RESEARCH & INNOVATION SHOWCASE

CIA-SecEval: A Simulation Framework for Evaluating Algorithmic Trade-offs in Multi-Drone Networks

Researcher: **Viktor Salihu** (S021136N) • Project Supervisor: **Dr. Viraj Dawarka** • Department of Computer Science

1. What is the Problem?

Autonomous multi-drone networks and Flying Ad-Hoc Networks (FANETs) form the backbone of modern decentralized fleet coordination. However, these environments are inherently exposed to adversarial security risks including traffic interception, message spoofing, and routing disruptions.

While implementing core security policies (the **CIA Triad**: Confidentiality, Integrity, and Availability) provides defense, it introduces heavy algorithmic footprints—causing processing bottlenecks, message growth, and link saturation. Currently, system architects lack any unified test environments to evaluate how security layers degrade fleet stability.

2. Why is this Problem Important?

Multi-agent UAV networks handle high-stakes operational mandates: emergency communication restoration, disaster zone diagnostics, and commercial infrastructure inspection. Failures are high-impact:

- **Insufficient Controls:** Risk vehicle hijacking, telemetry manipulation, and operational compromise.
- **Unmanaged Security Bloat:** Induces packet latency spikes and structural queue delays, triggering physical fleet collisions during flight path updates.

> *The ultimate challenge is establishing an empirical equilibrium point where security guarantees can be adjusted dynamically based on actual network traffic and swarm bounds.*

3. Current Literature Gaps

Existing scientific methodologies evaluate performance vectors in total isolation:

- **Aerodynamic Simulators:** Optimize strict flight mechanics or low-level navigation rules, completely disregarding cyber-security overheads.
- **Pure Cryptographic Papers:** Mathematically establish protocol robustness but rely on unrealistic, stable communication links with infinite computation pools.

Framework Platform	Security Analysis	Network Coupling
Standard UAV Toolsets	Absent	Static Range Only
Isolated Crypto Proposals	Strictly Verified	Decoupled/Ignored
CIA-SecEval Platform	**Fully Integrated**	**Dynamic Graph Coupling**

4. Methodology & Architecture

CIA-SecEval delivers a lightweight, configuration-driven simulation structure using `SimPy` event loops and `NetworkX` topological graphs to isolate security overhead metrics from flight control variables.

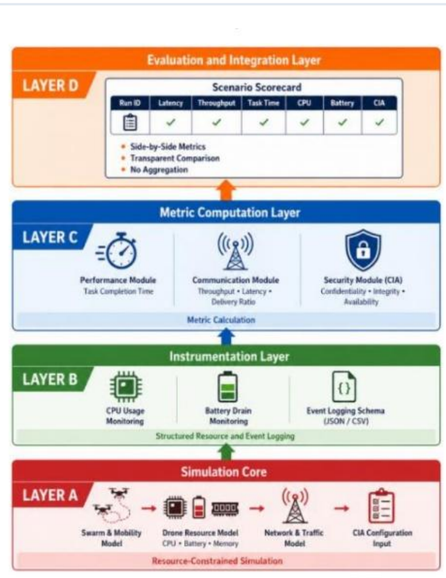

Figure 1: Modular architecture mapping processing overlays down to physical resource proxies.

5. Quantitative Experimental Results

Platform evaluation was benchmarked across diverse swarm limits to map data transport efficiency directly against computing stress indices.

Test Setup / Profile	Delivery Ratio (PDR)	Avg Latency	CPU Proxy Cost
Small Mesh Swarm (Baseline)	97.6%	29.78 ms	0.71
Small Mesh Swarm (CIA-High)	**100.0%**	**28.77 ms**	**15.86**
Constrained Fleet (Baseline)	79.3%	150.44 ms	0.78
Constrained Fleet (CIA-Medium)	**96.7%**	**167.14 ms**	**5.93**
Constrained Fleet (CIA-High)	90.7%	173.06 ms	17.84

96.7%
OPTIMAL PDR (CIA-MEDIUM)

22.8x
CPU PROXY SPIKE

6. Key Technical Insights & Discussion

The Over-Protection Paradox: Forcing maximal settings (`CIA-High`) inside congested channels actively degraded final throughput metrics (dropping reliability from 96.7% to 90.7%). The aggressive verification cycles and multi-path repetitions saturated buffers, causing packet dropouts.

Why CIA-SecEval Wins: It explicitly demonstrates that the most secure software configuration can become the primary threat vector to operational flight safety, enabling precise curve mapping prior to live deployment.

7. Conclusion & Future Work

Conclusion: The framework fulfills its criteria as a high-fidelity, resource-conscious test sandbox. It proves that multi-UAV safety relies on adaptive, context-driven parameters rather than unilateral encryption policies.

Future Direction: Mapping abstract software metrics to raw CPU cycle delays using physical embedded nodes (Raspberry Pi Zero/Jetson Nano blocks running OpenSSL) and creating real-time routing spoofing vectors.