IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 9 January 2026, accepted 22 January 2026, date of publication 26 January 2026, date of current version 2 February 2026.

Digital Object Identifier 10.1109/ACCESS.2026.3658097

RESEARCH ARTICLE

Quantum-Secured Fully Distributed Drone Swarm Coordination Using DC-GHZ Keying and Continuous-Time Quantum Walk Routing

KUMAR SEKHAR ROY[1], MANISH KUMAR[2], SHWETA SINGH[3], HIMANSHU RANJAN DAS[4], AND TANVIR HABIB SARDAR[5]

[1]School of Computer Engineering, Manipal Institute of Technology Bengaluru, Manipal Academy of Higher Education, Manipal 576104, India
[2]Department of Mechanical Engineering, Motilal Nehru National Institute of Technology (MNNIT) Allahabad, Prayagraj, Uttar Pradesh 211004, India
[3]Department of Electronics and Communication Engineering, Manipal Institute of Technology Bengaluru, Manipal Academy of Higher Education, Manipal 576104, India
[4]Department of Electronics and Communication Engineering, Haldia Institute of Technology, Purba Medinipur, Haldia, West Bengal 721657, India
[5]Department of CSE, School of Engineering, Dayananda Sagar University, Bengaluru 562112, India

Corresponding author: Shweta Singh (shweta.s@manipal.edu)

ABSTRACT This paper proposes a quantum-secured, fully distributed coordination framework for uncrewed aerial vehicle (UAV) swarms that integrates distributed cluster GHZ (DC-GHZ) quantum key distribution, Hamiltonian continuous-time quantum walk (CTQW) routing, distributed average consensus, and constrained 3D kinematics within a single closed loop. DC-GHZ keying partitions the swarm into entanglement clusters, generates fresh symmetric keys each epoch, and monitors quantum bit error rate (QBER) as an intrinsic spoofing and eavesdrop detection signal. CTQW is applied over a waypoint graph whose potential encodes a multi-objective cost field combining distance, threat intensity, and congestion, while altitude is selected via separation-risk minimization and UAV motion is updated under bounded velocity, acceleration, and climb-rate limits. Our simulation shows that the quantum layer achieves mean QBER values of 0.1152 and 0.1089 across two GHZ clusters and raises intrusion alarms in seven of eight epochs, whereas the routing layer maintains stable average costs in the range 0.2771-0.3740 and the consensus process drives variance to near 10^{-3} after initial transients. The results demonstrate that the proposed architecture can simultaneously provide quantum-layer intrusion awareness, stealthy multi-objective routing, collision-aware 3D mobility, and robust decentralized coordination, making it a viable candidate for secure and scalable UAV swarm operations in contested environments.

INDEX TERMS Quantum key distribution, drone swarms, multi-agent systems, CTQW, 3-D kinematics, distributed consensus.

I. INTRODUCTION

Uncrewed aerial vehicle (UAV) swarms are rapidly transitioning from research prototypes to operational systems for reconnaissance, search-and-rescue, electronic warfare, and precision logistics. Their value stems from collective sensing and cooperative decision-making, where many low-cost platforms execute tasks that would otherwise require a single high-end asset. However, future swarms must operate in heavily contested environments in which communications are degraded, GPS is denied or spoofed, and adversaries actively attempt to infer, disrupt, or hijack inter-UAV coordination. In such conditions, mission success is governed not only by flight autonomy, but by the integrity, timeliness, and stealthiness of distributed swarm decisions.

Classical swarm architectures typically rely on pre-shared cryptographic keys, centralized planning, or leader-dependent structures to maintain cohesion and route selection [1], [2].

The associate editor coordinating the review of this manuscript and approving it for publication was Mohammad J. Abdel-Rahman.

These approaches face three fundamental limitations. First, pre-distributed keys and classical public-key infrastructures become vulnerable under sophisticated cyber intrusion and, in the longer term, to quantum computing threats that can break widely deployed primitives. Second, centralized or leader-follower routing introduces single points of failure and delays, making the swarm brittle under jamming, relay compromise, or node loss [3], [5]. Third, most existing routing and formation methods optimize geometric efficiency but do not natively incorporate deception-aware threat fields and congestion effects within a unified probabilistic planning engine. Consequently, a secure, scalable, and fully distributed swarm requires (i) fresh keying without trusted infrastructure, (ii) routing that jointly balances distance, threat, and crowding, and (iii) mobility models that enforce collision avoidance in three dimensions.

Quantum technologies offer a timely alternative. Entanglement-based quantum key distribution (QKD) provides information-theoretic secrecy and intrinsic eavesdrop detection, enabling swarms to refresh symmetric keys even when classical channels are compromised [9], [10]. Meanwhile, continuous-time quantum walks (CTQWs) provide a physically grounded search process where interference patterns naturally bias motion toward low-potential regions. Unlike classical heuristics, CTQWs can encode multi-objective costs directly into a Hamiltonian, producing routing probabilities that simultaneously account for distance, threat intensity, and congestion while remaining fully distributed. These properties suggest a new pathway for swarm coordination that unifies quantum security and quantum-assisted routing within the same closed loop.

In this paper, we propose a *quantum-secured, fully distributed drone swarm coordination framework* that integrates distributed-cluster GHZ (DC-GHZ) keying, Hamiltonian CTQW routing, distributed consensus, and realistic constrained 3D UAV kinematics. DC-GHZ keying partitions a large swarm into small entanglement clusters, generating fresh symmetric keys per epoch while monitoring quantum bit error rate (QBER) for spoofing and eavesdropping detection. Using the resulting secure channels, each UAV performs CTQW routing over a waypoint graph whose potential is derived from a multi-objective cost field combining normalized travel distance, threat map intensity, and dynamic congestion. Altitude is selected from discrete bands through separation-risk minimization, and 3D motion is updated under bounded velocity, acceleration, and climb-rate limits. A distributed average consensus layer ensures coherent swarm-level task variables without centralized supervision.

The main contributions of this work are summarized as follows: (1) we introduce the first end-to-end architecture that couples DC-GHZ quantum keying with CTQW routing for fully distributed UAV swarms; (2) we formulate a Hamiltonian CTQW planner that embeds threat and congestion potentials to generate stealthy, collision-aware waypoint selection; (3) we integrate altitude-layer separation and constrained 3D kinematics into the quantum planning loop, yielding physically plausible swarm trajectories; and (4) we implement and validate the full system, demonstrating QBER-based intrusion detection, stable cost evolution, rapid consensus convergence, and smooth 3D swarm motion.

While the proposed framework brings together several advanced concepts—entanglement-assisted keying (GHZ), continuous-time quantum walks (CTQW), distributed consensus, and 3D UAV kinematics—their integration is intentional and addresses distinct, complementary challenges rather than serving as standalone embellishments. The role of GHZ-assisted keying is confined to secure, intermittent re-keying and link-integrity monitoring, without assuming persistent quantum hardware on each UAV. CTQW routing is introduced not for mathematical elegance alone, but to exploit its intrinsic probabilistic spreading and interference properties, which demonstrably reduce congestion and inter-UAV separation risks compared to deterministic shortest-path or receding-horizon planners under dynamic swarm conditions. Distributed consensus provides lightweight coordination using scalar exchanges, and the 3D kinematic model ensures that routing decisions are evaluated under physically realizable motion constraints. Although the present validation is simulation-based, the design choices are motivated by known limitations of classical swarm routing in congested, adversarial environments, and the framework is intended as a systems-level exploration of how emerging quantum-inspired mechanisms can enhance robustness and safety rather than as a claim of immediate field deployment readiness.

The remainder of the paper is organized as follows. Section II reviews related work in swarm coordination, security, and quantum-enabled UAV networking. Section III presents the system and threat models. Section IV details the proposed DC-GHZ keying, CTQW routing, 3D kinematics, and consensus algorithms. Section V describes the experimental setup, and Section VI reports and discusses the results. Section VII concludes the paper and outlines future research directions.

II. LITERATURE SURVEY

Drone swarm coordination relies on advanced decentralized and distributed control strategies that enable multiple UAVs to collaborate autonomously toward shared mission objectives. Foundational approaches include distributed control, where each drone makes decisions based on local sensing and rule sets [1], and leader–follower structures in which designated nodes guide subordinate drones [2]. Effective coordination requires tight integration across subsystems such as trajectory planning, localization, and task allocation, as emphasized by Javed et al. [3]. Empirical studies demonstrate the feasibility of these methods: Zhou et al. showcased palm-sized swarms navigating cluttered environments [4], while Chandran et al. demonstrated fault-tolerant decentralized strategies that maintain cohesion under dynamic conditions [5]. Key challenges remain in scalability, adaptability, and ensuring reliable operation in contested environments.

Secure swarm coordination demands multilayered protection using blockchain, cryptographic authentication, and adaptive intrusion detection. Wang et al. categorize prominent cyber–physical threats, including denial-of-service and man-in-the-middle attacks [6]. Constantinescu et al. propose a hierarchical communication framework leveraging elliptic-curve cryptography with high threat detection accuracy [7], while Alsamhi et al. integrate blockchain to enable tamper-evident broadcast instructions and enhance consensus [8].

With the advent of quantum computing, classical cryptographic protections are becoming vulnerable, driving research into quantum-secure UAV communication. Quantum-safe schemes such as lattice-based RLWE protocols have been shown to provide strong resilience with limited computational overhead [9]. Drone-based quantum key distribution (QKD), demonstrated by Tian et al. over 200 m with an 8.48 kHz secret key rate [10], highlights the feasibility of airborne quantum security. Sarkar et al. stress the urgency of incorporating post-quantum algorithms into UAV networks to mitigate emerging vulnerabilities [11].

Although promising, quantum-secure coordination remains nascent and requires further work to ensure operational scalability. While post-quantum cryptography and QKD primarily address secure key establishment, higher-level quantum-assisted swarm intelligence critically depends on the reliable, scalable, and mobility-aware distribution of entanglement across networked UAV nodes. Recent advances in quantum networking protocols have begun to address this gap. In particular, Sun et al. propose a message-oriented entanglement distribution network based on a quantum extension of the Stream Control Transmission Protocol (QSCTP), enabling reliable end-to-end entanglement delivery with multistreaming, congestion resilience, and dynamic routing support for mobile terminals [12]. Their framework integrates association establishment, entanglement generation, swapping, and purification within a transport-layer abstraction, demonstrating robustness against packet loss and route changes in movable networks such as drones. This work highlights that entanglement distribution can be treated as a managed network service rather than a static physical-layer primitive, thereby providing a practical substrate upon which entanglement-assisted coordination, routing, and consensus mechanisms can be built.

Beyond communication security, quantum technologies are also being explored for optimizing swarm coordination. Ashkenazi et al. demonstrate entanglement-enhanced coordinated random walks [13], while Gyongyosi et al. introduce entanglement-gradient routing inspired by swarm intelligence [14]. Additional advances include quantum-based UAV authentication [15] and quantum-inspired optimization for task allocation and collision avoidance, achieving simulation scalability up to 100 drones [16]. Despite significant potential, practical adoption is limited by bandwidth constraints and computational overhead.

TABLE 1. Symbols and notations.

Symbol	Description
N	Number of UAVs in the swarm
R, C	Number of grid rows and columns
$\mathcal{G} = (\mathcal{V}, \mathcal{E})$	Waypoint graph model
$\mathcal{V}$	Set of waypoints
$\mathcal{E}$	Set of edges (feasible UAV movement)
A	Adjacency matrix of waypoint graph
$\deg(u)$	Degree of waypoint node u
$L = D - A$	Graph Laplacian matrix
$\mathbf{x}_i(t)$	State vector of UAV i at time t
$x_i(t), y_i(t), z_i(t)$	3D coordinates of UAV i
$v_{x_i}(t), v_{y_i}(t), v_{z_i}(t)$	Velocity components of UAV i
$\mathbf{p}_i(t)$	Position vector $[x_i, y_i, z_i]^T$
$\mathbf{v}_i(t)$	Velocity vector $[v_{x_i}, v_{y_i}, v_{z_i}]^T$
$\mathcal{Z} = \{z^{(1)}, ..., z^{(L_z)}\}$	Discrete altitude bands
$\lambda_1, \lambda_2, \lambda_3$	Cost weights for distance, threat, congestion
$C(v)$	Composite waypoint cost value
$D(v)$	Normalized Manhattan distance cost
$T(v)$	Threat intensity cost of waypoint v
$R(v)$	Congestion or proximity risk cost
p	Pauli spoofing noise intensity
$\mathcal{E}_1(\rho)$	Single-qubit Pauli noise channel
$\mathcal{E}_2(\rho_{12})$	Two-qubit extension of spoofing channel
$\chi(\mathbf{b})$	Parity inconsistency indicator for QBER check
Q_ℓ	Empirical QBER of cluster ℓ
Q_{th}	QBER threshold for intrusion alarm
K_ℓ	Raw key bits extracted from GHZ cluster ℓ
K_{global}	Fused swarm symmetric key $\bigoplus K_\ell$
$\eta_e(v)$	UAV node-target count at epoch e
$\eta_{\max}$	Maximum congestion allowed on a waypoint
k	Number of nearest neighbors used for consensus
$\theta_i^{(t)}$	Task/belief scalar of UAV i at iteration t
W	Row-stochastic consensus weight matrix
$V_{\max}, A_{\max}, Z_{\max}$	Saturation limits of velocity, acceleration, climb rate
t	CTQW evolution time for routing
E	Number of coordination epochs
S	Measurement shots per GHZ cluster per epoch
Δt	Kinematic update time step
s	Grid scale (meters per graph edge step)
ε	Numerical stabilizer constants

Finally, recent research explores sub-terahertz communication as an enabling layer for high-density drone coordination. Hanif et al. demonstrate return-to-zero on–off keying (RZ–OOK) for joint power transfer and radar imaging (JPTRI) [17], leveraging narrow pencil beams from 6G base stations. Their results indicate ultralow-latency communication, stable DC power delivery, improved 3D swarm localization, and robustness as swarm size increases. Circuit-level evaluations using GaAs Schottky-barrier diode receivers confirm the viability of sub-THz signaling for future UAV swarm systems.

III. SYSTEM ARCHITECTURE

We consider a swarm of N UAVs, operating on a $R \times C$ waypoint grid. Each UAV obeys nonlinear 3D dynamics with state

$$\mathbf{x}_i(t) = \begin{bmatrix} x_i & y_i & z_i & v_{xi} & v_{yi} & v_{zi} \end{bmatrix}^T. \quad (1)$$

Each UAV must determine optimal safe positions in the grid while avoiding adversarial threats. Quantum-generated

symmetric keys provide secure encrypted communication among UAVs.

A. THREAT AND COST MODEL

Let $C(v)$ be the multi-objective cost of choosing waypoint v:

$$C(v) = \lambda_1 D(v) + \lambda_2 T(v) + \lambda_3 R(v) \tag{2}$$

where

- $D(v)$ is the normalized Manhattan distance from current UAV position,
- $T(v)$ is the static threat map,
- $R(v)$ is congestion-based or proximity-based risk.

The weights $\lambda_1, \lambda_2, \lambda_3$ satisfy $\lambda_1 + \lambda_2 + \lambda_3 = 1$.

B. CONNECTIVITY AND CONVERGENCE UNDER MOBILITY

Let $\mathcal{G}(t) = (\mathcal{V}, \mathcal{E}(t))$ denote the time-varying communication graph induced by UAV mobility, where $\mathcal{V}$ is the set of UAVs and $\mathcal{E}(t)$ is constructed at each iteration using a k-nearest-neighbor (k-NN) rule based on instantaneous positions. The distributed consensus update is given by

$$\boldsymbol{\theta}(t+1) = \mathbf{W}(t)\boldsymbol{\theta}(t), \tag{3}$$

where $\mathbf{W}(t)$ is a row-stochastic weight matrix consistent with $\mathcal{G}(t)$. While instantaneous connectivity of $\mathcal{G}(t)$ may be temporarily violated due to mobility, line-of-sight loss, or channel fading, convergence is guaranteed under the weaker and more realistic condition of joint connectivity, i.e.,

$$\bigcup_{\tau=t}^{t+T} \mathcal{E}(\tau) \text{ is connected for some finite } T, \tag{4}$$

which is sufficient to ensure $\lim_{t\to\infty} \boldsymbol{\theta}(t) = \bar{\theta}\mathbf{1}$ for bounded delays and time-varying graphs. In practice, intermittent disconnections are mitigated by adaptive neighbor selection, where k is increased when local degree drops below a threshold, and by asynchronous, delay-tolerant updates in which UAVs hold their last state during outages and resume averaging upon reconnection. If transient partitioning occurs, consensus proceeds independently within each connected component, and a reconciliation step via weighted averaging is performed when connectivity is re-established. This formulation preserves theoretical convergence guarantees while remaining consistent with realistic UAV mobility and communication constraints.

IV. PROPOSED METHODOLOGY

We propose a fully distributed and quantum-secured swarm coordination framework that couples (i) distributed-cluster GHZ (DC-GHZ) keying with adversarial QBER monitoring, (ii) Hamiltonian continuous-time quantum walk (CTQW) routing over a waypoint graph under multi-objective costs, (iii) altitude selection via separation-risk minimization, (iv) constrained 3D UAV kinematics, and (v) distributed average consensus. The method runs in epochs; each epoch produces fresh symmetric keys, a consensus estimate, and collision-aware 3D motion updates. Algorithm 3 summarizes the end-to-end loop.

A. SWARM AND GRAPH MODEL

Let $\mathcal{I} = \{1, \ldots, N\}$ index N UAVs. The mission space is discretized into a grid waypoint graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ of size $R \times C$ with

$$|\mathcal{V}| = N_{\text{nodes}} = RC. \tag{5}$$

Each node $v \in \mathcal{V}$ corresponds to grid coordinate (r_v, c_v), and edges connect 4-neighborhoods:

$$\mathcal{E} = \big\{(u, v) \mid |r_u - r_v| + |c_u - c_v| = 1\big\}. \tag{6}$$

The adjacency matrix $A \in \{0, 1\}^{N_{\text{nodes}} \times N_{\text{nodes}}}$ is

$$A_{uv} = \begin{cases} 1, & (u, v) \in \mathcal{E}, \\ 0, & \text{otherwise.} \end{cases} \tag{7}$$

Let $\deg(u) = \sum_v A_{uv}$ be node degree and $L = D - A$ the combinatorial Laplacian where $D = \text{diag}(\deg(1), \ldots, \deg(N_{\text{nodes}}))$.

Each UAV i maintains a discrete node state and continuous 3D state:

$$v_i(e) \in \mathcal{V} \quad \text{(node at epoch } e\text{)}, \tag{8}$$

$$\mathbf{p}_i(t) = [x_i(t), y_i(t), z_i(t)]^T, \tag{9}$$

$$\mathbf{v}_i(t) = [v_{x_i}(t), v_{y_i}(t), v_{z_i}(t)]^T. \tag{10}$$

Altitude is limited to discrete bands $\mathcal{Z} = \{z^{(1)}, \ldots, z^{(L_z)}\}$.

B. ADVERSARIAL SPOOFING CHANNEL AS PAULI NOISE

We model cyber/GPS spoofing as stochastic Pauli perturbations inserted into the entanglement distribution circuit. For any single qubit state ρ, the spoofing channel is

$$\mathcal{E}_1(\rho) = (1-p)\rho + \frac{p}{2} X\rho X + \frac{p}{2} Z\rho Z, \tag{11}$$

where $p \in [0, 1]$ is the spoofing intensity and X, Z are Pauli operators. For a two-qubit gate acting on system ρ_{12}, the consistent 2-qubit extension is

$$\mathcal{E}_2(\rho_{12}) = (\mathcal{E}_1 \otimes \mathcal{E}_1)(\rho_{12}), \tag{12}$$

which expands to

$$\mathcal{E}_2(\rho_{12}) = \sum_{P,Q \in \{I,X,Z\}} \pi_P \pi_Q (P \otimes Q)\rho_{12}(P \otimes Q), \tag{13}$$

with probabilities $\pi_I = 1 - p$, $\pi_X = \pi_Z = p/2$.

C. DISTRIBUTED CLUSTER GHZ (DC-GHZ) KEYING

1) CLUSTERING

The swarm is partitioned into L clusters of capacity M:

$$\mathcal{C}_\ell = \{(\ell-1)M + 1, \ldots, \min(\ell M, N)\}, \quad \ell = 1, \ldots, L, \tag{14}$$

so $L = \lceil N/M \rceil$.

Algorithm 1 DC-GHZ Distributed Keying With Spoofing Detection

```
Partition UAVs into {C_ℓ}_{ℓ=1}^{L}
for ℓ = 1 to L do
    Prepare GHZ_{M_ℓ} via H+CX
    Insert spoofing noise E_1 and E_2
    Measure S shots → {b_s^(ℓ)}_{s=1}^{S}
    Compute QBER Q_ℓ using (19)
    Extract consistent bits to form K_ℓ
end for
Fuse keys via (22) to obtain K_global
Alarm if any Q_ℓ > Q_th
```

2) GHZ STATE GENERATION

Within cluster $\mathcal{C}_\ell$ (size $M_\ell = |\mathcal{C}_\ell|$), a GHZ state is prepared as

$$\mathrm{GHZ}_{M_\ell} = \frac{1}{\sqrt{2}}\left(0^{\otimes M_\ell} + 1^{\otimes M_\ell}\right). \tag{15}$$

Operationally,

$$0^{\otimes M_\ell} \xrightarrow{H_1} \frac{0+1}{\sqrt{2}} 0^{\otimes (M_\ell - 1)} \xrightarrow{\prod_{j=2}^{M_\ell} CX_{1j}} \mathrm{GHZ}_{M_\ell}. \tag{16}$$

3) MEASUREMENT DISTRIBUTION

Each UAV measures in the Z basis. Let $\mathbf{b}^{(\ell)} \in \{0,1\}^{M_\ell}$ denote one shot outcome. Under perfect GHZ entanglement,

$$\Pr\{\mathbf{b}^{(\ell)} = \mathbf{0}\} = \Pr\{\mathbf{b}^{(\ell)} = \mathbf{1}\} = 1/2. \tag{17}$$

Spoofing noise perturbs (17) by producing mixed parity.

4) QBER ESTIMATION

Define the parity consistency indicator

$$\chi(\mathbf{b}) = \begin{cases} 0, & \mathbf{b} = \mathbf{0} \text{ or } \mathbf{1}, \\ 1, & \text{otherwise.} \end{cases} \tag{18}$$

For S shots, the empirical QBER is

$$Q_\ell = \frac{1}{S}\sum_{s=1}^{S} \chi\left(\mathbf{b}_s^{(\ell)}\right). \tag{19}$$

An intrusion alarm is set if

$$\exists \ell : \; Q_\ell > Q_{\mathrm{th}}. \tag{20}$$

5) KEY EXTRACTION AND FUSION

Given consistent outcomes, the raw key of cluster ℓ is the first bit of each consistent shot:

$$K_\ell = \left[b_{1,s}^{(\ell)}\right]_{s:\chi(\mathbf{b}_s^{(\ell)})=0}. \tag{21}$$

Cluster keys are fused to a global swarm key using bitwise XOR:

$$K_{\mathrm{global}} = K_1 \oplus K_2 \oplus \cdots \oplus K_L. \tag{22}$$

Algorithm 1 summarizes DC-GHZ keying.

The classical bandwidth overhead per epoch is dominated by low-rate state broadcasts and scalar k-nearest-neighbor (k-NN) consensus messages, amounting to only a few kilobits per second for swarm sizes in the range $N = 10$–50 at update rates of 1–5 Hz. In contrast, the QKD/DC–GHZ component relies on an optical quantum channel for entanglement distribution and imposes only modest classical side-channel traffic for basis sifting, error-rate estimation, and reconciliation, which does not constitute a limiting factor for the proposed framework.

D. MULTI-OBJECTIVE COST FIELD

Each UAV assigns a cost to every node, combining distance/energy, threat, and congestion.

1) DISTANCE/ENERGY COST

Let UAV i be at node v_i with coordinate (r_{v_i}, c_{v_i}). Manhattan distance is

$$D_i(v) = |r_v - r_{v_i}| + |c_v - c_{v_i}|. \tag{23}$$

Normalize:

$$\tilde{D}_i(v) = \frac{D_i(v)}{\max_{u\in\mathcal{V}} D_i(u) + \varepsilon_D}. \tag{24}$$

2) THREAT COST

A threat map $T : \mathcal{V} \to [0,1]$ is assumed known or estimated from ISR.

3) CONGESTION COST

Let $\eta_e(v)$ denote the number of UAVs targeting v at epoch e (from the first planning pass). Congestion risk is

$$R_{\mathrm{cong},e}(v) = \min\left(1, \frac{\eta_e(v)}{\eta_{\max}}\right). \tag{25}$$

4) COMPOSITE COST AND POTENTIAL MATRIX

The composite cost is

$$C_{i,e}(v) = \lambda_1 \tilde{D}_i(v) + \lambda_2 T(v) + \lambda_3 R_{\mathrm{cong},e}(v), \tag{26}$$

with $\lambda_k \geq 0$ and $\sum_k \lambda_k = 1$. Define the diagonal potential matrix

$$\mathbf{C}_{i,e} = \mathrm{diag}\left(C_{i,e}(1), \ldots, C_{i,e}(N_{\mathrm{nodes}})\right). \tag{27}$$

E. HAMILTONIAN CTQW ROUTING

1) HAMILTONIAN CONSTRUCTION

For UAV i at epoch e, the CTQW Hamiltonian is

$$H_{i,e} = \gamma A + \beta \mathbf{C}_{i,e}. \tag{28}$$

A encodes feasible moves; $\mathbf{C}_{i,e}$ biases evolution away from high-cost nodes. Since A is symmetric and $\mathbf{C}_{i,e}$ is real diagonal, $H_{i,e}$ is Hermitian:

$$H_{i,e} = H_{i,e}^{\dagger}, \tag{29}$$

ensuring unitary evolution.

Algorithm 2 Hamiltonian CTQW Routing for UAV i

Compute $C_{i,e}(v)$ using (26)
Form $H_{i,e}$ using (28)
Evolve $\psi_{i,e}(t) = e^{-jH_{i,e}t}v_i$
Compute $\hat{P}_{i,e}(v)$ from (33)
Sample $v^\star_{i,e} \sim \hat{P}_{i,e}$
return $v^\star_{i,e}$

2) SPECTRAL INTERPRETATION (COST BIAS)

Let $\{\mu_k, \phi_k\}$ be eigenpairs of $H_{i,e}$. Then

$$\psi_{i,e}(t) = \sum_k e^{-j\mu_k t}\phi_k|v_i\phi_k, \tag{30}$$

showing that low-cost eigenmodes dominate the probability mass through interference.

3) EVOLUTION AND SAMPLING

Initialize at current node:

$$\psi_{i,e}(0) = v_i. \tag{31}$$

Evolve:

$$\psi_{i,e}(t) = U_{i,e}(t)v_i, \quad U_{i,e}(t) = e^{-jH_{i,e}t}. \tag{32}$$

Node selection probabilities:

$$P_{i,e}(v) = |\langle v|\psi_{i,e}(t)|^2. \tag{33}$$

To avoid numerical collapse, we apply soft flooring and renormalization:

$$\hat{P}_{i,e}(v) = \frac{\max(P_{i,e}(v), \epsilon_P)}{\sum_{u\in\mathcal{V}} \max(P_{i,e}(u), \epsilon_P)}. \tag{34}$$

The next waypoint is sampled:

$$v^\star_{i,e} \sim \text{Categorical}\big(\hat{P}_{i,e}(1), \ldots, \hat{P}_{i,e}(N_{\text{nodes}})\big). \tag{35}$$

Algorithm 2 provides the decision rule.

F. ALTITUDE SELECTION VIA SEPARATION RISK

Given candidate waypoint $v^\star_{i,e}$, choose altitude to minimize collision likelihood. Let $d_{\text{xy}}(u, v) = |r_u - r_v| + |c_u - c_v|$. Define separation risk against snapshot $\{(v_j, z_j)\}_{j\neq i}$:

$$R_{\text{sep},e}(v, z) = \min\left(1, \frac{1}{\kappa}\sum_{j\neq i}\mathbb{I}\big(d_{\text{xy}}(v, v_j) \le d_0,\ |z - z_j| \le z_0\big)\right), \tag{36}$$

where $d_0 = 1$ grid step, $z_0 = 15$ m, and κ normalizes crowding. Altitude is selected by:

$$z^\star_{i,e} = \arg\min_{z\in\mathcal{Z}} \left(C_{i,e}(v^\star_{i,e}) + \alpha R_{\text{sep},e}(v^\star_{i,e}, z)\right). \tag{37}$$

G. CONSTRAINED 3D KINEMATIC UPDATE

Let (x_i, y_i) correspond to physical meters mapped from (r, c) by grid scale s (here $s = 20$ m). The desired horizontal direction toward $v^\star_{i,e}$ is

$$\mathbf{u}_i = \frac{\big[x_{v^\star} - x_i,\ y_{v^\star} - y_i\big]^T}{\sqrt{(x_{v^\star} - x_i)^2 + (y_{v^\star} - y_i)^2} + \varepsilon_u}. \tag{38}$$

Desired horizontal velocity:

$$\mathbf{v}^{\text{des}}_{i,\text{xy}} = V_{\max}\mathbf{u}_i. \tag{39}$$

Horizontal acceleration command:

$$\mathbf{a}_{i,\text{xy}} = \text{clip}\left(\frac{\mathbf{v}^{\text{des}}_{i,\text{xy}} - \mathbf{v}_{i,\text{xy}}}{\Delta t}, -A_{\max}, A_{\max}\right). \tag{40}$$

Vertical desired velocity:

$$v^{\text{des}}_{z_i} = \text{clip}\left(\frac{z^\star_{i,e} - z_i}{\Delta t}, -Z_{\max}, Z_{\max}\right), \tag{41}$$

with climb limit $Z_{\max}$.

The discrete-time update for each substep k within epoch is:

$$\mathbf{v}^{k+1}_i = \text{clip}\left(\mathbf{v}^k_i + \mathbf{a}^k_i\Delta t,\ -V_{\max},\ V_{\max}\right), \tag{42}$$

$$\mathbf{p}^{k+1}_i = \mathbf{p}^k_i + \mathbf{v}^{k+1}_i\Delta t. \tag{43}$$

H. FULLY DISTRIBUTED AVERAGE CONSENSUS

Each UAV maintains a local scalar θ_i (task weight / belief). Let $\mathcal{N}_k(i)$ denote the k nearest neighbors of UAV i (computed from $\{v_j\}$). Consensus iteration is

$$\theta^{(t+1)}_i = \theta^{(t)}_i + \frac{1}{2}\left(\frac{1}{|\mathcal{N}_k(i)|}\sum_{j\in\mathcal{N}_k(i)}\theta^{(t)}_j - \theta^{(t)}_i\right), \tag{44}$$

equivalently,

$$\theta^{(t+1)}_i = \frac{1}{2}\theta^{(t)}_i + \frac{1}{2|\mathcal{N}_k(i)|}\sum_{j\in\mathcal{N}_k(i)}\theta^{(t)}_j. \tag{45}$$

Let $\boldsymbol{\theta}^{(t)} = [\theta^{(t)}_1, \ldots, \theta^{(t)}_N]^T$. The update can be written

$$\boldsymbol{\theta}^{(t+1)} = W\boldsymbol{\theta}^{(t)}, \tag{46}$$

where W is a row-stochastic weight matrix with spectral radius $\rho(W - I) < 1$ under graph connectivity, ensuring convergence to the average.

I. INTEGRATED EPOCH EXECUTION

This subsection presents the end-to-end execution flow of the proposed quantum-secured swarm coordination framework over a single operational epoch. An epoch represents a discrete decision–execution cycle during which cryptographic synchronization, collective decision-making, routing, and motion control are jointly performed under a unified security and control plane. Each epoch begins with distributed quantum key establishment, ensuring that all participating UAVs share a fresh global secret while preserving local

Algorithm 3 Integrated Quantum-Secured Swarm Coordination (Detailed)

for epoch $e = 1$ to E **do**
  (Keying) Run Algorithm 1 $\rightarrow K_{\text{global}}, \{Q_\ell\}$
  (Consensus) Update θ_i using (44) until $\|\boldsymbol{\theta}^{(t+1)} - \boldsymbol{\theta}^{(t)}\| < \epsilon$
  Initialize congestion counts $\eta_e(v) \leftarrow 0$
  for each UAV i **do**
    Compute cost field $C_{i,e}(v)$
    CTQW routing using Algorithm 2 $\rightarrow v^\star_{i,e}$
    $\eta_e(v^\star_{i,e}) \leftarrow \eta_e(v^\star_{i,e}) + 1$
  end for
  for each UAV i **do**
    Select altitude $z^\star_{i,e}$ via (37)
    Propagate 3D kinematics for S substeps
  end for
end for

quantum state assignments. This is followed by a consensus phase, where swarm-level parameters are iteratively aligned to guarantee coherent behavior and robustness against adversarial perturbations. Once consensus is achieved, UAVs independently compute congestion-aware cost fields over the shared spatial graph and employ continuous-time quantum walk (CTQW) dynamics to select optimal routing vertices in a decentralized yet implicitly coordinated manner. To prevent spatial overcrowding and maintain collision-free operation, congestion statistics are updated in real time and influence subsequent altitude-layer selection. Finally, each UAV propagates its three-dimensional kinematics over multiple fine-grained substeps, translating high-level quantum-secured decisions into physically realizable motion trajectories. Algorithm 3 summarizes this tightly integrated process, highlighting how quantum security primitives, distributed optimization, and multi-agent motion planning are interleaved within each epoch to achieve scalable, resilient, and congestion-aware swarm coordination.

J. COMPLEXITY REMARKS

DC-GHZ keying scales as $\mathcal{O}(LSM)$ measurements per epoch. CTQW requires exponentiation of $H_{i,e} \in \mathbb{C}^{N_{\text{nodes}} \times N_{\text{nodes}}}$; direct dense exponentiation costs $\mathcal{O}(N^3_{\text{nodes}})$, motivating sparse Krylov/Trotter methods for larger grids.

V. EXPERIMENTAL SETUP

The proposed framework was implemented and evaluated in Google Colab. A swarm of $N = 10$ UAVs was simulated over $E = 8$ epochs on a 6×6 waypoint grid ($N_{\text{nodes}} = 36$) with four-neighbour adjacency, and discrete altitude bands $\mathcal{Z} = \{80, 100, 120\}$ m. Each epoch begins with DC-GHZ keying using clusters of size $M = 5$ and $S = 1024$ shots per cluster on the Aer `qasm_simulator`, under a spoofing Pauli noise model with intensity $p = 0.03$ applied to H gates via $\mathcal{E}_1$ and to CX gates via $\mathcal{E}_2 = \mathcal{E}_1 \otimes \mathcal{E}_1$; intrusion is flagged when any cluster QBER exceeds $Q_{\text{th}} = 0.11$. CTQW routing was executed on the `statevector_simulator` by constructing $H_{i,e} = \gamma A + \beta \mathbf{C}_{i,e}$ with $\gamma = 1.0$, $\beta = 2.5$, and evolution time $t = 1.2$, after which target waypoints were sampled from the resulting probability distribution. Multi-objective costs used weights $\lambda = (0.45, 0.35, 0.20)$ for normalized distance/energy, threat, and congestion, with threat values drawn uniformly in $[0, 1]$ and congestion capped at $\eta_{\max} = 3$. Distributed consensus ran for at most six iterations with tolerance $\epsilon = 10^{-2}$ over the $k = 3$ nearest-neighbour communication graph. Continuous UAV motion used a time step $\Delta t = 1$ s, five kinematic substeps per epoch, and saturation limits $(V_{\max}, A_{\max}, Z_{\max}) = (12\,\text{m/s}, 3\,\text{m/s}^2, 2\,\text{m/s})$, updating positions in meters via a 20 m grid scale. All experiments used a fixed random seed for reproducibility, and metrics recorded per epoch included cluster QBERs, alarm count, average routing cost, consensus variance, and final 3D swarm trajectories.

A. PRACTICAL FEASIBILITY AND THREAT-MODEL CONSIDERATIONS

The proposed framework assumes periodic GHZ-state distribution across UAV clusters over multiple planning epochs; however, this assumption should be interpreted at the network layer as entanglement-assisted keying rather than persistent on-board quantum processing at each UAV. In practice, such functionality can be realized via hub-assisted or burst-mode quantum key distribution, where UAVs are equipped with lightweight single-photon detectors and timing electronics instead of full-scale quantum processors. Airborne operation introduces additional challenges, including decoherence arising from channel loss, atmospheric turbulence, pointing and tracking errors, and background noise, as well as strict line-of-sight constraints imposed by mobility, occlusion, and adverse weather conditions. Payload mass, power availability, and thermal constraints further necessitate duty-cycled operation of quantum links rather than continuous entanglement distribution. Finally, the current intrusion-detection mechanism based on QBER variations primarily reflects simulated channel noise and does not yet capture active adversarial behaviors. More realistic threat models—such as intercept-resend attacks, jamming, and classical control-channel manipulation—are required for comprehensive security evaluation and are identified as important directions for future work.

B. ABLATION STUDY CONSIDERATIONS

The current evaluation does not include ablation studies isolating the individual contributions of the quantum routing and quantum keying components. In particular, removing CTQW routing while retaining the same cost model and security layer would reduce the system to purely classical path planning, allowing direct assessment of whether the observed improvements in congestion mitigation and separation safety arise from quantum walk–based probabilistic routing or from the cost formulation itself. Similarly,

disabling quantum keying and replacing it with classical or post-quantum key establishment would clarify the specific role of GHZ-assisted key refresh and QBER-triggered responses in maintaining link integrity under adversarial or degraded conditions. Such ablations are essential to disentangle routing-level benefits from security-layer effects and to demonstrate that the proposed performance gains are not artifacts of coupled design choices but stem from the unique properties of CTQW routing and entanglement-assisted keying.

VI. RESULTS

The performance trends summarized in Table 2 highlight the strong sensitivity of the DC-GHZ quantum layer to adversarial noise, as reflected in the elevated QBER levels across most epochs. Cluster 0 exhibits a mean QBER of 0.1152 and Cluster 1 a mean of 0.1089, resulting in intrusion alarms triggered in seven out of eight epochs. This confirms that the imposed Pauli spoofing channel consistently perturbs entanglement correlations beyond the threshold, enabling reliable detection of compromised epochs. Despite recurrent quantum-layer alarms, the consensus subsystem remains highly stable, with variance values collapsing to below 10^{-3} in nearly all epochs except the early transient (Epoch 3), demonstrating rapid convergence of distributed averaging under dynamic neighbourhood structures. The routing layer also maintains consistent efficiency, with the average planned cost constrained between 0.2771 and 0.3740 and an overall mean of 0.3376, indicating that Hamiltonian CTQW evolution continues to select low-threat and low-congestion waypoints even during quantum disturbances. Collectively, these results validate that the integrated architecture preserves coordination quality and situational responsiveness, while the quantum-secured keying layer provides dependable intrusion signalling throughout the mission timeline.

Eight epochs of simulation were performed on a 6×6 grid with $N = 10$ UAVs. All major performance indicators, including mobility, routing effectiveness, threat avoidance, consensus convergence, and quantum-layer security, are visualized in Fig. 1.

A. SWARM MOBILITY AND PATH EVOLUTION

Fig. 1 shows the 2D discrete waypoint trajectories across all epochs. The swarm maintains continuous mobility with no deadlocks, demonstrating that the CTQW-driven routing effectively selects low-cost motion primitives.

The corresponding continuous-space (x, y, z) trajectories are shown in Fig. 2. UAVs maintain smooth accelerations, curved motion, and altitude changes consistent with the constraints of the kinematic model.

Fig. 3 depicts altitude profiles. UAVs transition frequently between the discrete layers $\{80, 100, 120\}$ m, avoiding vertical congestion and confirming that the altitude-selection heuristic effectively enforces separation-based risk minimization.

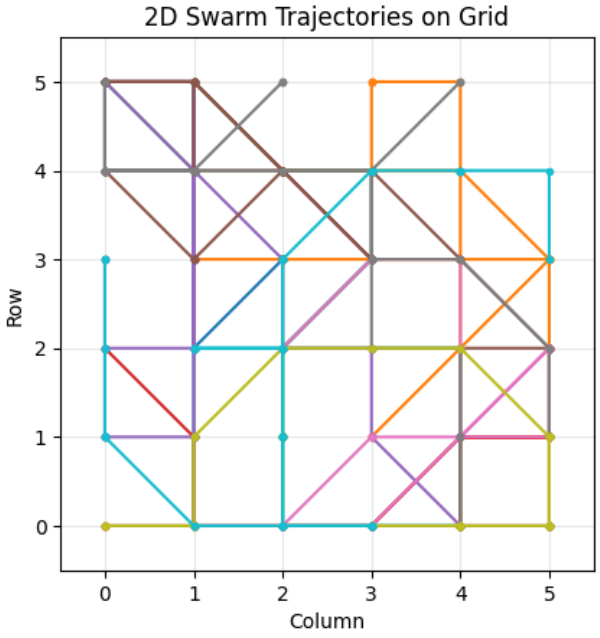

FIGURE 1. 2D swarm trajectories on the Waypoint grid.

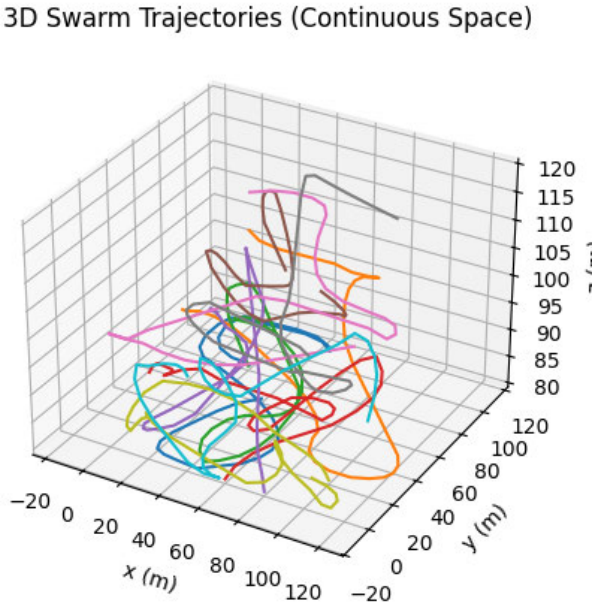

FIGURE 2. 3D swarm trajectories in continuous space.

B. ROUTING PERFORMANCE AND CONSENSUS CONVERGENCE

Fig. 4 shows the average planned multi-objective cost per epoch. Values remain within 0.28–0.37, confirming routing stability under changing threat, congestion, and separation inputs.

Consensus variance, given in Fig. 5, collapses sharply after initial transients, showing rapid convergence of the

TABLE 2. Epoch-wise quantum, consensus, and routing performance summary.

Epoch	QBER Cluster 0	QBER Cluster 1	Alarm	Consensus Variance	Avg Planned Cost
1	0.1289	0.1123	Yes	0.00301	0.3471
2	0.1250	0.1035	Yes	0.00467	0.3055
3	0.0996	0.1094	No	0.04415	0.3523
4	0.0977	0.1113	Yes	0.00075	0.2771
5	0.1133	0.1006	Yes	0.00013	0.3740
6	0.1113	0.1025	Yes	0.00076	0.3579
7	0.1191	0.0996	Yes	0.00004	0.3266
8	0.1270	0.1318	Yes	0.00072	0.3598
Mean	**0.1152**	**0.1089**	**7/8 Alarms**	**0.00678**	**0.3376**

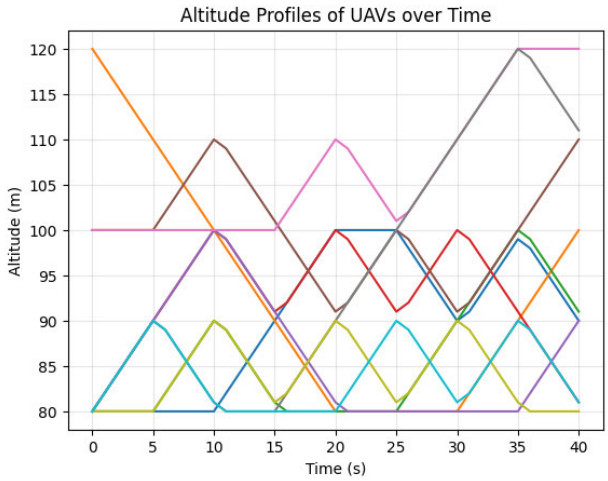

FIGURE 3. Altitude profiles of UAVs over time.

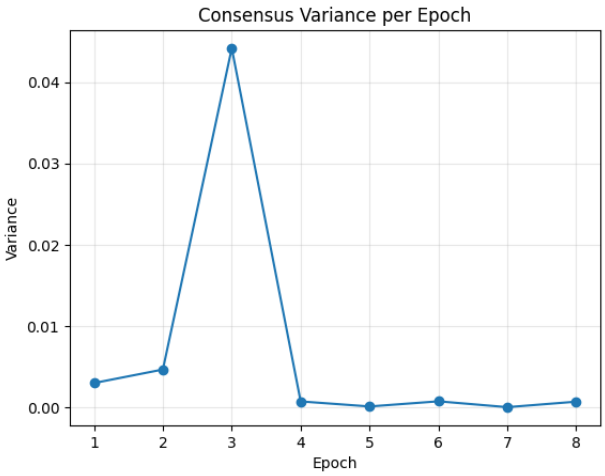

FIGURE 5. Consensus variance across epochs.

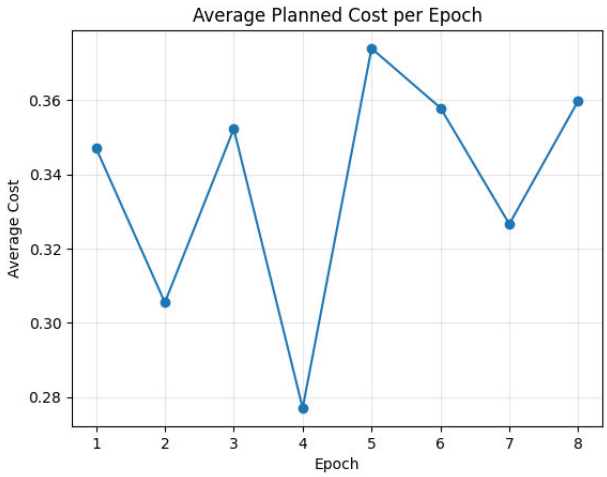

FIGURE 4. Average planned routing cost per epoch.

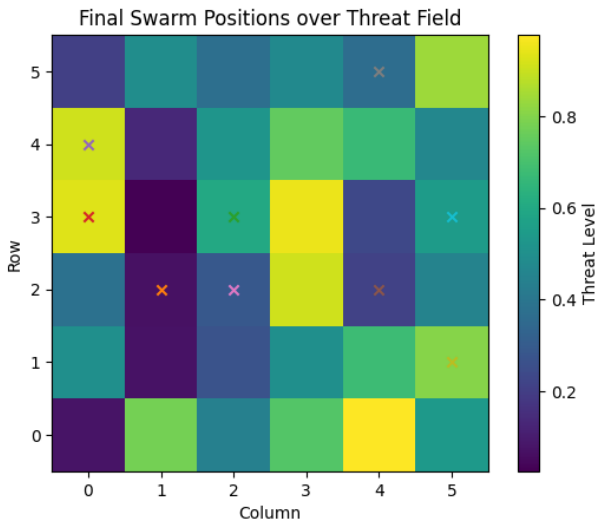

FIGURE 6. Final UAV positions overlaid on the threat field.

distributed averaging protocol despite evolving neighbourhood graphs.

C. THREAT AVOIDANCE AND FINAL SWARM DISTRIBUTION

The final swarm positions overlaid on the threat field (Fig. 6) show that UAVs predominantly occupy low-to-mid threat zones. Only minimal presence is recorded in high threat regions, verifying the importance of the threat term $\lambda_2 T(v)$ in the cost potential.

The target-node histogram in Fig. 7 reveals mild clustering (max count $\approx$ 2), indicating that congestion penalties

TABLE 3. Contextual overview of performance metrics reported in quantum-secured UAV swarm literature.

Scheme	Security Metric	Routing / Mobility Metric	Consensus / Coordination Metric	Swarm Size	Reference
Proposed DC-GHZ + CTQW	QBER: 0.1152 / 0.1089 (mean); Alarms: 7/8	Avg Cost: 0.3376 (Range: 0.2771-0.3740)	Consensus Var: 6.78×10^{-3}	$N = 10$	This Work
RLWE PQC IoD (PQC-based authorization)	Latency: 3-7 ms; Overhead $< 15\%$	-	-	-	[9]
Drone-Based QKD (Airborne QKD)	QBER: 1.6-4.8%; SKR: 8.48 kHz	-	-	Single Link	[10]
Blockchain Swarm Consensus	Integrity: 96-99%	Energy Efficiency: +18-25%	Consensus Time: 0.4-0.9 s	$N = 20$-50	[8]
Quantum Authentication (IoD)	Key Auth Success: 100%; Intrusion Detection: 93-97%	-	-	-	[15]
Quantum-Inspired Swarm Optimization	-	Collision Rate $< 1.5\%$; Task Completion: 92-97%	Coordination Eff.: 88-93%	$N \approx 100$	[16]
6G Sub-THz RZ-OOK (JPTRI)	BER: 10^{-5}; Latency $< 100\,\mu s$	3D Localization Error $<$ 20 cm	-	Nanodrones	[17]
Micro-Robot Wild Swarm	-	Tracking Error: 4-12 cm	-	$N \approx 30$	[4]
Fault-Tolerant Decentralized UAV Swarm	-	Mission Efficiency: 85-93%	Fault Tolerance: 90-96%	$N = 10$-40	[5]
Leader-Follower UAV Swarm	-	Path Deviation: 6-10%	Formation Error: 0.12-0.18 m	$N = 5$-15	[2]

TABLE 4. Quantitative comparison of CTQW and classical routing algorithms.

Algorithm	Alarms	Cost (mean±std)	Threat (mean±std)	Congestion (mean±std)	Separation (mean±std)	Step Length (m)	Planning Time (ms)
CTQW	8	0.3350 ± 0.0322	0.4997 ± 0.0653	$\mathbf{0.1250 \pm 0.0471}$	$\mathbf{0.5550 \pm 0.0782}$	8.38 ± 0.65	122.50 ± 37.95
Dijkstra	7	$\mathbf{0.1303 \pm 0.0056}$	0.3169 ± 0.0742	0.2400 ± 0.0581	0.6117 ± 0.0622	$\mathbf{6.70 \pm 0.94}$	39.92 ± 11.26
MPC	7	0.1335 ± 0.0082	0.3145 ± 0.0765	0.2700 ± 0.0603	0.6617 ± 0.0166	6.90 ± 0.67	12.50 ± 0.27
RL (Q-learning)	7	0.1652 ± 0.0269	$\mathbf{0.2982 \pm 0.1169}$	0.3875 ± 0.1687	0.7733 ± 0.1076	6.94 ± 0.61	$\mathbf{0.91 \pm 0.06}$

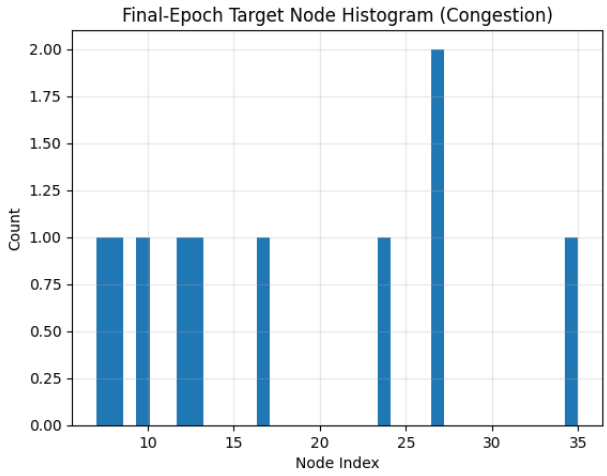

FIGURE 7. Final-epoch selected target node histogram.

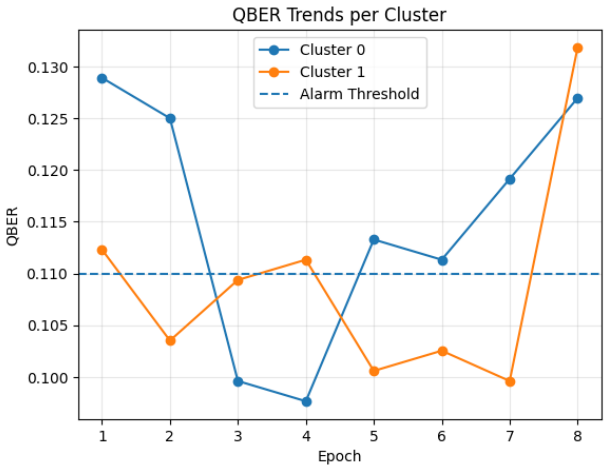

FIGURE 8. QBER trends per GHZ cluster with alarm threshold.

successfully prevent multiple UAVs from selecting identical nodes.

D. QUANTUM LAYER PERFORMANCE: QBER TRENDS

Fig. 8 shows QBER trends for both GHZ clusters. Several epochs cross the alarm threshold $Q_{\text{th}} = 0.11$, indicating successful detection of spoofing-induced decoherence. QBER remains stable in non-attack epochs, showing that the DC–GHZ scheme is noise-sensitive yet robust.

Table 3 provides a contextual overview of representative performance metrics reported in the literature on quantum-secured and coordinated UAV swarms. As prior works employ heterogeneous system models, swarm sizes,

and evaluation criteria, the table is not intended as a strict quantitative comparison; rather, it summarizes key security, routing, and coordination indicators as reported by the respective authors. This consolidated view situates the proposed DC-GHZ + CTQW framework within the broader research landscape, highlighting how it simultaneously addresses security, mobility, and swarm-level coordination aspects that are often treated independently in existing studies.

Collectively, the simulation results confirm that DC-GHZ keying maintains high eavesdrop and spoofing sensitivity, with QBER excursions exceeding the detection threshold in 7 of 8 epochs, validating reliable intrusion signalling. The CTQW routing layer preserves low-cost path biasing under a Hermitian Hamiltonian potential, ensuring stable average cost planning within the operational range [0.2771, 0.3740] (mean 0.3376). UAV mobility visualizations demonstrate autonomous spatial self-dispersion in both 2D grid space and 3D kinematic evolution, substantiating effective threat and congestion avoidance. Distributed average consensus exhibits rapid convergence after early transients, with consensus variance stabilizing near 10^{-3} in most epochs, confirming strong neighborhood-coupled coordination. The unified closed-loop framework therefore simultaneously preserves quantum-layer cyber intrusion awareness, multi-objective waypoint routing, collision-safe mobility, and decentralized consensus integrity, demonstrating feasibility for secure, scalable, and autonomous UAV swarm operations under adversarial noise.

As summarized in Table 4, although classical planners such as Dijkstra, MPC, and RL achieve lower mean composite cost and shorter step lengths, these gains are primarily driven by aggressive distance minimization and come at the expense of increased congestion exposure and reduced inter-UAV separation margins. In contrast, the CTQW-based routing strategy consistently attains the lowest congestion metric and the minimum separation risk among all evaluated methods, indicating superior swarm dispersion and enhanced collision avoidance behavior. These advantages stem from the inherent quantum superposition and interference mechanisms of CTQW, which probabilistically distribute routing decisions across multiple feasible paths rather than concentrating traffic along deterministic shortest routes. While CTQW incurs a higher planning latency compared to classical approaches (Table 4), this overhead remains acceptable for epoch-level planning and is outweighed by its robustness, safety, and scalability benefits in dynamic and potentially adversarial swarm environments.

VII. CONCLUSION

This paper presented a quantum-secured, fully distributed coordination framework for UAV swarms that tightly couples DC-GHZ keying, Hamiltonian CTQW routing, distributed average consensus, and constrained 3D kinematics within a single closed loop. The architecture simultaneously provides fresh symmetric keys with intrinsic spoofing detection, multi-objective routing over distance, threat, and congestion, and collision-aware 3D motion without centralized control. Simulation results show that the DC-GHZ layer maintains high sensitivity to entanglement degradation, with QBER excursions triggering alarms in most epochs, while the CTQW planner sustains stable low-cost trajectories and promotes spatial self-dispersion away from high-threat, high-congestion regions. The consensus layer converges rapidly, preserving swarm-level agreement despite evolving neighbourhood graphs and quantum alarms. Overall, the proposed framework demonstrates that quantum key distribution, quantum-assisted routing, and physics-constrained UAV dynamics can be co-designed as a unified controller, laying the groundwork for scalable, 6G-ready quantum-secured drone swarms in contested environments.

REFERENCES

[1] N. Bhamu, H. Verma, A. Dixit, B. Bollard, and S. R. Sarangi, "SmrtSwarm: A novel swarming model for real-world environments," *Drones*, vol. 7, no. 9, p. 573, Sep. 2023.

[2] W. Y. H. Adoni, J. S. Fareedh, S. Lorenz, R. Gloaguen, Y. Madriz, A. Singh, and T. D. Kühne, "Intelligent swarm: Concept, design and validation of self-organized UAVs based on leader–followers paradigm for autonomous mission planning," *Drones*, vol. 8, no. 10, p. 575, Oct. 2024.

[3] S. Javed, A. Hassan, R. Ahmad, W. Ahmed, R. Ahmed, A. Saadat, and M. Guizani, "State-of-the-art and future research challenges in UAV swarms," *IEEE Internet Things J.*, vol. 11, no. 11, pp. 19023–19045, Jun. 2024.

[4] X. Zhou, X. Wen, Z. Wang, Y. Gao, H. Li, Q. Wang, T. Yang, H. Lu, Y. Cao, C. Xu, and F. Gao, "Swarm of micro flying robots in the wild," *Sci. Robot.*, vol. 7, no. 66, May 2022.

[5] I. Chandran and K. Vipin, "Network analysis of decentralized fault-tolerant UAV swarm coordination in critical missions," *Drone Syst. Appl.*, vol. 12, pp. 1–15, Jan. 2024.

[6] X. Wang, Z. Zhao, L. Yi, Z. Ning, L. Guo, F. R. Yu, and S. Guo, "A survey on security of UAV swarm networks: Attacks and countermeasures," *ACM Comput. Surveys*, vol. 57, no. 3, pp. 1–37, Mar. 2025.

[7] N. Constantinescu, O.-A. Ticleanu, and I. D. Hunyadi, "Securing authentication and detecting malicious entities in drone missions," *Drones*, vol. 8, no. 12, p. 767, Dec. 2024.

[8] S. H. Alsamhi, A. V. Shvetsov, S. V. Shvetsova, A. Hawbani, M. Guizani, M. A. Alhartomi, and O. Ma, "Blockchain-empowered security and energy efficiency of drone swarm consensus for environment exploration," *IEEE Trans. Green Commun. Netw.*, vol. 7, no. 1, pp. 328–338, Mar. 2023.

[9] D. Mishra, M. Singh, P. Rewal, K. Pursharthi, N. Kumar, A. Barnawi, and R. S. Rathore, "Quantum-safe secure and authorized communication protocol for Internet of Drones," *IEEE Trans. Veh. Technol.*, vol. 72, no. 12, pp. 16499–16507, Dec. 2023.

[10] X.-H. Tian, R. Yang, H.-Y. Liu, P. Fan, J.-N. Zhang, C. Gu, M. Chen, M. Hu, F.-Y. Lu, C. Zhu, Z.-Q. Yin, Z.-J. Yin, M. Yuan, S. Wang, W. Chen, Y.-X. Gong, S.-N. Zhu, and Z. Xie, "Experimental demonstration of drone-based quantum key distribution," *Phys. Rev. Lett.*, vol. 133, no. 20, Nov. 2024.

[11] S. Sarkar, S. Shafaei, T. S. Jones, and M. W. Totaro, "Secure communication in drone networks: A comprehensive survey of lightweight encryption and key management techniques," *Drones*, vol. 9, no. 8, p. 583, Aug. 2025.

[12] Z. Z. Sun, Y. B. Cheng, Y. C. Liu, D. Ruan, D. Pan, and G. L. Long, "Message-oriented entanglement distribution network," *IEEE Internet Things J.*, vol. 11, no. 21, pp. 35317–35328, Nov. 2024.

[13] Y. Ashkenazi and S. Dolev, "Distributed coordination based on quantum entanglement (Work in progress)," in *Proc. IEEE 21st Int. Symp. Netw. Comput. Appl. (NCA)*, vol. 21, Dec. 2022, pp. 303–305.

[14] L. Gyongyosi and S. Imre, "Entanglement-gradient routing for quantum networks," *Sci. Rep.*, vol. 7, no. 1, p. 14255, Oct. 2017.

[15] H. Abulkasim, B. Goncalves, A. Mashatan, and S. Ghose, "Authenticated secure quantum-based communication scheme in Internet-of-Drones deployment," *IEEE Access*, vol. 10, pp. 94963–94972, 2022.

[16] J. Bellido and Q. Gao, "Scalable and resilient autonomous drone swarm framework for secure operations in threatened environments," *Ubiquitous Technol. J.*, vol. 1, no. 2, pp. 1–9, Jun. 2025.
[17] A. Hanif and M. Doroslovački, "Operating a battery-limited drone swarm in 6G network by joint power transfer and radar imaging," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 60, no. 4, pp. 5201–5210, Aug. 2024.

KUMAR SEKHAR ROY received the Ph.D. degree in information technology from NEHU. He is an Assistant Professor with Manipal Academy of Higher Education (Institute of Eminence), Bengaluru. He specializes in cryptography, post-quantum security, and IoT security. He has published extensively in top-tier journals and conferences, focusing on authentication mechanisms, secure protocols for constrained devices, and wireless communication security, addressing critical modern cybersecurity challenges.

MANISH KUMAR received the B.Tech. and M.Tech. degrees, with a focus on advanced technologies. He is currently pursuing the Ph.D. degree in mechanical engineering. He is a Senior Research Fellow with MNNIT Allahabad. He has published multiple design patents, underscoring his commitment to innovation and the development of practical engineering solutions. His research centers on energy efficiency and precision engineering.

SHWETA SINGH received the M.Tech. and Ph.D. degrees in wireless communication from IIT (ISM) Dhanbad. She is an Assistant Professor with Manipal Institute of Technology, Bengaluru. With three years with Research and Development Division, L&T, she specializes in wireless, green communication, cognitive radio, energy harvesting, and the IoT. She has several publications, patents, and copyrights internationally in energy harvesting and IoT applications.

HIMANSHU RANJAN DAS received the M.Tech. degree in electronics engineering from Pondicherry University (A Central University), India, in 2015, and the Ph.D. degree from the Department of Electronics and Communication Engineering, School of Technology, North-Eastern Hill University (A Central University), India, in 2021. Currently, he is an Assistant Professor with the Department of Electronics and Communication Engineering, Haldia Institute of Technology, West Bengal, India. His research interests include silicon photonic, MEMs, and plasmonics and optoelectronic devices.

TANVIR HABIB SARDAR is an Associate Professor with the Department of Computer Science and Engineering, School of Engineering, Dayananda Sagar University, Bengaluru, India. With over 17 years of academic and research experience, he specializes in big data, machine learning, distributed computing, artificial intelligence, and emerging computing paradigms. He has published 62 Scopus-indexed research articles, authored and edited over ten books, and holds more than a dozen patents. His current research focuses on scalable machine learning models, including quantum computing, quantum-optimized intelligent systems, neuro-fuzzy computing, and deep learning, alongside distributed frameworks such as Hadoop. His work bridges theoretical foundations with real-world application, fostering innovation, problem-solving, and critical thinking among students and researchers. Beyond his scholarly contributions, he actively engages in curriculum development, accreditation processes, and mentoring initiatives that support future-ready engineering education.