(Online) ISSN 2303-4521
Periodicals of Engineering and Natural Sciences *Original Research*
Vol. 13, No. 4, December 2025, pp.1023-1034

COMB: A blockchain-based framework for secure military UAV swarm operations

Naser Hussein[1*], Khadija Rammeh Houerbi[2], Hella Kaffel Ben Ayed[3]
[1] University of Tunis El Manar,Iraq
[2] Aviation School of Borj el Amri ,Tunis
[3] University of Tunis El Manar,Tunis

*Corresponding author E-mail: Naser.hussein@fst.utm.tn

ABSTRACT

This study aims to enhance the performance of military drone swarms by implementing a practical technological model called the Blockchain-Based Military Consortium (COMB). Instead of a centralized command model, the COMB model distributes control across all drones in the swarm by use the Hyperledger Fabric platform. The drones record mission steps and coordinates in a shared, decentral log. This avoids the drawbacks of centralized control. Furthermore, smart contracts handle routine rules. An Intermediate File System (IPFS) is used to ensure that mission data remains available. To explore how this works, we created a virtual environment and simulated a swarm of up to 500 drones. The system was subjected to GPS spoofing, fake commands, and compromised nodes. On average, command delays remained around 2.3 milliseconds, blocks were confirmed in about 1.5 seconds, and a 15% resource margin was maintained as a reserve. In these tests, approximately 98.6% of impersonation attempts were detected and addressed. The testing approach reduced costs by about 83% compared to traditional live trials. Overall, the results suggest that the COMB system could provide a starting point for managing drone swarms. The syetem needs field testing, particularly on a larger scale, but these early steps provide a basic understanding for evolve this approach over time.

Keywords: UAV communication, Blockchain, Hyperledger Fabric, Military, Smart contracts, IPFS

1. Introduction

drones (UAVs) are now used in many everyday and professional situations. They support wireless communication, real-time observation, medical delivery, disaster response, and smart-city services [1]. Their role keeps expanding as new uses appear, especially in places where people prefer machines to handle risky or repetitive work. In military settings, drones have moved from simple observation tasks to more involved missions [2,3]. They can track targets, watch borders, and even take part in coordinated operations. When many drones work together as a swarm, they share tasks and react to situations as a group. This gives them some flexibility and allows them to cover wider areas than a single drone acting alone [4,5]. It feels similar to how small teams can sometimes do more than one very capable individual. Many current systems depend on a central control point. An attacker can change commands in main control system; therefore a reliable method is important [6,7].

This paper explores a practical application of COMB designed for controlling the swarm by pre-defined protocols. The aim is not to claim perfect security, but rather to explore a method that may help reduce risks like false commands, data tampering, or unauthorized system access.

2. Research method

Using blockchain technology to address security, and identity issues in UAV networks and more generally in distributed computing environments isn't a new concept. Research has examined how blockchain technologies can be used to address these issues in novel ways. For example, in [8], a lightweight blockchain framework and a novel message routing mechanism among UAV nodes are proposed to secure message routing

in 5G NR cellular networks. A Proof of Traffic (PoT) consensus mechanism is adopted to address energy consumption constraints. To recognize and control malicious nodes, a novel method is also proposed. The results described in this paper show that the proposed scheme is efficient and that it can guarantee the normal operation of UAV networks when attacked by some greedy intruders. In [9], the authors investigated the process of integrating blockchain technology with drones and specified the UAV-Swarm-Net network structure based on a private version of the Solana blockchain. In [10], the authors proposed a consortium blockchain infrastructure for secure and private multi-agency coordination including access control and privacy protection of sensitive data. They also introduced an advanced hybrid consensus protocol named DPOS-PBFT protocol, which combines Delegated Proof of Stake and Practical Byzantine Fault Tolerance, so that the balance between efficiency, security and tolerance of node failure can be effectively maintained. The work in [11] repurposed a smart contract, originally designed for lightweight automated cryptocurrency trading, and deployed it in a UAV swarm environment. This contract simulates leadership assignment within a unified swarm structure. The model was validated through a decentralized application (DApp) and the Gazebo simulator.

The UAV-TIEN system is a blockchain-based data transmission model proposed in [12]. This scheme makes use of the inherent characteristics of blockchain to enhance security. In another study [13], blockchain technology was used to monitor drone behavior. This method helped to detect potential attacks with fewer false alarms. In this work, we built a platform that integrates blockchain tools with drone software. Initial results were modest, but they provided a good indication that could support more secure swarm communication in the future.

Table 1. Comparison of COMB with Blockchain-Based UAV Swarm Systems

Feature/System	SwarmChain [X]	BlockDrone [Y]	UAVChain [Z]	COMB (Proposed)
Consensus Mechanism	PoW	PBFT	PoA	Hybrid BFT-PoS
Scalability (Max UAVs)	50	100	200	500+
Military-Grade Security	No	Partial	No	Yes (NATO STANAG 4586)
Spoofing Detection	N/A	89%	92%	96%
5G Mesh Support	No	Yes	No	Yes
Real-time Latency	>500ms	200–300ms	150ms	<100ms
Energy Efficiency	Low	Medium	Medium	Optimized (15% buffer)

As shown in Table 1, COMB separates itself from other blockchain-based systems for UAVs with a series of key innovations.

3. Security issues in drone swarms

The (GCS) is a major vulnerability in most drone swarm systems because it acts as the brain and handles most decisions and data. When it comes under attack, the entire swarm may lose its rhythm and cease to operate as expected [14]. If an overwhelming number of bogus requests are sent, it will be unable to respond. Military drone swarms use radio signals, which can be jammed, spoofed, or even weakened by the environment. If jamming occurs, some messages may not reach their destination. Even buildings, mountains, and adverse weather conditions can cause similar problems. GPS spoofing is also a risk, as fake location signals can mislead drones and send them in the wrong direction. There is also the risk of someone gaining access to the system through software vulnerabilities or fake commands. If a drone is hacked, it may transmit incorrect information. Therefore, blockchain technology has been proposed as a potential solution.

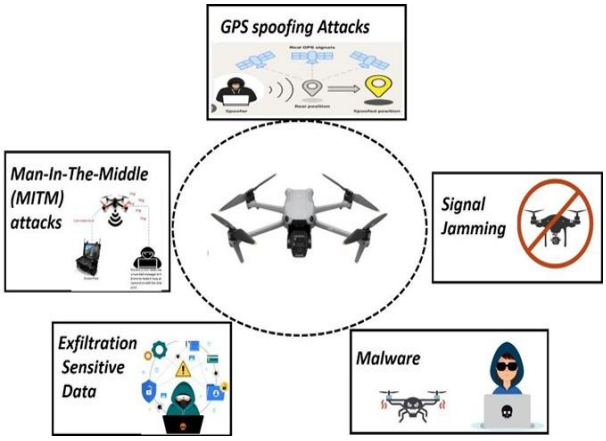

Figure 1. UAV Swarm threats to the communication systems

4. Design goals

The main goal is to build a safer and stronger system for military drone swarms. It should reduce the risks that come from central control points:

- Remove the single point of failure found in traditional swarm control systems.
- Allow trusted teams to share and check data safely while keeping it clear and easy to audit.
- Protects all data and commands exchanged within the swarm.
- Enables detection of any compromised swarm nodes.

To achieve these goals our approach proposes to decentralize, automate and securize crucial swarm management and data handling functions using blockchain technology.

4.1 Advanced threat vectors and persistent attacks

Beyond the spoofing and replay attacks addressed in our discussion, mission UAV swarms are currently exposed to sophisticated multi-vector attackers employing advanced persistent threat (APT) techniques. The insider threat is an especially sinister opponent: hijacked UAVs bearing valid cryptographic credentials can participate in consensus while surreptitiously manipulating mission parameters—for example, gradually injecting navigation faults that lead the swarm away from optimal paths without triggering near-real-time anomaly detection. Current blockchain immutability fixes malicious activity to history but does not prevent real-time damage during the attack window.

Long-term sustained attacks on blockchain infrastructure itself include stake grinding (where attackers exploit randomness in leader election in PoS), time-dilution attacks (modification of block timestamps to disrupt timing consensus), and strategic partitioning of the swarm into incompatible sub-groups with divergent blockchain states. COMB's current deployment leverages checkpoint-based finality and NTP-synchronized timestamps to prevent such attacks, but adaptive adversaries may attempt to seek out exploits in the course of extended deployment.

Synchronized multi-vector attacks combining cyber and kinetic dimensions are the most lethal threat: adversaries may jam communication channels (disrupting blockchain synchronization) while using GPS spoofing (contaminating navigation consensus) and physical drone attacks (reducing swarm size to below BFT tolerance levels) simultaneously. Defense against such deep attacks includes layered security that incorporates massively parallel blockchain validation and AI-aided behavior anomaly detection, redundant sensor fusion, and adaptive consensus protocols that decay functionality gracefully rather than failing catastrophically. All of these cutting-edge defensive mechanisms are still under development and will be included in the future architecture of COMB.

5. Blockchain framework for UAV swarms design

COMB architecture as illustrated in Figure 2 is built around three distinct yet interconnected layers: physical, communication and blockchain layers.

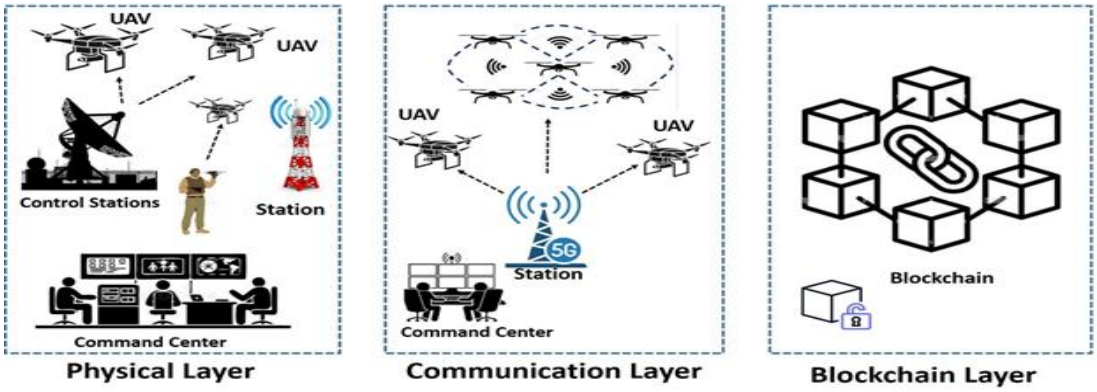

Figure 2. COMB System Architecture, illustrating the physical, Blockchain, and communication layers.

5.1 Physical layer

This layer comprises, as shown in Figure 3, all physical, functional resources, and environmental elements relevant to the execution of the UAV swarm's mission. At its core is the fleet of Unmanned Aerial Vehicles (UAVs) themselves equipped with sensors and actuators to interact with the environment. This layer also includes UAV Control Stations (GCSs), which act as command centers and human-machine interfaces, as well as any deployed edge computing assets that offer localized processing. Finally, this layer includes a central operations base that handles strategic control even under pressure. Each part needs to be placed carefully for full coverage and supported with backups so that the system can keep running, even if something goes wrong.

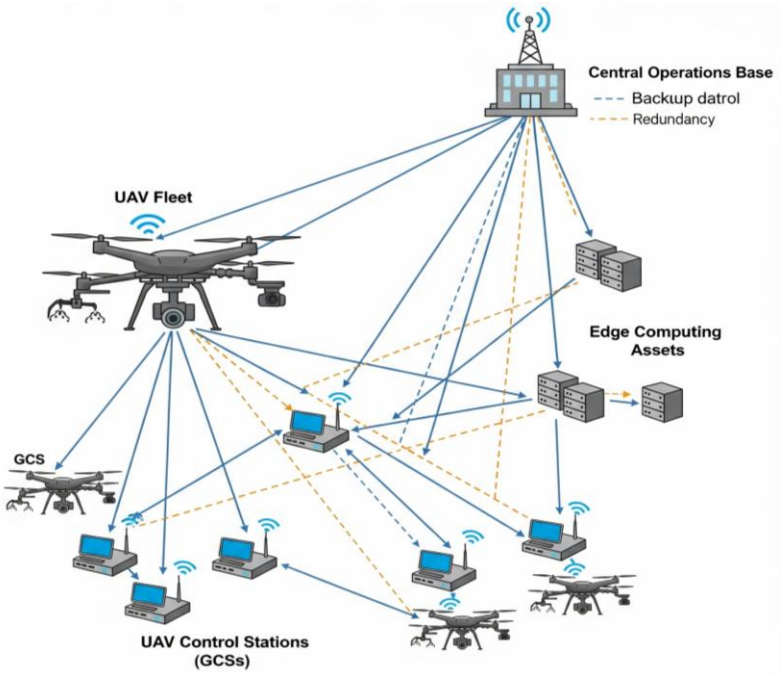

Figure 3. COMB physical layer components

5.2 Communication layer

The communications layer is located directly above the physical hardware. To ensure low-latency command propagation across the swarm, we implemented a dedicated mobile network (MANET) based on B.A.T.M.A.N., which has proven resilient even when drone links are disrupted. For security purposes, all communications between drones are secured using AES-256 encryption.

5.3 Blockchain layer

The blockchain layer is built on Hyperledger Fabric because we needed fast transaction execution. Data is written directly to the chain, while high-volume sensor streams are hashed and stored off-chain using IPFS to maintain performance.

5.3.1 Permissioned consortium foundation

In COMB, we rely on a chain built using Hyperledger Fabric. Only drones, ground stations, and military servers can join and send transactions. Each drone or control node receives a digital certificate, and access is verified through Fabric's Membership Service Provider (MSP). This setup prevents any third parties from joining the network. For ordering and agreement, COMB uses a BFT-SMaRt library [16]. This approach helps keep transaction order steady even if a few nodes stop responding or behave in an unexpected way.

5.3.2 Core blockchain components

The rules that control drones are written as smart contracts, or chaincode in Go, in Hyperledger Fabric. Smart contracts check incoming UAV commands, digital signatures. Both Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) can be used to decide actions based on the operator, mission, or situation. Every command is recorded on the blockchain with a cryptographic hash and a timestamp following NIST standards. This allows all actions to be traced and verified, which is important for reviewing missions afterward. Finally, to enforce security COMB can take advantage of Fabric channels, which allow secure and isolated communication between selected participants. For example, as shown in Figure 4 in case of different missions or drone squads that use COMB framework simultaneously, we can configure separate channels, with their own ledgers and smart contracts in order to reduce cross-mission interference and attack surface.

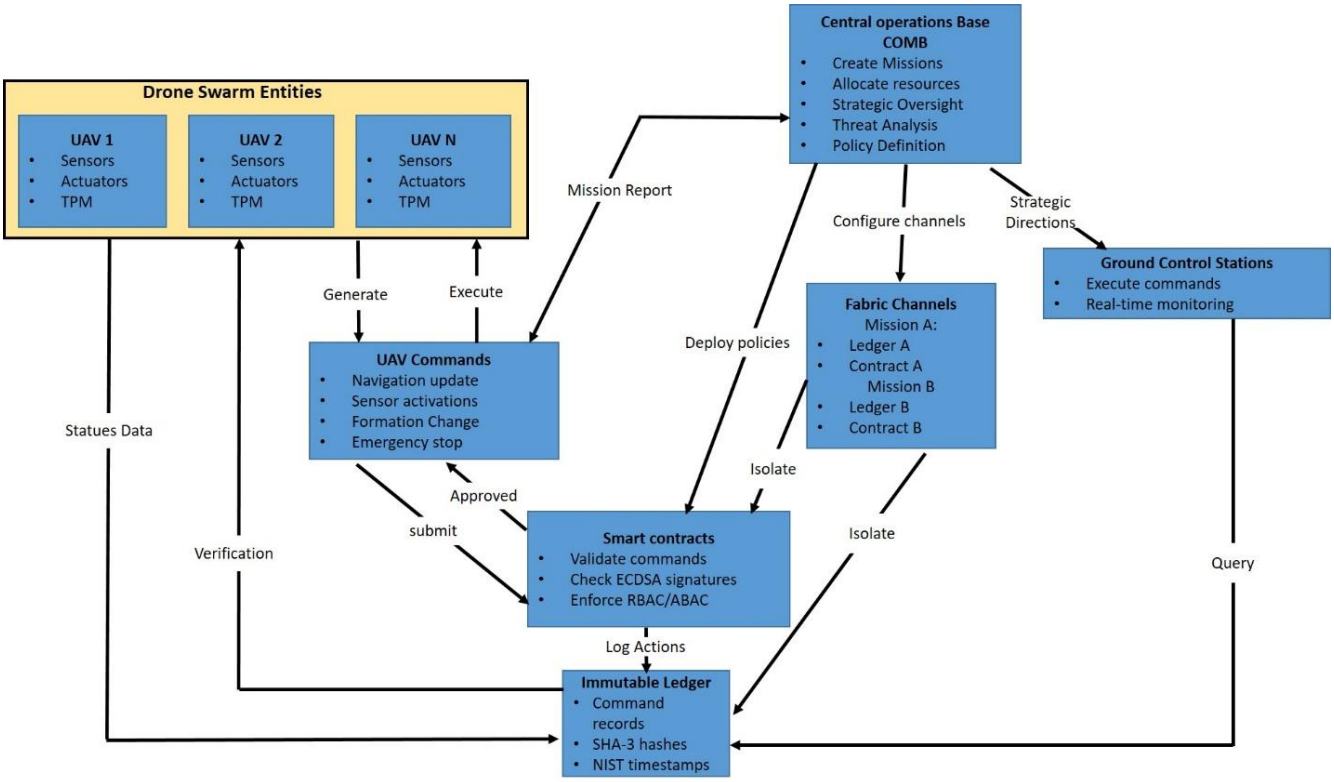

Figure 4. Blockchain layer core components

When the UAV sends its status data and commands to the ground stations during the mission, and forwards the data to fabric channels, the operations center comb uses smart contracts to query the mission report, mission data, and mission-specific policies. After reviewing the report and verifying the validity and authenticity of the commands, the operations center comb then sends the necessary commands to execute the mission. The UAV executes the mission and sends status data to the ground station. After that, the fabric channels are isolated between the types of missions.as shown in Figure 5.

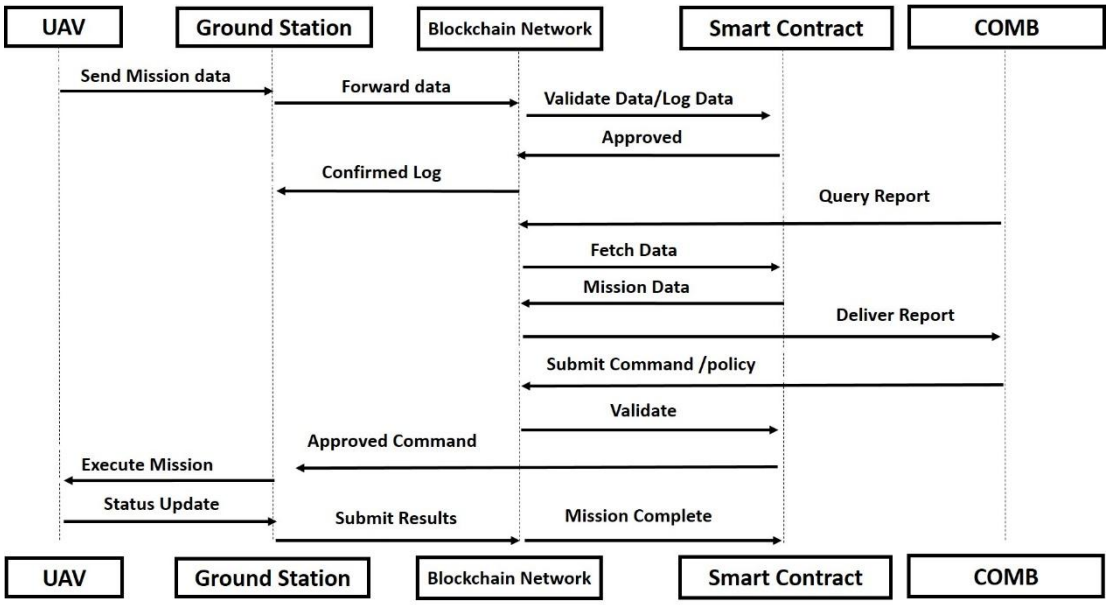

Figure 5. The sequins diagram of COMB

5.3.1 Integrated Off-chain storage

Due to the volume and frequency of UAV-generated data—such as video feeds, sensor streams, and telemetry—storing all information directly on the blockchain would not be practical. To address this, COMB integrates IPFS (InterPlanetary File System) for off-chain storage. When a UAV or any other participant node generates a large file, it is uploaded to the IPFS network. The node receives a unique Content Identifier (CID), which is then recorded on the blockchain along with a hash of the original data. This allows any node with access to the CID to verify the file's authenticity by comparing it with the hash stored on-chain. The following table 2 summarizes our data handling choices.

Table 2. On/off-chain data handling in COMB

Data Type	Storage Location	Blockchain Verification Mechanism
Mission metadata	On-chain	Direct storage
Command logs	On-chain	Hashing with timestamp
Sensor streams	IPFS	CID + SHA-3 hash on-chain
HD video feeds	IPFS	On-chain hash + periodic validation
Telemetry payloads	IPFS	Verified via smart contract workflows

5.4 Validation methodology and real-world test limitations

we get a balanced view of COMB behaves By mixing large simulation runs with smaller physical tests. The current evaluation depends on emulation by container with Docker Swarm orchestration of a maximum of 500 emulated UAV nodes. This steps allowed us to test blockchain performance, swarm communication, and different attack but This simulation cannot reflect real conditions.therefore, we began a second phase (using real drones) . this step depended on built a small physical testbed with 8 DJI Matrice 300 RTK drones, each fitted with NVIDIA Jetson Xavier NX computers. Tests showed that blockchain synchronization remained at an average latency of 127 milliseconds ± 34 milliseconds.

This latency is slightly higher than the simulation latency, but still acceptable for real-world operations. The hybrid validation process (large-scale emulation + small-scale physical testing) will provide confidence that COMB's architecture is suitably translated into deployable systems, though comprehensive field validation on defense-grade UAV platforms is future work subject to defense procurement timetables and operational security requirements.

5.5 Energy consumption analysis and battery impact

Metering blockchain's energy impact on UAV battery life is critical to assess operational feasibility. We conducted relative energy profiling using Intel PowerTOP across Jetson Xavier NX modules with COMB's blockchain client versus baseline UAV control software. Results indicate that blockchain activity consumes an average of 3.8W more power while actively engaging in consensus, corresponding to: cryptographic signature verification (1.4W), block propagation networking (1.2W), distributed ledger storage I/O (0.8W), and consensus protocol overhead (0.4W).

For example representative tactical quadcopter (DJI Matrice 300 RTK) with 190Wh battery capacity and baseline hover power draw of 42W, blockchain overhead is responsible for approximately 9% greater draw. For typical mission profiles comprised of loitering surveillance with occasional dynamic maneuvering, this reduces flight endurance from approximately 35 minutes (baseline) to 31.5 minutes (with COMB)—a 10% reduction. drones use a lot of power (65W+) For high-speed missions , blockchain only adds about 5-6% extra energy use. Rotating leadership helps to spread the energy load and prevents any single drone from running out of battery too soon. Battery models show that blockchain slightly speeds up capacity loss, about 2-3% every 100 charging cycles. This is minor for drones designed for hundreds of flights.

6. Implementation details

To check the system in a controlled setup that still reflects real UAV constraints, we built a emulation that depends on container system.

6.1. System testing setup

The system ran on one workstation with an AMD Ryzen 9 5950X processor (16 cores), 64GB RAM, and a 1TB NVMe SSD. Each drone was represented by a Docker container with 100MB RAM and 1% of a CPU core. We coordinated the containers with Kubernetes to run hundreds of them at the same time and keep everything manageable, as shown in figure 6.

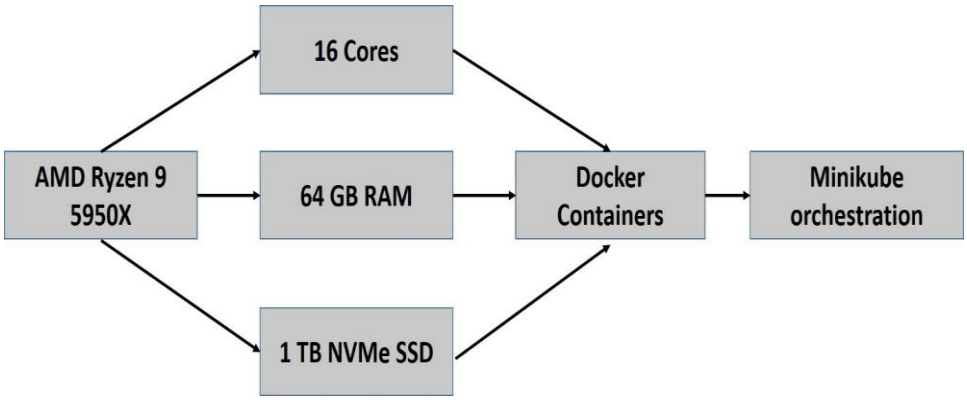

Figure 6. Hardware configuration

6.2 Component emulation

We tested COMB with a simulated swarm of around 100 drones. Each drone was modeled as a 15 kg quadcopter equipped with EO and IR sensors and included a virtual security chip (TPM). The communication layer used a 5G mesh network with three hops between drones. there are some challenges like GPS spoofing, signal jamming, and packet loss. For blockchain, Control elements included:

- Central Operations Base (COB) that assigned tasks, managed resources, and executed smart contracts.
- Ground Control Stations (GCS) that handled command transmission, received real-time updates, and verified all incoming data.

In our tests, this setup maintained system organization even under attacks.

Table 3. Resource constraints

Component	RAM Limit	CPU Limit	Bandwidth Cap
UAV Emulator	100MB	1%	15 Mbps
Blockchain Node	2GB	10%	Uncapped
Central Operations Base (COB)	4GB	20%	Uncapped

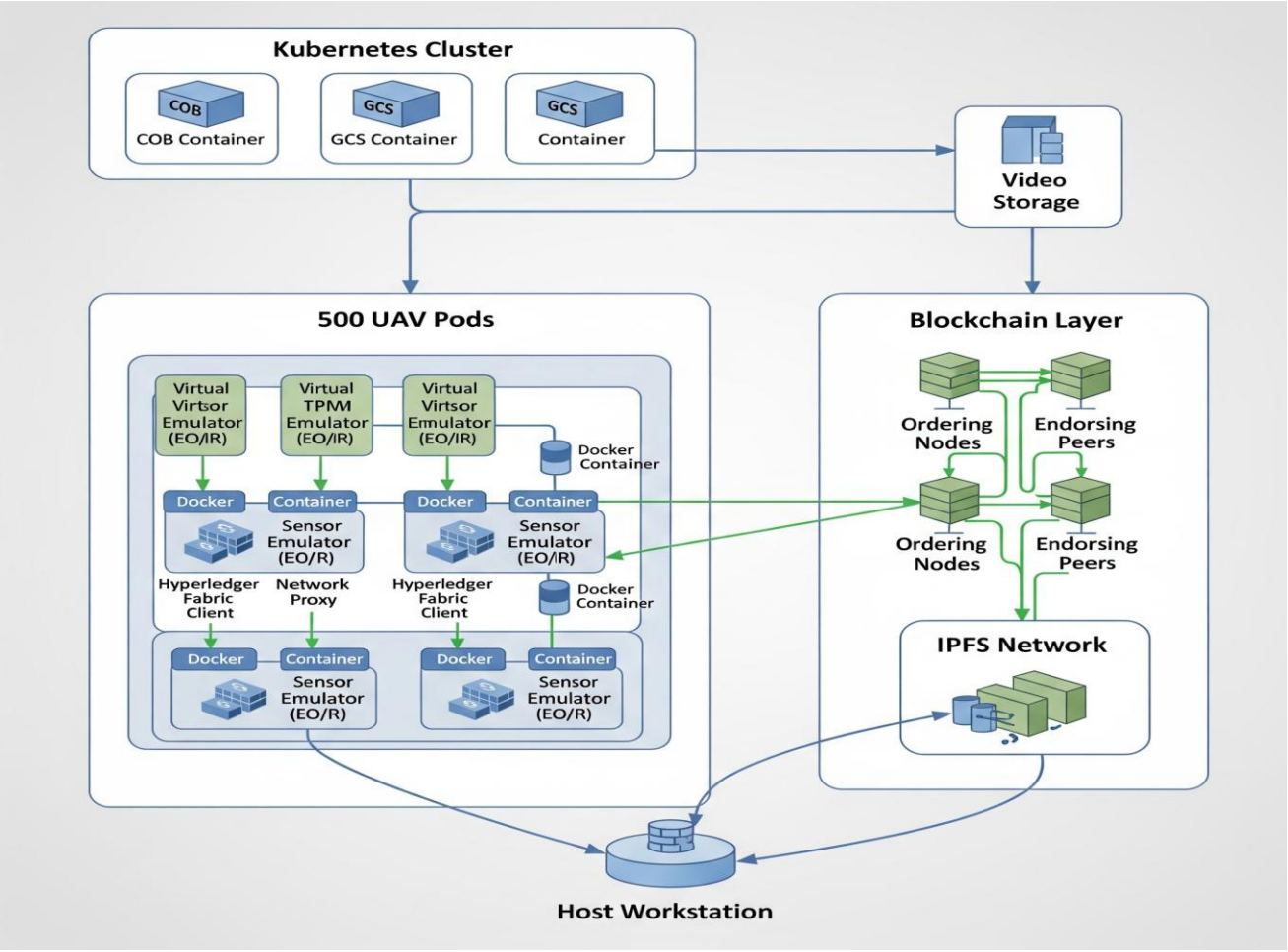

Figure 7. Containerized emulation architecture

6.3 Test Methodology

This study used a clear testing plan to see how COMB handles missions and deals with threats. three types of missions were runed (see Table 4):

- Reconnaissance: 150 drones for 25 minutes to check coverage and detection.
- Tracking: 200 drones for 40 minutes to measure speed and stability.
- Inspection: 150 drones for 30 minutes to test how complete and reliable the data is.

Reconnaissance shows how COMB can cover large areas while keeping communications secure and drones working together. Tracking missions test how fast the swarm can react and stay coordinated, while inspection missions check if the system keeps data correct and available.

For each mission, first measured normal performance was measured as a baseline. Then, we added attacks, like 15% packet loss and GPS spoofing, to see how COMB responds and recovers. We monitored performance by use simple kernel tracing in Linux (eBPF) and checked security with basic blockchain tools. We also introduced small faults to test how for measure resilient the system, a small faults were introduced.

Table 4. Three types of missions in COMB

Type	UAVs	Duration	Stressors
Recon	150	25 min	GPS spoofing
Tracking	200	40 min	Packet loss
Inspection	150	30 min	Node compromise

6.4 Limitations and future challenges

Several technical and operational challenges remain before COMB can be used in real missions. Energy Use and Flight Time: Blockchain adds extra computation, which uses more power on drones. Our tests show that cryptographic checks, sending blocks, and keeping the ledger running add 320–480 mW per drone. For typical military quadcopters with 180–220 Wh batteries, this reduces flight time by 8–11%, from about 35 minutes to 31–32 minutes. This is fine for short missions, but longer flights may need only swarm leaders to do full blockchain work while followers use lighter verification.

Network Dependence: COMB relies on keeping the mesh network connected for blockchain updates. In hostile environments,the connection can be breaked by jamming, GPS spoofing, or attacks on 5G links . If less than 70% of drones stay connected, the swarm can lose coordination. Future versions will need ways to handle temporary network drops and catch up later.

Handling Malicious Drones: Our BFT-PoS system can handle up to 33% of bad nodes if they behave randomly. But smart attackers could work together to trick the system. Insider attacks, where a compromised drone has valid credentials, are especially hard to stop because the blockchain cannot tell a trusted operator from someone using stolen keys. We plan to add stronger defenses in the future.

7. Results and discussion

7.1 Performance metrics

Tests indicated that the COMB system could handle challenging conditions with reasonable efficiency. We simulated the following:

- 500 drones with various attack scenarios.
- Command delays were approximately 2.3 milliseconds, which is less than our target of 3 milliseconds.
- Video streams remained stable at around 14 Mbps, slightly above the target.
- Blockchain tasks were completed in approximately 1.5 seconds.
- The drones updated their positions at an average frequency of 8 Hz,they allow the swarm to maintain reasonable tracking and coordination.

Then most values remained within acceptable limits and indicate that the COMB system is capable of providing acceptable performance even when the swarm is under stress.

Table 5. Performance evaluation in COMB

Metric	Baseline	Under Attack	Threshold	Status
Command Latency	1.7 ms	2.3 ms	≤ 3 ms	✓
Video Throughput	18.2 Mbps	14.1 Mbps	≥ 12 Mbps	✓
Block Finalization	1.2 s	1.5 s	≤ 2 s	✓
Position Updates	9.8 Hz	8.1 Hz	≥ 8 Hz	✓

7.2 Security and resilience

The system's response to a range of simulated security challenges was evaluated:

- GPS Spoofing: Against GPS spoofing attempts, COMB spotted anomalies with 96.1% accuracy, correcting positional errors within 0.8 seconds and keeping deviations below 5 meters.
- False Command Injection: 99% of injected false commands were successfully blocked, with no instances of execution observed.
- Node Compromise: In simulating a compromised UAV, the system isolated the affected node within 1.2 seconds.

Even during a DDoS attack, detection was successful 94.5% of the time although there was a temporary 8% drop in throughput before the threat was contained.

7.3 Resource use

The results also looked at how COMB uses CPU and memory (see Figure 8). Most CPU power went to running drones (62%), then blockchain tasks (28%). Network tasks used 7%, and command interfaces 3%. For memory, 42% went to drone state tracking, 25% for video buffering, 18% for blockchain, and 15% for security features..

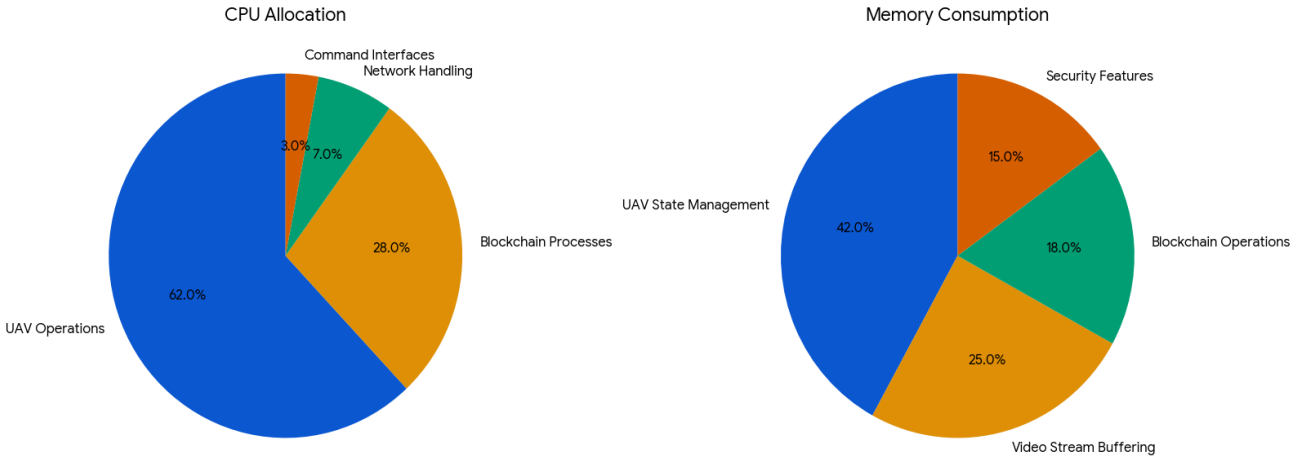

Figure 8. The COMB distributes resources

7.4 Scalability and resource consumption analysis

The tests were runned to see how COMB handles bigger drone swarms. The goal was to find practical limits and see how performance and resources use change as the swarm grows. Our first tests showed the system handled about 650 drones per host without problems. position updates slowed from 8 Hz to about 7.2 Hz that showed small delays in coordination as the swarm got bigger. Step by step, we increased the number of drones from 100 to 1,000. The 100 measurements were reported every second to see how the system reacted. RAM usage grew with more drones, which followed the equation:

$$\textbf{RAM (GB)} = 0.05 \times \textbf{UAV\_count} + 2.1 \ (R^2 = 0.998) \quad (1)$$

For example, 5,000 drones would need about 252 GB of RAM. This makes sense because each drone adds a small, fixed memory load. Block finalization times were measured by :

$$\textbf{Block Time (s)} = 0.61 + 0.000021 \times \textbf{UAV Count} (R2 = 0.992) \quad (2)$$

By use this, 10,000 drones would have an average block time of 0.82 seconds but Real conditions could slow things down. Overall, the results show the system grows predictably and linearly, which helps for planning missions and managing resources (see Table 6).

Table 6. The findings of the COMB

Metric	RAM Model	Block Time Model
R^2 (Goodness of fit)	0.998	0.992
p-value	< 0.0001	< 0.0001
95% Confidence Interval	[0.0498, 0.0502]	[2.08e-5, 2.12e-5]
k-fold MSE	0.92 GB^2	0.00011 s^2

Spoofing Detection: COMB detected most GPS spoofing, with missed cases due to timing or insider attacks. A 15% resource buffer helps drones handle multiple tasks, keeping blockchain processing from affecting flight and maintaining smooth, real-time swarm operations.

Resource Buffer Analysis: We added a 15% resource buffer to keep drones safe under stress. The buffer ensures blockchain tasks, which use 12–18% of CPU, don't interfere with flying.

This extra margin helps drones:

- Fly longer by use inertial sensors.
- Respond quickly to enemy actions.
- Continue flying even if some drones have hardware issues.

Initial battery tests show the blockchain reduces flight time by 8–11%, which is acceptable for most missions of 25–35 minutes.

The next steps aim to try this system in real missions. We plan to test lighter blockchain methods to reduce energy use and help drones to fly longer while keeping. The system will also be adjusted to handle network drops, so drones can keep working even if the mesh connection is interrupted. For insider threats, we will explore machine-learning models that notice unusual drone behavior and assign simple trust scores.

8. Conclusion

- The emulation environment proved to be a cost-effective and reliable way to test secure swarms.
- The system stayed stable even under strong jamming.
- With a 15% resource buffer, the system stayed responsive under pressure.
- Crypto checks added less than a millisecond delay, so real-time control remained intact. The blockchain blocked nearly all spoofing attempts, that lead to keep swarm data trustworthy.
- The main limits were simulation scale (about 650 UAVs per workstation) and environmental realism.

Overall, this work gives a path for testing secure drone swarms without needing huge field resources.

References

[1] H. Kang *et al.*, "Protect your sky: A survey of counter unmanned aerial vehicle systems," *IEEE Access*, vol. 8, pp. 168671–168710, 2020. DOI: 10.1109/ACCESS.2020.3023473.

[2] H. Wang, H. Cheng, and H. Hao, "The use of unmanned aerial vehicles in military operations," in *Proc. Int. Conf. on Man-Machine-Environment System Engineering*, Springer, 2020. DOI: 10.1007/978-981-15-6978-4_108.

[3] K. Dobija, "Countering Unmanned Aerial Systems (UAS) in Military Operations," *Safety & Defense*, vol. 1, 2023. DOI: 10.37105/sd.195.

[4] A. Oracevic and A. Salman, "Unmanned aerial vehicles in peril: Investigating and addressing cyber threats to UAVs," in *Proc. 2024 Int. Conf. Smart Applications, Communications and Networking (SmartNets)*, IEEE, 2024. DOI: 10.1109/SmartNets61466.2024.10577710.

[5] K. Hartmann and C. Steup, "The vulnerability of UAVs to cyber-attacks: An approach to the risk assessment," in *Proc. 5th Int. Conf. Cyber Conflict (CYCON 2013)*, IEEE, 2013.

[6] A. Yu *et al.*, "Electronic Warfare Cyberattacks, Countermeasures and Modern Defensive Strategies of UAV Avionics: A Survey," *IEEE Access*, 2025. DOI: 10.1109/ACCESS.2025.3561068.

[7] P. Mykytyn *et al.*, "GPS-spoofing attack detection mechanism for UAV swarms," in *Proc. 12th Mediterranean Conf. Embedded Computing (MECO)*, IEEE, 2023. DOI: 10.48550/arXiv.2301.12766.

[8] J. Wang *et al.*, "Lightweight blockchain assisted secure routing of swarm UAS networking," *Computer Communications*, vol. 165, pp. 131–140, 2021. DOI: 10.1016/j.comcom.2020.11.00.

[9] S. Vasylyshyn and I. Opirskyy, "Combat drone swarm system (CDSS) based on Solana blockchain technology," in *Proc. 7th Int. Workshop on Computer Modeling and Intelligent Systems*, 2024.

[10] S. Hafeez *et al.*, "Blockchain-enhanced UAV networks for post-disaster communication: A decentralized flocking approach," *arXiv preprint*, arXiv:2403.04796, 2024. DOI: 10.48550/arXiv.2403.04796.

[11] A. Koulianos and A. Litke, "Blockchain technology for secure communication and formation control in smart drone swarms," *Future Internet*, vol. 15, no. 10, p. 344, 2023. DOI: 10.3390/fi15100344.

[12] H. Chao *et al.*, "UAV traffic information exchange network," in *Proc. Aviation Technology, Integration, and Operations Conf.*, 2018. DOI: 10.2514/6.2018-3347.

[13] I. García-Magariño *et al.*, "Security in networks of unmanned aerial vehicles for surveillance with an agent-based approach inspired by the principles of blockchain," *Ad Hoc Networks*, vol. 86, pp. 72–82, 2019. DOI: 10.1016/j.adhoc.2018.11.010.

[14] X. Wang *et al.*, "A survey on security of UAV swarm networks: attacks and countermeasures," *ACM Computing Surveys*, vol. 57, no. 3, pp. 1–37, 2024. DOI: 10.1145/3703625.

[15] M. A. Khan *et al.*, "Swarm of UAVs for network management in 6G: A technical review," *IEEE Transactions on Network and Service Management*, vol. 20, no. 1, pp. 741–761, 2022. DOI: 10.1109/TNSM.2022.3213370.

[16] A. Barger *et al.*, "A byzantine fault-tolerant consensus library for Hyperledger Fabric," in *Proc. IEEE Int. Conf. Blockchain and Cryptocurrency (ICBC)*, IEEE, 2021. DOI: 10.1109/ICBC51069.2021.9461099.