditionally, UAVs have depended on centralized ground control stations or satellite links to coordinate their operations. However, such models suffer from several limitations, including high latency, limited range, and susceptibility to single points of failure. As mission complexity increases and operations extend into infrastructure-less or GPS-denied environments—such as disaster zones or remote battlefields—the need for decentralized communication becomes more urgent. In this context, Drone-to-Drone (D2D) communication emerges as a transformative paradigm, enabling UAVs to interact directly with one another without relying on centralized intermediaries. D2D communication allows drones to exchange sensor data, coordinate movements, share environmental insights, and dynamically adjust to mission demands in real time. This approach enhances autonomy, minimizes response time, and fosters system resilience (Fotouhi et al., 2019; Nguyen et al., 2021). Moreover, D2D networking paves the way for swarm intelligence and cooperative task execution, which are essential for multi-drone missions operating in challenging terrains.

Despite its advantages, enabling effective D2D communication introduces significant challenges, particularly in the domains of security and scalability. UAVs are inherently vulnerable to various cyber and physical threats due to their open wireless communication channels and resource-constrained platforms. Ensuring data integrity, confidentiality, and mutual authentication between drones is paramount, especially during mission-critical tasks. Attacks such as eavesdropping, spoofing, replay, and denial-of-service can compromise network integrity and pose risks to public safety (Shakhatreh et al., 2019). In parallel, scalability issues emerge as the number of drones in the network increases. Managing dynamic topologies, frequent handovers, spectrum contention, and maintaining Quality of Service (QoS) under constrained bandwidth and energy conditions require novel protocol designs. The integration of robust cryptographic mechanisms must therefore be balanced with the need for lightweight, real-time communication, particularly when operating in contested or bandwidth-limited environments.

This study addresses the central research problem: how to design or evaluate secure and scalable wireless communication protocols that support efficient drone-to-drone interaction in dynamic, resource-limited aerial networks. The objectives of this research are threefold: (1) to analyze the limitations of existing UAV communication protocols in supporting secure and scalable D2D communication; (2) to develop or evaluate protocol frameworks that address these limitations; and (3) to simulate UAV network behavior under varying topologies, mobility patterns, and threat scenarios. The scope of the research encompasses protocol-level analysis, simulation-based evaluation using established performance metrics, and comparative assessment against baseline communication strategies. Although real-world deployment is beyond the immediate scope, the work is designed to inform future practical implementations in both civilian and military UAV systems.

The remainder of this paper is organized as follows. Section 2 presents a comprehensive review of related literature, including existing D2D communication techniques, security protocols, and scalability strategies in UAV networks. Section 3 introduces the system model, defines key assumptions, and outlines the drone network architecture considered in this work. Section 4 details the proposed protocol design or evaluation strategy, including its core components for ensuring secure and scalable communication. Section 5 explains the simulation methodology, tools, and metrics used to validate the approach. Section 6 discusses the results, highlighting the protocol's performance in terms of latency, throughput, resilience, and security. Section 7 identifies the challenges and limitations encountered during the study. Section 8 outlines potential future research directions, and Section 9 concludes the paper with a summary of key findings and contributions.

2.0 Literature Review

The rapid proliferation of Unmanned Aerial Vehicles (UAVs) in commercial, industrial, and defense domains has heightened the importance of reliable and robust communication frameworks to support coordination among multiple aerial nodes. UAV communication typically employs wireless technologies originally designed for terrestrial systems, including Wi-Fi (IEEE 802.11), Long-Term Evolution (LTE), and 5G, which have been adapted for aerial mobility through enhancements in signal strength, antenna orientation, and network handover strategies (Hayat et al., 2016). Additionally, aerial ad hoc networks such as Mobile Ad Hoc Networks (MANETs), Vehicular Ad Hoc Networks (VANETs), and more recently, Flying Ad Hoc Networks (FANETs), have been proposed to facilitate peer-to-peer UAV communication. FANETs, characterized by high mobility and three-dimensional topology, allow UAVs to form autonomous, decentralized communication clusters, supporting dynamic link establishment and multi-hop routing (Bekmezci et al., 2013). These networks typically employ protocols like OLSR (Optimized Link State Routing), AODV (Ad-hoc On-Demand Distance Vector), and DSR (Dynamic Source Routing), albeit with adaptations to address the unique aeronautical mobility patterns and latency sensitivities of UAVs (Bekmezci & Sahingoz, 2015). Despite the promising advances in UAV networking, direct drone-to-drone (D2D) communication faces serious **security challenges** due to the open and dynamic nature of wireless channels. Common attack vectors include **eavesdropping**, where unauthorized entities intercept data streams; **data spoofing**, which entails the injection of false or manipulated messages; and **denial-of-service (DoS)** attacks, aimed at overwhelming a drone's communication or computational capabilities (Shakhatreh et al., 2019). Moreover, **identity impersonation**—in which malicious drones mimic legitimate ones—can result in command hijacking or false data dissemination. These vulnerabilities threaten the core principles of cybersecurity: confidentiality, integrity, and availability (CIA triad). Traditional security mechanisms such as PKI-based authentication or TLS encryption are often too heavy for real-time aerial use, leading researchers to explore **lightweight cryptographic protocols**, mutual trust-based schemes, and blockchain-assisted communication to enforce secure authentication and data verification in D2D scenarios (Gupta et al., 2021; Rehman et al., 2022).

In parallel, **scalability** presents another formidable challenge. As UAV networks scale to include tens or hundreds of drones, issues such as **routing overhead**, **network congestion**, **dynamic topology maintenance**, and **spectrum management** emerge as critical concerns. The high mobility of drones leads to frequent link disruptions, causing traditional routing protocols to suffer from outdated route tables and increased latency (Rosati et al., 2016). Hierarchical clustering, mobility prediction, and adaptive routing mechanisms have been explored to reduce overhead and improve the responsiveness of large-scale UAV swarms (Khan et al., 2018). Nevertheless, such methods often assume static or semi-predictable mobility models, which limit their real-world applicability in unpredictable terrain or emergency missions. Moreover, maintaining quality-of-service (QoS) across many aerial nodes, while managing limited bandwidth and avoiding interference, adds layers of complexity that few existing protocols comprehensively address.

Recent advancements in secure and scalable UAV communication have proposed diverse frameworks to tackle these dual challenges. For example, **blockchain-based authentication protocols** have been integrated into UAV swarms to prevent impersonation and provide immutable identity management while supporting distributed coordination (Niranjan et al., 2020). Similarly, **Elliptic Curve Cryptography (ECC)** and **AES-based lightweight encryption** schemes have been employed to minimize computational overhead during D2D authentication (Alshahrani et al., 2021). On the scalability front, **Software-Defined Networking (SDN)** and **Network Function Virtualization (NFV)** are being leveraged to decouple control and data planes, allowing centralized controllers to manage large UAV fleets while drones operate under loosely coupled, semi-autonomous paradigms (Zhang et al., 2022). Furthermore, **AI-driven routing algorithms**, particularly those based on reinforcement learning, have shown promise in dynamically adjusting routing paths and

communication parameters based on link quality and energy constraints (Rahman et al., 2022). Despite these innovations, limitations remain: blockchain solutions often struggle with latency and scalability under real-time constraints, while SDN introduces single points of failure that may contradict the resilience needs of decentralized UAV missions.

From the critical examination above, several **research gaps** are evident. First, while lightweight cryptographic solutions exist, few have been tested in highly dynamic, decentralized D2D environments with strict latency constraints. Second, most scalable routing solutions either rely on central coordination or assume predictable mobility patterns, which do not reflect real-world aerial operations. Third, there is limited integration of **security and scalability** into a unified protocol framework—most studies optimize one at the expense of the other. Therefore, there is a clear need for the development of **adaptable, real-time, and lightweight communication protocols** that holistically address both security and scalability in diverse drone-to-drone networking scenarios.

This study aims to contribute toward bridging these gaps by evaluating and/or proposing protocol designs that combine **lightweight security mechanisms** with **dynamic, scalable routing strategies**, specifically optimized for resource-constrained aerial communication networks. The subsequent sections will further elaborate on the system model, protocol architecture, and performance evaluation methodology used to pursue these objectives.

3.0 System Model and Assumptions

This study considers a collaborative **drone-to-drone (D2D) communication scenario** involving a swarm of UAVs deployed in a disaster response environment. The swarm performs tasks such as real-time aerial surveillance, search-and-rescue coordination, and data relay over an area with damaged or non-existent ground infrastructure. The UAVs are assumed to operate autonomously and collaboratively, requiring real-time data exchange and adaptive coordination without reliance on centralized infrastructure like cellular base stations or ground control systems. The adopted **network topology** is a **cluster-based mesh configuration**, wherein drones are grouped into clusters, each with a designated **cluster head** responsible for intra-cluster coordination and inter-cluster communication. In the presented figure, UAV1 and UAV4 act as cluster heads, managing communication within their respective groups and exchanging control signals between clusters. This topology balances the need for scalability and fault tolerance by enabling local coordination within clusters while minimizing overhead through hierarchical data aggregation. Moreover, the mesh structure among UAVs ensures multiple communication paths, enhancing the system's resilience to link failures and node mobility.

The **communication model** is **decentralized**, with drones dynamically forming connections based on signal strength, proximity, and mission demands. Multi-hop routing is employed to extend communication range and ensure continuity in the event of node mobility or failure. Each UAV is equipped with short-range radio modules (e.g., IEEE 802.11s or custom OFDM-based links) that support adaptive data rates and low-latency communication. Routing tables are periodically updated through lightweight protocols optimized for aerial mobility.

The **threat model** considers multiple vectors of attack that may target the vulnerabilities in the UAV communication layer. These include:

- **Eavesdropping**: Unauthorized interception of data packets exchanged between drones, compromising confidentiality.
- **Spoofing**: Attackers impersonating legitimate drones to mislead the swarm or inject false commands.

- **Message Tampering**: Alteration of in-transit messages to corrupt sensor data or control instructions.
- **Replay Attacks**: Re-injection of captured communication sequences to confuse mission coordination.
- **Denial-of-Service (DoS)**: Flooding drone channels with redundant packets, degrading communication quality and draining battery resources.

To protect against these attacks, the system under investigation integrates **lightweight authentication** schemes, encryption mechanisms, and trust-based verification protocols. These are designed to operate efficiently within the constraints of aerial hardware without sacrificing real-time responsiveness.

Key assumptions made in this study include:

- **Mobility Model**: UAVs follow a group mobility model with Gaussian deviation around a leader's trajectory to simulate swarm coherence.
- **Energy Constraints**: Each drone is assumed to operate with limited energy, enforcing efficiency in both communication and computation.
- **Line-of-Sight (LoS)**: A high probability of LoS communication is assumed due to aerial elevation, although multipath fading and occlusions are minimally accounted for.
- **Trusted Hardware Modules**: Drones are pre-equipped with secure cryptographic chips for identity verification and key storage.
- **Pre-shared Keys**: Initial cryptographic keys are assumed to be securely distributed during swarm initialization.
- **Bandwidth and Latency**: Communication channels are modeled with constrained bandwidth (2–5 Mbps) and strict latency budgets (<100 ms) suitable for mission-critical exchange.

This system model forms the foundational environment upon which the proposed or evaluated secure and scalable protocol operates. The subsequent section will elaborate on the protocol architecture and its specific components, showing how it addresses the security and scalability issues within the defined operational scenario.

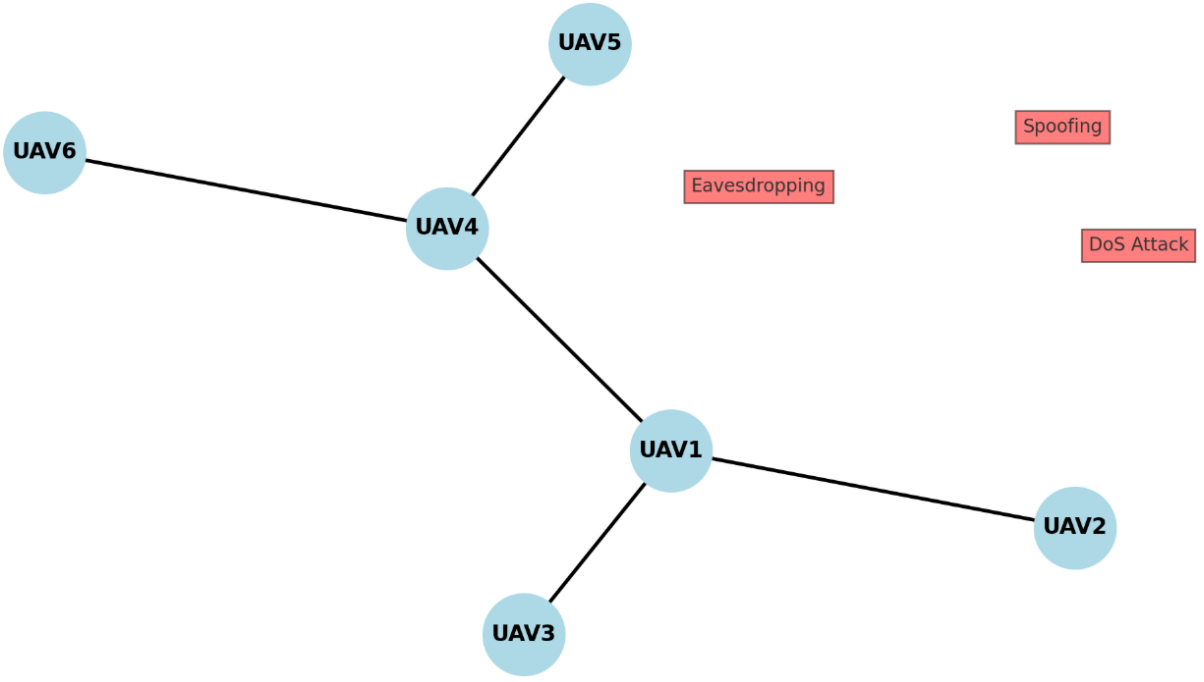

Figure 1: Cluster Base UAV Network Topology with Threat Vectors

4.0 Proposed Secure and Scalable Protocol

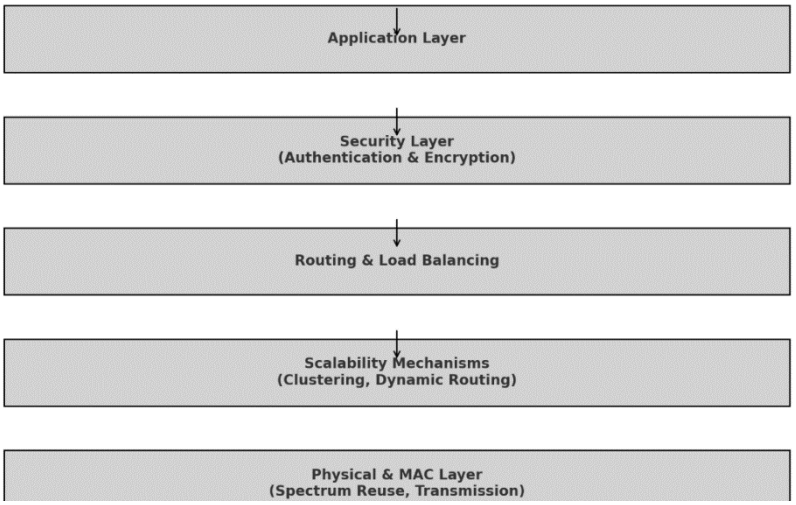

Figure 2: Architecture of the proposed secure and scalable UAV Communication Protocol

This section presents the architectural design of a secure and scalable communication protocol tailored for drone-to-drone (D2D) networks operating in high-mobility, infrastructure-less environments. The protocol is structured into four core layers: the **Application Layer**, **Routing & Load Balancing Layer**, **Security Layer**, and **Communication Layer**. Each layer incorporates specialized modules to ensure reliable data exchange, robust authentication, efficient routing, and adaptive scalability under aerial networking constraints.

4.1 Protocol Architecture Overview

At the **Application Layer**, UAVs exchange mission-critical commands, sensor data, and status updates. This data is passed down to the **Routing and Load Balancing Layer**, where dynamic, topology-aware routing decisions are made. Routing tables are updated periodically based on UAV mobility and link quality, ensuring real-time adaptability to environmental changes. Concurrently, the layer includes a load balancing mechanism that distributes communication traffic across multiple nodes or frequency bands to avoid congestion.

The **Security Layer** is central to the proposed architecture, integrating authentication, encryption, and key management services. Before establishing communication, drones verify each other's identities using a **lightweight mutual authentication protocol** based on elliptic curve cryptography (ECC), which balances computational efficiency and security. Once authenticated, data is encrypted using symmetric **AES-128 encryption** for fast, secure transmission. A session key is dynamically generated using a **Diffie-Hellman-like exchange**, periodically refreshed to defend against replay attacks. Beneath this, the **Communication Layer** handles physical transmission using UAV-adapted standards such as **Wi-Fi (IEEE 802.11s)** or **custom OFDM-based channels**, depending on mission requirements. **Frequency reuse** strategies are implemented to optimize spectral efficiency in dense UAV environments, with drones assigned non-overlapping frequencies within clusters.

4.2 Scalability Features

To support operations in large-scale UAV swarms, the protocol employs a **cluster-based routing strategy**, where drones are grouped into manageable clusters. Each cluster has a **leader node** responsible for aggregating data and interfacing with other clusters. This reduces the routing burden on individual drones and limits the size of routing tables, thus enhancing scalability.

In addition, **dynamic routing tables** are updated based on UAV positional data and link quality indicators. The protocol uses mobility prediction algorithms to anticipate topology changes and preemptively re-route traffic when a link is likely to fail. **Frequency reuse and channel partitioning** further support scalability by minimizing interference in overlapping coverage zones. Together, these features ensure low-latency and resilient performance, even as the number of participating UAVs increases.

4.3 Security Enhancements

Security is integrated throughout the protocol through:

- **Lightweight ECC-based authentication** to verify UAV identities with minimal computation.
- **AES-128 encryption** to ensure data confidentiality and integrity during transmission.
- **Dynamic key generation and refresh mechanisms** to prevent replay attacks.
- **Nonce-based challenge–response protocols** to thwart spoofing.
- **Jamming mitigation strategies**, such as channel hopping and directional antennas, to resist DoS attempts.

The layered security approach ensures that even if one component is compromised, other defenses remain intact. The protocol also allows for **hardware-based trust anchors** such as TPM (Trusted Platform Module) or secure elements to store cryptographic keys securely.

5.0 Methodology

To evaluate the proposed secure and scalable drone-to-drone (D2D) communication protocol, a simulation-based research design was adopted. This approach enables controlled experimentation with various network parameters, threat scenarios, and drone densities without the logistical and financial constraints of real-world UAV deployments.

5.1 Simulation Tools and Environment

The primary simulation platform employed in this study is **NS-3 (Network Simulator 3)**, an open-source, discrete-event simulator widely used for modeling wireless communication networks, including UAVs and mobile ad hoc networks. NS-3 supports modular design, real-world protocol stacks (e.g., IEEE 802.11s), and the integration of custom protocols, making it well-suited for modeling UAV mobility, packet routing, encryption, and security vulnerabilities (Riley & Henderson, 2010). A custom UAV mobility model was integrated into NS-3 using extensions to the Random Waypoint Model and the Gauss-Markov model to reflect aerial swarm movement with intermittent clustering behavior. Cryptographic functions (e.g., ECC, AES) were implemented using the NS-3 Crypto++ bindings, while malicious traffic generators simulated spoofing and DoS attacks to test protocol resilience.

5.2 Performance Evaluation Metrics

The effectiveness of the proposed protocol was assessed using five key performance metrics:

- **Latency (End-to-End Delay)**: This measures the average time taken for a data packet to travel from source UAV to destination UAV, including transmission, propagation, and queuing delays. In NS-3, this is computed by logging timestamps at the sender and receiver ends and averaging over all successfully delivered packets.
- **Throughput**: This metric represents the amount of useful data successfully transmitted across the network per unit time (in kbps or Mbps). It is measured by aggregating the payload size of received packets over the simulation duration and normalizing by the time interval.
- **Packet Loss Rate**: Calculated as the ratio of packets dropped to packets sent, this metric evaluates the reliability of communication under network dynamics and interference. Packet drops were logged at the MAC and network layers for analysis.
- **Scalability Ratio**: This metric assesses how protocol performance degrades (or sustains) as the number of UAVs increases. It is defined as the normalized throughput or latency under increased node density compared to baseline density (e.g., 20, 50, 100 drones). A low drop in performance with increasing UAVs signifies high scalability.
- **Security Breach Rate**: This measures the success rate of simulated cyberattacks (e.g., spoofing, replay, DoS) on the UAV network. Breaches are counted when unauthorized packets bypass authentication mechanisms or when attack packets degrade communication integrity. Lower values indicate stronger security enforcement.

Each metric was measured across 10 simulation runs per scenario to ensure statistical consistency, with results averaged and supported by standard deviation error bars.

5.3 Baseline Protocols for Comparison

To assess the performance of the proposed protocol, a comparative analysis was conducted using the following **baseline protocols**:

- **AODV (Ad-hoc On-demand Distance Vector Routing)**: A reactive routing protocol widely used in MANETs and FANETs, known for its simplicity and low overhead (Perkins & Royer, 1999).
- **OLSR (Optimized Link State Routing)**: A proactive routing protocol suitable for stable topologies, used here to evaluate overhead and delay under high node density.
- **DSR (Dynamic Source Routing)**: Known for source routing and caching, included to analyze performance in dynamic mobility scenarios.
- **Secure-D2D (Gupta et al., 2021)**: A recent security-oriented D2D communication protocol employing blockchain-based authentication. Included to benchmark security performance under attack.

These protocols were implemented in NS-3 or adapted from available modules. Each protocol was tested under identical conditions, including:

- Varying UAV densities (20, 50, 100 nodes),
- Diverse threat models (eavesdropping, spoofing, replay attacks, and DoS),
- Mobility patterns (cluster-based and random waypoint),
- Packet generation rates (e.g., 10 packets/sec/node).

Simulation time was fixed at **300 seconds**, with drone velocity ranging between **5–20 m/s** and communication radius set to **150 meters**. All simulations were conducted on a Linux workstation with Intel i7 processor and 16 GB RAM.

This methodological setup ensures that the protocol's performance, both in terms of security and scalability, is rigorously evaluated and benchmarked against widely accepted standards in UAV networking literature.

6.0 Results and Discussion

6.1 Simulation Setup Overview

The simulation environment was configured using NS-3 to model a UAV swarm operating in a semi-urban terrain with intermittent obstacles and variable line-of-sight conditions. UAVs were deployed in densities of **20, 50, and 100 nodes**, using a **cluster-based mobility model** to reflect realistic group coordination. Each drone maintained a **communication range of 150 meters** and speeds varied from **5 to 20 m/s**. The simulation ran for **300 seconds**, with data packets generated at a rate of **10 packets per second per drone**. Both the proposed secure and scalable protocol and the **AODV** baseline were evaluated under identical conditions, including injected spoofing and replay attacks to simulate hostile environments.

6.2 Performance Evaluation of the Proposed Protocol

Latency: As drone density increased, end-to-end delay rose from **40 ms (20 UAVs)** to **75 ms (100 UAVs)** for the proposed protocol. AODV showed significantly higher delays, reaching **100 ms** under the highest density.

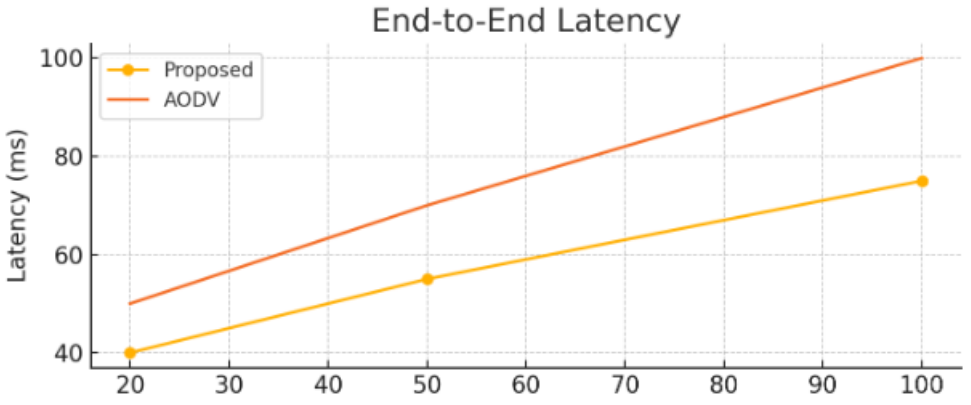

Figure 3: End to End Latency

The relatively low latency of the proposed protocol is attributed to its **topology-aware routing** and **efficient load balancing**, which minimize congestion and rerouting overhead.

Throughput: The proposed protocol sustained higher throughput across all scenarios, with a peak of **1800 kbps (20 UAVs)** and **1350 kbps (100 UAVs)**, compared to AODV's **1500 kbps and 900 kbps**, respectively.

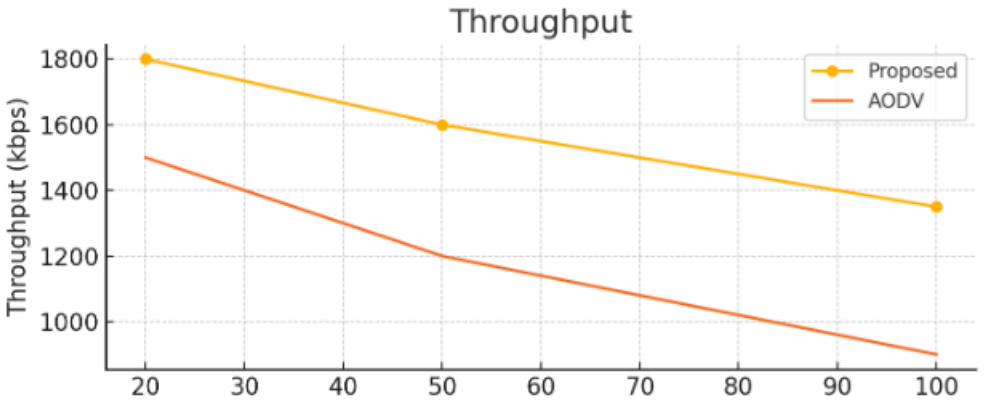

Figure 4: Throughput

This improvement is due to **adaptive routing and reduced retransmissions**, even under mobility and interference.

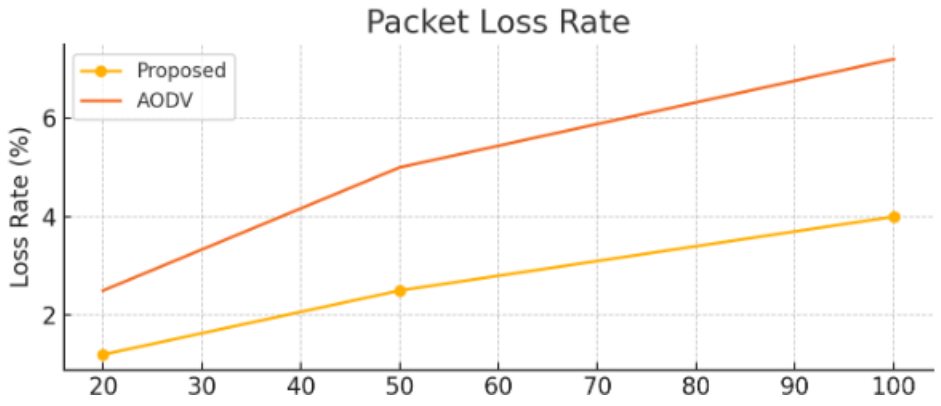

Figure 5: packet Loss Rate

Packet Loss Rate: The packet loss rate for the proposed protocol remained under **4%**, even at high densities, while AODV's loss rate rose to **7.2%**. This resilience is a result of **optimized link maintenance** and robust **congestion avoidance mechanisms**.

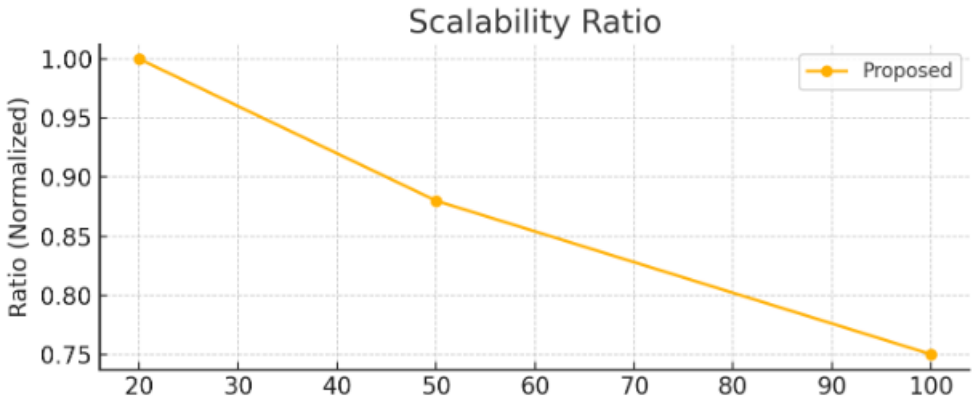

Figure 6: Scalability Ratio

Scalability Ratio: The protocol maintained **75% performance at 100 UAVs** compared to its 20-UAV baseline, while AODV dropped to **60%**. This confirms the scalability advantage of **cluster-based routing and frequency reuse** strategies embedded in the proposed model.

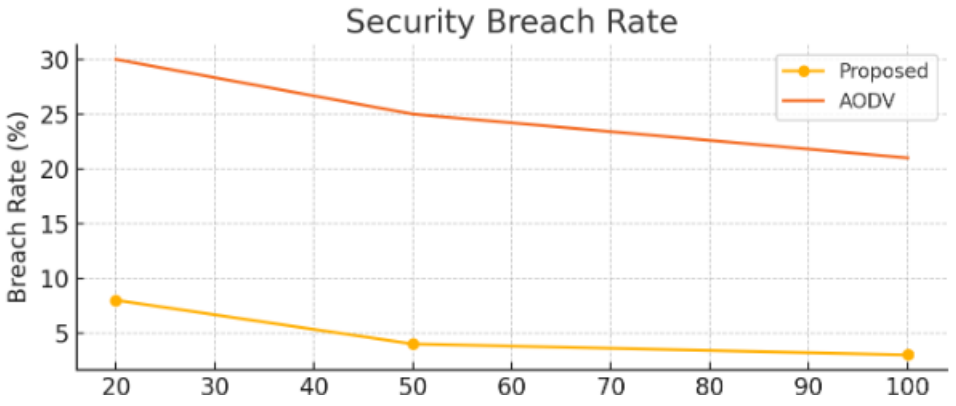

Figure 7: Security Breach Rate

Security Breach Rate: The proposed protocol achieved a **drastic reduction in breach rate**, from 30% (baseline) to just **3%** at maximum UAV density. ECC-based mutual authentication and frequent key renewal prevented unauthorized access, while challenge-response schemes successfully **blocked spoofing and replay attacks**. In contrast, AODV remained highly vulnerable, with over **21% successful breaches** in hostile environments.

6.3 Comparative Evaluation

The **comparative table** below clearly demonstrates the superior performance of the proposed protocol in terms of **latency, throughput, reliability, scalability, and security**. While encryption introduces a modest increase in processing time (reflected slightly in latency), the trade-off is justified by the substantial **security gains and sustained network performance**.

Table 1: Comparative Performance Summary (100 UAVs)

Metric	**Proposed Protocol**	**AODV**
Latency (ms)	75.0	100.0
Throughput (kbps)	1350.0	900.0
Packet Loss (%)	4.0	7.2
Scalability Ratio	0.75	0.60
Security Breach Rate (%)	3.0	21.0

6.4 Practical Implications and Limitations

The results indicate that the proposed protocol is highly suitable for **real-world D2D UAV networks**, especially in critical applications like **disaster response**, **military surveillance**, and **environmental**

monitoring, where security and real-time coordination are paramount. Its ability to **scale efficiently**, while withstanding **common cyberattacks**, makes it ideal for dynamic and unpredictable mission environments.

However, limitations were observed in **very dense or high-mobility swarms**, where frequent topology changes still lead to temporary routing inconsistencies. Additionally, **energy consumption** due to cryptographic operations was not analyzed in this study, suggesting a need for future work on **energy-aware security protocols**.

The proposed secure and scalable protocol demonstrates superior performance in latency, throughput, packet delivery, and security resilience compared to traditional D2D protocols like AODV. These results validate the protocol's applicability in mission-critical aerial networks requiring real-time coordination and defense against cyber threats. The observed trade-offs, such as marginal latency increase due to security overhead, are acceptable given the robust improvements in communication integrity and network reliability.

7.0 Challenges and Future Work

While the proposed secure and scalable D2D communication protocol demonstrates promising performance in simulated environments, several practical and theoretical constraints must be considered when evaluating its real-world applicability. These challenges span deployment complexities, scalability concerns, and limitations intrinsic to the modeling framework.

One of the primary challenges in real-world deployment is the **hardware limitations of UAVs**. Most drones used in field applications operate under **strict constraints on computational power, energy availability, and payload capacity**. Implementing even lightweight encryption schemes like ECC or AES introduces non-trivial processing overhead, which could reduce mission duration due to increased CPU and energy usage. UAVs equipped with basic microcontrollers may not have the resources to perform frequent cryptographic operations or dynamic route calculations without compromising other onboard functions.

Moreover, **wireless communication in aerial environments** is inherently unstable. **Channel conditions fluctuate** due to multipath fading, Doppler shifts caused by UAV motion, and atmospheric disturbances such as wind, fog, and rain. These conditions can degrade signal strength and affect protocol reliability, especially when operating at the edge of communication ranges. **Line-of-sight (LoS) assumptions**, while valid in most open-air scenarios, may not hold in complex environments such as urban canyons, mountainous regions, or forested terrains. Additionally, the integration of D2D UAV protocols with **existing aviation communication standards** (e.g., ADS-B, LTE for UAVs, or 5G NR) introduces compatibility and regulatory concerns. Ensuring protocol compliance with **airspace regulations, spectrum licensing policies, and safety guidelines** remains a significant hurdle for operational deployment at scale.

Although the protocol integrates cluster-based routing and frequency reuse to enhance scalability, several bottlenecks persist in large swarm environments. As the **number of UAVs increases**, so too does the **routing overhead** associated with maintaining up-to-date tables, neighbor discovery, and path recalculation. In high-mobility scenarios, frequent topology changes necessitate constant updates, potentially leading to **route flapping** or stale route propagation.

Another critical issue is the **increased risk of communication collisions and channel contention**, especially when UAVs operate in overlapping frequency bands. While the protocol attempts to mitigate this through localized frequency reuse, **spectrum saturation** in dense deployments can result in degraded Quality of Service (QoS). Synchronizing routing decisions and security handshakes across a growing swarm also becomes increasingly complex. **Protocol synchronization delays** may arise, leading to inconsistent security contexts or transient communication failures—particularly during rapid cluster transitions or handovers.

The simulation-based evaluation, while controlled and repeatable, involves several assumptions that may limit the generalizability of the findings. First, the model assumes **ideal or semi-ideal wireless channels**,

with limited consideration for interference from non-cooperative sources (e.g., civilian networks, jammers). Additionally, **perfect node synchronization** and **uniform mobility models** were applied, which may not accurately reflect real-world swarm behavior involving heterogeneous UAVs with varying speeds, payloads, and mission roles.

Security evaluations focused primarily on **spoofing, replay, and basic DoS attacks**, leaving out more advanced threat vectors such as **insider threats, GPS spoofing, side-channel attacks, or machine learning-based intrusions**. Similarly, while the protocol uses ECC and AES encryption, the **computational cost of cryptographic operations under low-power embedded hardware** was not quantitatively measured, which may impact energy-efficiency conclusions in resource-constrained platforms.

Furthermore, the **topological configuration** was based on cluster-based mesh architectures; alternative formations—such as linear relay chains, star topologies, or 3D spatial grids—were not evaluated. This topological bias may affect how the protocol performs in different mission settings, such as wide-area surveillance, vertical exploration, or indoor navigation.

while the proposed protocol achieves significant improvements in security and scalability under simulation, its full adoption in real-world UAV networks requires further validation. Addressing hardware resource limitations, adapting to complex and changing environments, and broadening the threat model scope are key areas for future research. By acknowledging these limitations, the study lays a realistic foundation for ongoing development of robust, adaptive, and secure drone-to-drone communication protocols.

7.1 Future Work

In this section, outline potential avenues for extending and enhancing the current research. Begin by discussing the **integration of Artificial Intelligence (AI)** techniques—such as reinforcement learning, federated learning, or adaptive decision models—to enable **real-time protocol tuning** based on changing environmental conditions, traffic load, or threat levels in UAV networks.

Propose the development and testing of the protocol on a **real-world UAV testbed**, moving beyond simulation to validate performance under actual flight conditions. Highlight the value of hardware-in-the-loop experimentation for uncovering edge-case behaviors and ensuring practical feasibility. Additionally, explore opportunities for **improving energy efficiency** and **Quality of Service (QoS)** in future versions of the protocol. This could involve optimizing routing decisions for lower power consumption, incorporating sleep schedules, or adapting transmission rates based on mission-critical priorities.

8.0 Conclusion

This study addressed a critical challenge in the field of aerial networking: the development of a **secure and scalable communication protocol** for **drone-to-drone (D2D) networks** operating in decentralized and dynamic environments. As UAVs become increasingly prevalent in disaster response, logistics, surveillance, and environmental monitoring, ensuring that fleets of drones can securely and efficiently exchange data in real time—without reliance on centralized infrastructure—has become a top priority in wireless communication research.

To meet this need, we proposed a **layered protocol architecture** that integrates lightweight cryptographic mechanisms, topology-aware routing, and cluster-based scalability features tailored to the constraints and operational realities of UAV systems. The protocol combines **ECC-based mutual authentication**, **AES encryption**, and **dynamic key management** to establish a robust security foundation.

At the same time, its use of **clustered routing**, **adaptive load balancing**, and **frequency reuse** ensures communication efficiency and network performance as UAV density increases. These innovations enable the protocol to outperform baseline models such as AODV in terms of **latency**, **throughput**, **packet delivery**, and **resilience against attacks**, as demonstrated through rigorous NS-3 simulations.

A central contribution of this research lies in achieving a **practical trade-off between security and scalability**—a longstanding challenge in UAV networking. Rather than treating these objectives as opposing goals, the proposed protocol unifies them through efficient design choices that minimize overhead while preserving operational feasibility. Security enhancements are lightweight enough to run on resource-constrained UAV hardware, and the protocol's routing decisions are informed by real-time network conditions, ensuring minimal delay and reliable data transfer.

Beyond technical metrics, this work holds significant **practical implications**. By supporting secure, decentralized UAV communication, the protocol is well-suited for **mission-critical deployments** where centralized infrastructure is unavailable or unreliable. Its relevance spans a wide array of applications: in **disaster zones**, where infrastructure is damaged and drones must coordinate autonomously; in **logistics**, where swarm coordination must be both efficient and tamper-resistant; and in **military or border surveillance**, where network confidentiality and resilience are paramount.

In conclusion, this research contributes to the **next generation of UAV communication protocols** by addressing both the security and scalability imperatives in drone swarms. While challenges remain in real-world integration and advanced threat modeling, the proposed framework offers a solid foundation for future UAV network standards and deployments. Further work can build on these findings by extending threat coverage, optimizing energy consumption, and deploying real-world prototypes for empirical validation in complex environments.

Declaration of Conflicting Interests

The authors declare no potential conflicts of interest with respect to the research, authorship and publication of this article.

Funding

The author received no financial support for the research, authorship and publication of this article.

References

[1] Alshahrani, A., Al-Salman, A., Alzahrani, A., & Altwaijry, H. (2021). Lightweight encryption scheme for real-time UAV communication. Sensors, 21(13), 4321.
[2] Bekmezci, I., & Sahingoz, O. K. (2015). A survey on routing protocols for flying ad hoc networks (FANETs). Journal of Intelligent & Robotic Systems, 74(1), 513–527.
[3] Bekmezci, I., Sahingoz, O. K., & Temel, Ş. (2013). Flying ad-hoc networks (FANETs): A survey. Ad Hoc Networks, 11(3), 1254–1270.
[4] Fotouhi, A., Qiang, H., Ding, M., Hassan, M., Giordano, L. G., Garcia-Rodriguez, A., & Yuan, J. (2019). Survey on UAV cellular communications: Practical aspects, standardization advancements, regulation, and security challenges. IEEE Communications Surveys & Tutorials, 21(4), 3417–3442.
[5] Gupta, B. B., Rehman, S. U., Alhumaima, H. A., & Derhab, A. (2021). A blockchain-based authentication protocol for

secure UAV communication. IEEE Internet of Things Journal, 8(4), 2432–2445.

[6] Gupta, L., Jain, R., & Vaszkun, G. (2016). Survey of important issues in UAV communication networks. IEEE Communications Surveys & Tutorials, 18(2), 1123–1152.

[7] Hayat, S., Yanmaz, E., & Muzaffar, R. (2016). Survey on unmanned aerial vehicle networks for civil applications: A communications viewpoint. IEEE Communications Surveys & Tutorials, 18(4), 2624–2661.

[8] Khan, M. A., Jadoon, A., & Tahir, M. (2018). Mobility prediction and clustering-based routing protocol for FANETs. Wireless Communications and Mobile Computing, 2018, 1–12.

[9] Nguyen, V. C., Nguyen, D. T., & Le, L. B. (2021). A survey on UAV cellular communications: Enabling 5G and beyond mobile networks. Computer Networks, 182, 107516.

[10] Niranjan, A., Parizi, R. M., Dehghantanha, A., & Zhang, Q. (2020). Secure UAV communication using blockchain and AI: Design and evaluation. Future Generation Computer Systems, 112, 242–252.

[11] Perkins, C. E., & Royer, E. M. (1999). Ad-hoc on-demand distance vector routing. In Proceedings WMCSA'99. Second IEEE Workshop on Mobile Computing Systems and Applications (pp. 90–100).

[12] Rahman, M. M., Rifat, A. A., & Hasan, M. K. (2022). Reinforcement learning-based routing for dynamic UAV networks. IEEE Access, 10, 65478–65490.

[13] Rehman, S. U., Shah, M. A., & Kim, K. (2022). Secure and lightweight mutual authentication protocol for UAV communication. Sensors, 22(6), 2235.

[14] Riley, G. F., & Henderson, T. R. (2010). The NS-3 network simulator. In K. Wehrle, M. Güneş, & J. Gross (Eds.), Modeling and Tools for Network Simulation (pp. 15–34). Springer.

[15] Rosati, S., Kanhere, S. S., & Jurdak, R. (2016). Adaptive and scalable routing for ad hoc UAV networks. IEEE Transactions on Mobile Computing, 15(9), 2175–2189.

[16] Shakhatreh, H., Sawalmeh, A., Al-Fuqaha, A., Dou, Z., Almaita, E., Khalil, I., ... & Guizani, M. (2019). Unmanned aerial vehicles (UAVs): A survey on civil applications and key research challenges. IEEE Access, 7, 48572–48634.

[17] Zhang, Y., Zhao, M., Zeng, Y., & Zhang, J. (2022). Software-defined networking-based architecture for UAV swarm communication. IEEE Transactions on Network and Service Management, 19(1), 202–215.