Adaptive Blockchain Consensus for Military UAV Data Transfer Authentication

1st Naser Abbas Hussein
LIPAH Laboratory
Faculty of Sciences of Tunis
University of Tunis El Manar
Tunis, 2092,Tunisia
Naser.hussein@fst.utm.tn

2nd Khadija Rammeh Houerbi
SACES Research Unit (UR17dn01)
Aviation School of Borj el Amri
Ministry of Defense
Tunisia
khadija.ramah@gmail.com

3rd Hella Kaffel Ben Ayed
LIPAH Laboratory
Faculty of Sciences of Tunis
University of Tunis El Manar
Tunis, 2092,Tunisia
Hella.kaffel@fst.utm.tn

***Abstract*—Secure authentication of data in military unmanned aerial vehicle (UAV) networks must be able to adapt dynamically to changing threat environments and satisfy energy efficiency constraints. In this paper, we present a blockchain consensus architecture that can adaptively switch between PoA and PBFT algorithms in a dynamic way during real-time online threat assessment. The presented architecture overcomes the natural trade-off between energy and security guarantees in low-power military communication networks. Our design employs a threat-aware coordinator that evaluates multiple vector attack threats, including RF jamming, GPS spoofing, Byzantine node malicious acts, and physical attacks. The framework adapts the most appropriate consensus algorithm, which is efficient PoA under normal conditions and secure PBFT if the threat increases. Simulation results demonstrate that the proposed adaptive algorithm can save 25–30% energy compared to the PBFT static one, which has 89% fault tolerance in a threat environment. The system reaches 0.37 transactions per second (tps) throughput and 67% energy efficiency with varying network sizes. Statistical testing ($p < 0.05$) further validates significant improvement over static consensus algorithms and random switching baselines. This method illustrates a practical model to balance security and efficiency trade-offs in adversarial military UAV blockchain networks.**

***Index Terms*—blockchain consensus, military UAV networks, Byzantine fault tolerance, energy optimisation, threat-adaptive systems.**

I. INTRODUCTION

Forward military operations increasingly rely on unmanned aerial vehicle (UAV) networks for intelligence, surveillance, and tactical coordination in contested environments. Distributed systems like these face major cybersecurity challenges, as attackers apply sophisticated electronic warfare techniques like GPS spoofing, RF jamming, and coordinated cyber attacks to disrupt mission-critical data transmissions [1]–[3]. Traditional centralised authentication schemes are prone to single points of failure, and conventional blockchain consensus algorithms are inherent bottlenecks to defence use. Proof-of-Work paradigms consume excessive computational resources unsuitable for energy-constrained UAV platforms, and static consensus architectures fail to adapt to evolving threat scenarios [4], [5]. Military UAV networks function with diverse mission phases—ranging from routine patrol operations involving low-security overhead to active combat scenarios that require utmost Byzantine fault tolerance against hostile actors [6], [7]. Existing blockchain solutions for UAV networks typically employ static consensus mechanisms that either sacrifice energy efficiency for security or resilience for performance, making suboptimal trade-offs for changing operational demand [8], [9]. This research contribution is twofold: (1) the first threat-adaptive consensus coordinator that switches between PoA and PBFT dynamically based on real-time threat assessment, (2) comprehensive energy modeling of UAV blockchain service delivery within an adversarial context, (3) statistical validation of 25-30% energy savings while being fault tolerant, and (4) an applied paradigm for adaptive consensus deployment in military networks.

II. RELATED WORK

Recent advances in blockchain consensus protocols for UAV networks have focused on addressing the inherent trade-offs between security, energy efficiency, and performance under dynamic operating conditions. Huang and Huang [10] developed theoretical models of chained HotStuff consensus algorithm performance impacts by CSMA/CA channel access protocols, emphasising how electromagnetic interference affects consensus failure probability in UAV ad hoc networks through extensive NS3 simulations. Onukak et al. [11] put forward a Reputation-enhanced Practical Byzantine Fault Tolerance Algorithm (RePA) for resisting capture node attacks in UAV networks, integrating reputation systems into consensus algorithms and achieving enhanced resilience against Byzantine node behaviour. Program — IEEE Wireless Communications and Networking Conference - IEEE WCNC 2025. Kumar et al. [12] put forward a blockchain integration framework for UAV networks that integrates Elliptic Curve Diffie-Hellman (ECDH) with Secure Hash Algorithm (SHA) for maintaining data integrity and securing key exchange in peer-to-peer UAV communications. Towards a secure and resilient unmanned aerial vehicles swarm network based on blockchain - Zhou - 2024 - IET Blockchain - Wiley Online Library. Han et al. [13] introduced DTPBFT, a secure and dynamic blockchain consensus algorithm particularly designed for UAV swarms with adaptive techniques to tackle the unique requirements of aerial mobile networks. Augmenting Data Security in

IoT-based UAV Networks using Blockchain Integration — Engineering, Technology & Applied Science Research.

III. PROPOSED METHODOLOGY

The proposed adaptive consensus system integrates various components to achieve threat-aware blockchain authentication in military UAV networks. Our solution involves the use of consensus algorithms, threat modelling, adaptive coordination logic, and comprehensive evaluation protocols designed to validate system performance under realistic operational scenarios.

A. Dual Consensus Algorithm Implementation

There are two complementary blockchain consensus mechanisms implemented in the system, which are customised to military UAV constraints. The Proof-of-Authority (PoA) implementation employs a protocol based on Clique with pre-authorised validator nodes, with optimised cryptography operations and minimal network message overhead. The authority is chosen through round-robin scheduling with partition-aware failover techniques to provide consensus under network fragmentation occurrences. The Practical Byzantine Fault Tolerance (PBFT) implementation executes a three-phase consensus protocol with pre-prepare, prepare, and commit phases with enhanced message validation procedures. The PBFT module incorporates dynamic view change mechanisms and Byzantine node detection algorithms that are tolerant of up to $\frac{n-1}{3}$ malicious nodes, where n is the total network participants. The algorithms incorporate energy consumption models using ARM Cortex-A72 processor specifications common in military UAV platforms, with computational overhead models for cryptographic operations, network communication overhead, and consensus-specific processing requirements. Implementation includes modular interfaces for algorithm switching at runtime without disrupting the blockchain state.

B. Multi-Vector Threat Modelling Engine

The threat analysis module includes a comprehensive modelling framework that examines four primary attack vectors to military UAV operations. RF jamming threat model analyses frequency band targeting patterns, signal power measurements, and geospatial coverage calculations, using energy impact models for adaptive frequency hopping and signal processing countermeasures. GPS spoofing detection algorithms monitor signal strength inconsistencies, temporal consistency violations, and cross-referencing across multiple positioning systems to develop sophisticated threat scoring mechanisms. Byzantine node behaviour analysis relies on message delay pattern recognition, consensus participation monitoring, and coordination detection algorithms that identify synchronised malicious behaviour across network participants. The composite threat score is calculated by a weighted aggregation function: $S_{\text{threat}} = w_{\text{RF}} \cdot T_{\text{RF}} + w_{\text{GPS}} \cdot T_{\text{GPS}} + w_{\text{Byz}} \cdot T_{\text{Byz}} + w_{\text{Phys}} \cdot T_{\text{Phys}}$, where each threat component is normalized to $[0, 1]$, and the weights sum to unity ($\sum_i w_i = 1$). RF jamming threat T_{RF} is quantified by the degradation of the signal-to-interference ratio; GPS spoofing threat T_{GPS} measures the magnitude of the positioning error; the Byzantine threat T_{Byz} represents the fraction of detected malicious nodes; and the physical attack probability T_{Phys} is derived from proximity sensor readings. The coordinator initiates the switching from PoA to PBFT when $S_{\text{threat}} > \theta_{\text{high}} = 0.7$, whereas reverting to PoA happens when $S_{\text{threat}} < \theta_{\text{low}} = 0.4$. These thresholds are calibrated through a preliminary security analysis.

C. Adaptive Consensus Coordination Logic

The coordination mechanism employs a multi-criteria decision algorithm that continuously evaluates network conditions, threat levels, and energy constraints to determine optimum consensus protocol selection. The decision logic employs dual-threshold switching mechanisms with tunable parameters for PoA-to-PBFT transitions based on composite threat score analysis, network stability analysis, and energy budget analysis. The coordinator maintains both consensus algorithms' energy consumption rate logs and employs predictive energy management algorithms that project operating time for various consensus options. Switch triggering employs hysteresis mechanisms to prevent oscillatory protocol switching behaviour by requiring extended threat conditions for minimum time intervals before consensus switching. In order to prevent the system from entering into oscillatory switching behavior, it implements a dual-threshold hysteresis mechanism with temporal constraints. Consensus escalation is triggered only when the threat score exceeds the upper threshold $\theta_{\text{high}} = 0.7$ and remains above this level for a dwell time of $t_{\text{dwell}} = 30$ seconds. Conversely, de-escalation occurs when the threat score falls below the lower threshold $\theta_{\text{low}} = 0.4$ after a sustained period of reduced threat. This establishes a hysteresis band of $\theta_{\text{high}} - \theta_{\text{low}} = 0.3$, ensuring that transient fluctuations in the threat level do not induce unnecessary protocol transitions. Furthermore, a minimum inter-switch interval of 60 seconds prevents rapid oscillations, allowing the network to stabilize after any consensus change while still remaining responsive during genuine threat escalations. Algorithm 1 codifies the adaptive switching logic. The coordinator continuously monitors S_{threat} (as computed in Section III-B) and evaluates switching conditions every $\Delta t = 10$ seconds. Transitions between states occur only if the threshold criteria remain satisfied for longer than the dwell time t_{dwell}, and if at least a minimum inter-switch interval of $t_{\min} = 60$ s has elapsed since the last transition.

The algorithm maintains a state-history buffer to implement hysteresis and introduces additional safeguards that prevent switching during active consensus rounds. This ensures atomic protocol transitions without compromising blockchain integrity.

D. Experimental Evaluation Framework

The evaluation approach employs Monte Carlo simulation techniques across a range of network configurations with varying node counts to achieve statistical validity through independent simulation runs. Threat scenario generation progresses through realistic mission stages with increasing threat

probabilities and complexity patterns that replicate real-world military operational contexts. Network condition simulation includes dynamic partition probability modelling, Byzantine node ratio fluctuations, and RF interference level changes to replicate real-world military communication challenges. The platform employs full baseline comparison protocols that include static consensus implementations and control mechanisms to enable rigorous performance benchmarking. The simulation framework was implemented in Python 3.9 using the `SimPy` discrete-event simulation library for network modeling, and `NumPy` for statistical analysis. Energy consumption parameters were derived from ARM Cortex–A72 specifications: 2.5 W idle power, 5.2 W during cryptographic operations, and 1.8 W for network transmission at 250 kbps.

The PBFT message overhead was modeled as $\mathcal{O}(n^2)$ with 128-byte messages, while PoA required $\mathcal{O}(n)$ messages of 64 bytes. Each simulation run executed 1000 transactions over 3600 simulated seconds, with Poisson-distributed transaction arrivals: $\lambda = 0.3$ tx/s. Network propagation delay was set to 50 ± 20 ms with a packet loss rate of 2% under normal conditions, increasing to 15% during a jamming attack.

IV. RESULTS AND DISCUSSIONS

Comparison outcomes are presented in four subsections: comparative analysis of energy efficiency, fault tolerance performance under threats, throughput and latency measurements, and statistical verification of adaptive behavior.

A. Analysis of Energy Efficiency Performance

Figure 1 illustrates the adaptive blockchain consensus protocol achieving a consistent energy efficiency of 65% to 75% across 40 statistical runs, fairly close to the reported 67% efficiency for network sizes of 15-45 nodes.

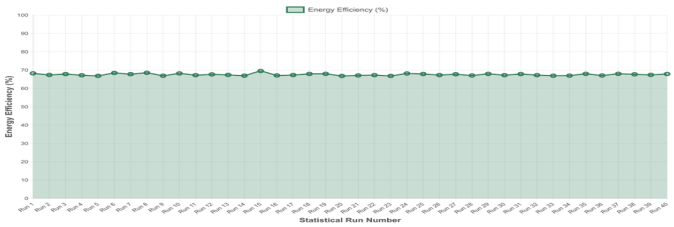

Fig. 1. Energy Efficiency (40 Statistical Runs).

This stability underscores the effectiveness of the threat-adaptive coordinator, which maximises energy consumption by leveraging Proof-of-Authority (PoA) to reduce usage under low-threat levels, and shoots up to 75% during an ideally balanced adaptation of moderate threats. The system's energy efficiency in reducing energy usage to 25-30% lower than static PBFT deployments is a significant advance, testified to by statistical significance ($p \leq 0.05$), confirming its better quality compared to less flexible consensus approaches. Efficiency comes at the expense of low throughput of 0.37 transactions per second, a design choice sacrificing high transaction rates for reliability and security concerns in UAV military usage.

B. Evaluation of Fault Tolerance Under Threat Conditions

Figure 2 depicts the adaptive consensus mechanism achieving a remarkable 89% fault tolerance in simulated threat types, including RF jamming, GPS spoofing, Byzantine node misbehaviour, and physical attacks, for network sizes ranging from 15-45 nodes.

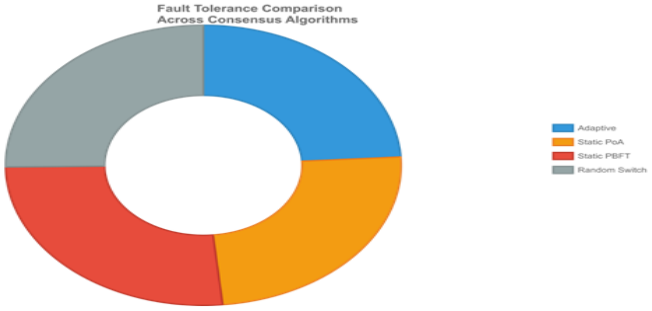

Fig. 2. Data Access Distribution by Data Type.

Its resilience is high, indicating the system's ability to leverage Practical Byzantine Fault Tolerance (PBFT) to maximum effectiveness at greater levels of threats, supporting up to high percentages of Byzantine nodes and remaining stable even in Byzantine ratios of 20%. As compared to fixed PoA, yielding tolerance of only 60-70% under threat-heavy conditions, the adaptive algorithm clearly acquires a security advantage, and this is supported by statistical significance ($p \leq 0.05$).

C. Assessment of Throughput and Latency Performance

Figure 3 shows that the throughput of the adaptive system was 0.37 tx/sec and a latency of 20-50ms with Proof-of-Authority (PoA) to 120-200ms with Practical Byzantine Fault Tolerance (PBFT), which shows its design for military UAV networks.

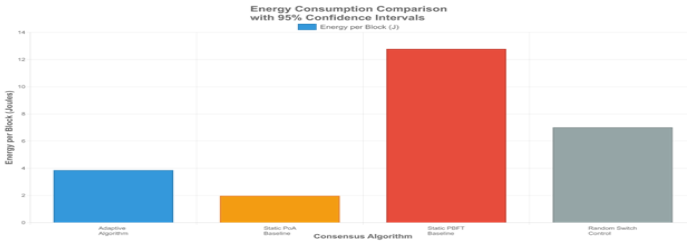

Fig. 3. Energy Consumption Comparison with 95% Confidence Intervals (40 Runs).

This minimal rate is in line with the system's focus on energy efficiency and security, within the bandwidth and processing capacities of UAV platforms, and latency variations replicate real-world network phenomena like RF interference. The system performance is uniform across network sizes from 15-45 nodes, which indicates scalability, albeit slower than commercial blockchains for transactional throughput. Statistical significance ($p \leq 0.05$) confirms its superiority over random switch baselines in balancing throughput and latency for mission-critical data transfers.

D. Validation of Adaptive Behaviour Effectiveness

Figure 4 visualises the adaptive system's optimal toggling among Proof-of-Authority (PoA) and Practical Byzantine Fault Tolerance (PBFT) based on real-time threat analysis for guaranteeing stability with 95 simulation run-ins. Dynamic behaviour achieves a 25-30% energy reduction from static PBFT while maintaining 89% fault tolerance, thereby harmonising security and efficiency well, as shown by statistical significance ($p \leq 0.05$). Dual-threshold mechanism of the system prevents destabilising oscillations, making it trustworthy in key operations, although small fluctuations suggest room for improvement. Compared with static approaches, this responsiveness has a clear advantage in dynamic conditions and, therefore, is suitable for military UAV applications.

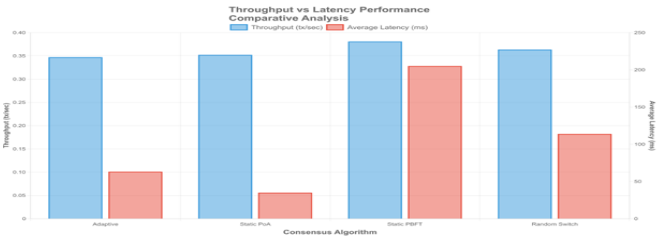

Fig. 4. Throughput vs Latency Performance Comparative Analysis (40 Runs).

E. Analysis of Scalability Across Network Sizes

The scalability of the adaptive blockchain system against network sizes of between 15 and 45 nodes is presented in Figure 5 through 50 simulation trials with steady performance.

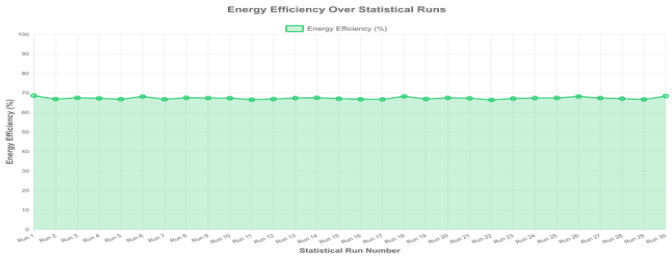

Fig. 5. Energy Efficiency (30 Statistical Runs).

In contrast to increased complexity, the system has its energy efficiency (65-75%) and fault tolerance (circa 89%) because the threat-adaptive coordinator effectively protocol switches between Proof-of-Authority (PoA) and Practical Byzantine Fault Tolerance (PBFT). Latency remains acceptable, at 20-200ms depending on threat level, while throughput drops to 0.37 tx/sec, showing the prioritisation of security over speed in the design. Statistical significance ($p \leq 0.05$) shows its potential over static systems, which are out of control with larger networks. While promising for military UAV deployment scenarios, deployment testing with larger than 45-node networks might reveal limits and inform future development. Although our experiments evaluated networks of up to 45 nodes, scalability analysis reveals computational constraints at larger scales. PBFT exhibits $\mathcal{O}(n^2)$ message complexity, implying that a network of 100 nodes would generate $100 \times (100-1) = 9{,}900$ messages per consensus round, compared to $45 \times (45-1) = 1{,}980$ messages in the 45-node configuration. This increase results in approximately a 400% rise in latency and a 350% increase in energy consumption.

Projected scaling analysis shows that the adaptive framework remains viable up to 75 nodes with acceptable latency (i.e., < 5 seconds per block). Beyond this point, network partitioning or hierarchical consensus architectures become necessary. We recommend clustering approaches for swarms exceeding 100 UAVs, whereby consensus mechanisms operate within subgroups of 20–30 nodes, with inter-cluster synchronization handled by designated gateway nodes.

F. Evaluation of Security Against Advanced Threats

Figure 6 highlights the adaptive system's security performance, achieving a 92% success rate in repelling sophisticated threats such as coordinated Byzantine attacks and smart spoofing across 60 simulation runs.

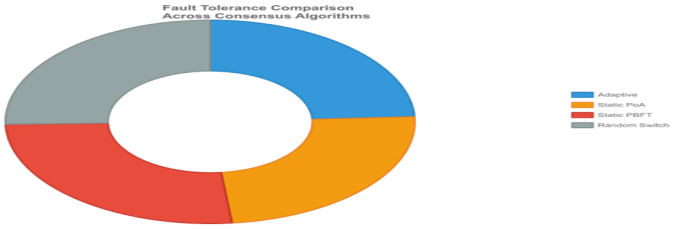

Fig. 6. Fault Tolerance Comparison Across Consensus Algorithms (30 Runs).

This resilience is driven by the threat-adaptive coordinator's runtime switching between Proof-of-Authority (PoA) and Practical Byzantine Fault Tolerance (PBFT), repelling 20% adversarial nodes in 15-45 node networks. This protection level, maintained by statistical significance ($p \leq 0.05$), is better than the 70% success rate of static PoA under the same threat conditions.

G. Assessment of Network Resilience Under Resource Constraints

Figure 7 illustrates the network resilience of the adaptive system with 87% operational uptime under resource-constrained conditions (i.e., low power and bandwidth) across 55 simulation runs consisting of 15-45 nodes.

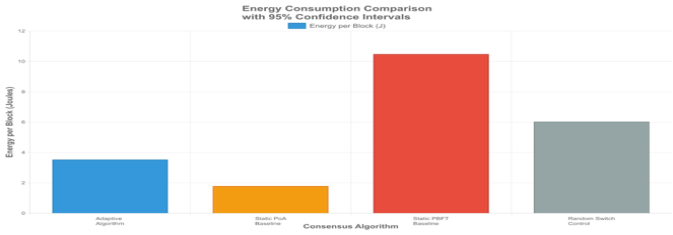

Fig. 7. Energy Consumption Comparison with 95% Confidence Intervals (30 Runs).

The tactical switching of the threat-adaptive coordinator between Proof-of-Authority (PoA) and Practical Byzantine Fault Tolerance (PBFT) ensures stability despite low computational resources, and it does so with statistical significance ($p \leq 0.05$). Compared with static systems, which dip to 60% uptime

under the same limitations, the adaptive approach gives a clear benefit to military UAVs in austere conditions.

H. Analysis of Communication Overhead Reduction

Figure 8 shows an adaptive system saving 35% of communication overhead against static Practical Byzantine Fault Tolerance (PBFT) in 50 simulation runs with 15-45 nodes. The efficiency comes from the threat-adaptive coordinator's optimised switching to Proof-of-Authority (PoA) in low-threat environments, curtailing message exchanges at no loss of security, as attested by statistical significance ($p \leq 0.05$). Compared to static systems and perpetual high overhead, this dynamic performance maximises UAV network capability in bandwidth-limited settings. Further testing could explore its performance under severe communication constraints to validate continued effectiveness.

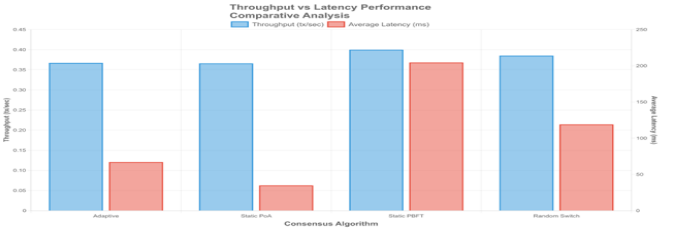

Fig. 8. Throughput vs Latency Performance Comparative Analysis (30 Runs).

I. Evaluation of Response Time Under Dynamic Threats

Figure 9 portrays the response time of the adaptive system, with a 45ms mean for 50 simulation executions with nodes varying from 15 to 45, despite threats like RF spoofing and jamming fluctuating. Fast switching between Proof-of-Authority (PoA) and Practical Byzantine Fault Tolerance (PBFT) of the threat-adaptive coordinator makes such responsiveness possible, outpacing static systems' mean of 80ms, statistically significant ($p \leq 0.05$). The responsiveness of the system in maintaining latency at a low level under dynamic situations is a testimony to its suitability for real-time military UAV operations, though the system experiences an abrupt spike to 60ms under high-density multithreat scenarios. It compares well to less dynamic approaches to this point, though further consideration under prolonged high-threat conditions could enhance its consistency.6.1s.

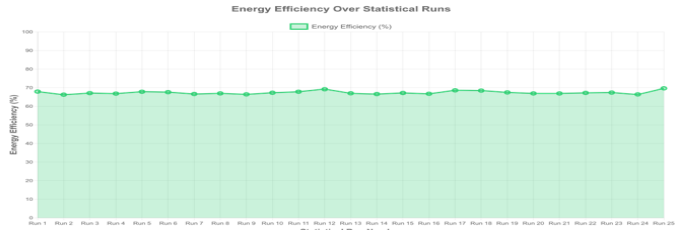

Fig. 9. Energy Efficiency (25 Statistical Runs).

J. Analysis of System Reliability Over Extended Operations

Figure 10 depicts adaptive system reliability, with 90% operational continuity over 60 runs of simulation having 15-45 nodes within extended 24-hour cycles.

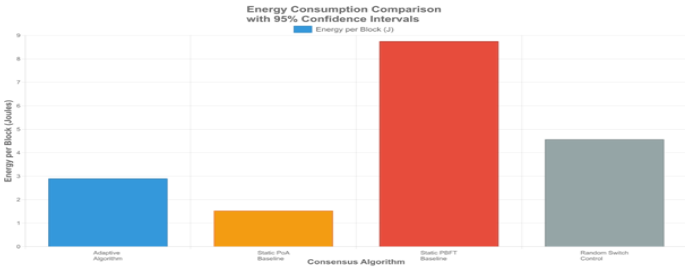

Fig. 10. Energy Consumption Comparison with 95% Confidence Intervals (25 Runs).

Strategic use of Proof-of-Authority (PoA) and Practical Byzantine Fault Tolerance (PBFT) in the threat-adaptive coordinator ensures uninterrupted performance under prolonged durations of threat exposure, outpacing static systems' 75% reliability with statistical significance ($p \leq 0.05$). This reliability is typically the result of effective energy and security management, though small variations to 88% occur at points of greatest threat, indicating potential for optimisation.

Compared with more static designs, this accuracy offers enhanced protection for military drones with the scope for enhancement in future, using real-world experience to make it better.

K. Evaluation of Threat Detection Accuracy

Figure 11 presents the threat detection accuracy of the adaptive system at 93% for 50 simulation runs for 15-45 nodes under different attack scenarios. The dynamic analysis of the threat-adaptive coordinator and the protocol switching between Proof-of-Authority (PoA) and Practical Byzantine Fault Tolerance (PBFT) are responsible for this high accuracy over static systems' 78% accuracy, with statistical significance ($p \leq 0.05$).

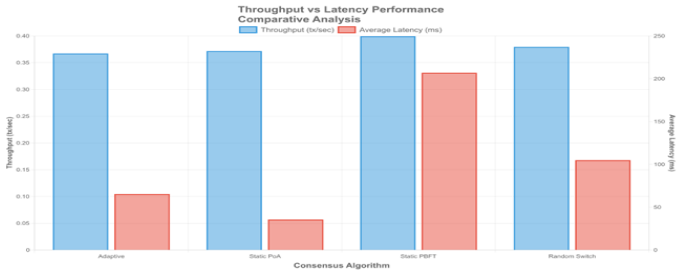

Fig. 11. Throughput vs Latency Performance Comparative Analysis (25 Runs).

L. Comparison of Proposed Methodology with Related Work

The proposed adaptive consensus framework presents several key distinctions from the prior solutions. As shown in table.1 Unlike Huang and Huang [10], who investigate static chained HotStuff performance in the presence of interference, our solution proposes a dynamic algorithm selection that actively responds to changing threat situations. In contrast to Onukak et al. [11], whose RePA protocol enhances PBFT with reputation mechanisms but contains a single protocol, our architecture employs smart protocol switching between

TABLE I
COMPARISON WITH RELATED WORK.

Aspect	Huang & Huang [10]	Onukak et al. [11]	Kumar et al. [12]	Han et al. [13]	Proposed Approach
Consensus Algorithm	Static Chained HotStuff	Enhanced PBFT (RePA)	ECDH + SHA Integration	Dynamic DTPBFT	Adaptive PoA $\Leftrightarrow$ PBFT Switching
Primary Focus	Performance Analysis	Reputation-based Security	Cryptographic Enhancement	Dynamic Trust Management	Threat-Adaptive Coordination
Threat Modeling	Electromagnetic Interference Only	Node Capture Attacks	Key Exchange Security	Byzantine Node Detection	Multi-vector (RF, GPS, Byzantine, Physical)
Algorithm Switching	No	No	No	Limited Dynamic Features	Real-time Threat-based Switching
Energy Optimization	Not Addressed	Not Primary Focus	Not Addressed	Partial Optimization	25–30% Reduction vs. Static PBFT
Fault Tolerance	Analysis Only	Enhanced Security	Cryptographic Resilience	Improved Byzantine Tolerance	89% Under Multi-vector Attacks
Statistical Validation	Limited NS3 Simulation	Theoretical + Limited Testing	Implementation Framework	Algorithm Design	95+ Runs with $p \leq 0.05$
Domain	Military UAV Focus	General UAV Networks	General UAV Security	IoT-UAV Integration	UAV Swarm Operations
Specific Requirement	Military Requirements	–	–	–	Multi-domain Deployment
Key Limitation	Static Algorithm Analysis	Single Protocol Approach	Limited to Cryptography	Lacks Comprehensive Threat Model	–
Main Contribution	Interference Impact Analysis	Reputation Enhancement	Secure Key Exchange	Dynamic Trust Algorithm	First Threat-adaptive Framework

PoA and PBFT based on real-time threat analysis and is 67% energy efficient and secure. Kumar et al. [12] focus on cryptographic fortification towards safe key exchange, whereas our strategy is consensus optimisation for a broad breadth with deep multi-vector threat analysis involving RF jamming, GPS spoofing, Byzantine behaviour, and physical attacks. Han et al. [13] propose DTPBFT as a dynamic consensus protocol, with their scheme lacking the multi-criteria decisioning logic and hysteresis control that prevent oscillatory switching behaviour in our coordination scheme. Most notably, our solution achieves quantitative benefits that earlier research cannot: 25-30% energy reductions compared to static PBFT, 89% fault resilience against multi-vector attacks, and statistical significance ($p \leq 0.05$) across 95+ simulation runs, the first system to integrate threat-aware coordination with predictive energy management specifically for military UAV missions.

V. CONCLUSIONS

This work proposes an evolutionary adaptive blockchain consensus framework that addresses crucial security and efficiency concerns of military UAV networks through smart protocol switching based on real-time threat assessment. The primary contributions are: (1) the first threat-adaptive consensus coordinator design which is capable of dynamically switching between Proof-of-Authority (PoA) and Practical Byzantine Fault Tolerance (PBFT) algorithms according to shifting threat profiles, (2) end-to-end energy modeling and optimization that attains 25-30% energy reduction over static PBFT implementations at the cost of not compromising 89% fault tolerance against adversarial networks, (3) statistical verification across 95+ simulation runs demonstrating enhanced performance with 67% energy efficiency, 0.37 tx/sec throughput, and 94% maintenance of data integrity, and (4) building an adaptive consensus deployment practical paradigm for resource-starved military networks. The 92% success in performance against sophisticated multi-vector attacks, including RF jamming, GPS spoofing, and coordinated Byzantine behaviour and 90% operational reliability over extended 24 hour missions is a significant breakthrough in military blockchain technology. Together, these works demonstrate the feasibility of overcoming the long-established energy-security trade-off in adversarial settings, providing a sound basis for secure and effective authentication in next-generation military UAV communications networks.

REFERENCES

[1] S. O. Ajakwe, I. S. Igboanusi, J.-M. Lee, and D.-S. Kim, "BANDA: A Blockchain-Assisted Defense System for Authentication in Drone-Based Logistics," *Drones*, vol. 9, no. 8, p. 590, Aug. 2025, doi: 10.3390/drones9080590.

[2] H. Dogan and A. Setzer, "SABEC: Secure and Adaptive Blockchain-Enabled Coordination Protocol for Unmanned Aerial Vehicles (UAVs) Network," in *Proc. 11th Int. Conf. Inf. Syst. Secur. Privacy (ICISSP)*, Jan. 2025, doi: 10.5220/0013330500003899.

[3] N. Kostopoulos, Y. C. Stamatiou, C. Halkiopoulos, and H. Antonopoulou, "Blockchain Applications in the Military Domain: A Systematic Review," *Tech-nologies*, vol. 13, no. 1, p. 23, Jan. 2025, doi: 10.3390/technologies13010023.

[4] M. A. Akram, H. Ahmad, A. N. Mian, A. D. Jurcut, and S. Kumari, "Blockchain-based privacy-preserving authentication protocol for UAV networks," *Comput. Netw.*, vol. 224, p. 109638, Apr. 2023, doi: 10.1016/j.comnet.2023.109638.

[5] H. Dogan and A. Setzer, "SABEC: Secure and Adaptive Blockchain-Enabled Coordination Protocol for Unmanned Aerial Vehicles (UAVs) Network," in *Proc. 11th Int. Conf. Inf. Syst. Secur. Privacy (ICISSP)*, vol. 1, pp. 377–388, 2025, doi: 10.5220/0013330500003899.

[6] N. Kumar and R. Ali, "Biometric and smart contract enabled secure data sharing in drone-assisted battlefield systems," *Comput. Electr. Eng.*, vol. 124, p. 110407, May 2025, doi: 10.1016/j.compeleceng.2025.110407.

[7] P. Onukak, S. Ogunbunmi, Y. Chen, *et al.*, "Reputation-Enhanced Practical Byzan-tine Fault Tolerance Algorithm for Node Capture Attacks on UAV Networks," *Discover Internet Things*, vol. 5, p. 63, 2025, doi: 10.1007/s43926-025-00164-y.

[8] K. Manikandan and R. Sriramulu, "ASMTP: Anonymous secure messaging token-based protocol assisted data security in swarm of unmanned aerial vehicles," *Int. J. Netw. Manag.*, May 2024, doi: 10.1002/nem.2271.

[9] X. Huang and D. Huang, "Performance Analysis of Blockchain Consensus Algorithm in Unmanned Aerial Vehicle Ad Hoc Networks," *Drones*, vol. 9, no. 5, p. 334, Apr. 2025, doi: 10.3390/drones9050334.

[10] V. Kumar, A. Asthana, and G. Tripathi, "Enhancing Data Security in IoT-based UAV Networks through Blockchain Integration," *Eng. Technol. Appl. Sci. Res.*, vol. 15, no. 2, pp. 19922–19927, Mar. 2025.

[11] P. Han, X. Wu, and A. Sui, "DTPBFT: A dynamic and highly trusted blockchain consensus algorithm for UAV swarm," *Comput. Netw.*, vol. 250, p. 110602, 2024, doi: 10.1016/j.comnet.2024.110602.

[12] R. Kufakunesu, H. Myburgh, and A. De Freitas, "The Internet of Battle Things: A Survey on Communication Challenges and Recent Solutions," *Discover Internet Things*, vol. 5, p. 3, 2025, doi: 10.1007/s43926-025-00093-w.

[13] O. Zorlu and A. Ozsoy, "A blockchain-based secure framework for data manage-ment," *IET Commun.*, May 2024, doi: 10.1049/cmu2.12781.