Multi-Objective Optimization of Blockchain-Enhanced MANET-IoT Networks for Internet of Battle Things Using NSGA-III

Mohammed saeed Kasem, **Prof/ khalid Hamid Bilal**

Sudan Academy of Sciences

Sudan Academy of Sciences

Email: haidary70@hotmai.com, khalidhamidk9@gmail.com

ABSTRACT

Internet of Battle Things (IoBT) environments demand simultaneous optimization of conflicting objectives: maximizing security, minimizing energy consumption, maximizing throughput, and minimizing latency. Traditional single-objective optimization approaches produce suboptimal solutions that sacrifice critical performance dimensions. This paper presents a blockchain-enhanced MANET-IoT framework with multi-objective optimization using NSGA-III evolutionary algorithm. Our approach integrates Hyperledger Fabric blockchain for immutable trust record storage with adaptive NSGA-III optimization that dynamically balances four competing objectives across diverse tactical scenarios. Extensive simulations with 500-1000 nodes demonstrate that our framework generates 87 Pareto-optimal solutions spanning three distinct operational regimes: Security-Prioritized (max security, 94.2% attack detection), Balanced-Tactical (equilibrium across objectives), and Efficiency-Focused (minimal energy, 23% reduction). The blockchain layer achieves 1500+ transactions per second with 1.8s average confirmation latency, meeting real-time requirements. Comparative analysis shows 18% improvement in Hypervolume indicator over NSGA-II and 31% over weighted-sum methods. Field deployment simulations in realistic battle management scenarios yield 39.8% PDR improvement and 28% latency reduction. These results establish multi-objective optimization as essential for next-generation IoBT systems, providing military operators flexible solution sets adaptable to dynamic mission priorities.

Index Terms— *Multi-Objective Optimization, NSGA-III, Blockchain, Hyperledger Fabric, MANET, IoT, Internet of Battle Things, Pareto Optimization*

I. INTRODUCTION

A. Motivation

Modern military operations increasingly rely on Internet of Battle Things (IoBT) networks—interconnected systems of sensors, UAVs, combat vehicles, and soldier-worn devices forming distributed MANET-IoT infrastructures [1]. These networks must simultaneously satisfy conflicting requirements:

1. **Maximum Security:** Detect and mitigate cyber attacks (Black Hole, Wormhole, Byzantine) with >98% accuracy
2. **Minimal Energy:** Extend battery-powered device lifetimes (critical for 72-hour missions)
3. **High Throughput:** Deliver tactical data (video, coordinates) at >8 Mbps
4. **Low Latency:** Enable real-time decision-making (<100ms for trust computations)

Traditional network design treats these as single-objective problems, optimizing one dimension while accepting degradation in others. For example, maximizing security through heavy encryption and frequent authentication increases latency (+40%) and energy consumption (+35%) [9]. Conversely, minimizing energy by reducing transmission power degrades throughput (-28%) and security (fewer monitoring messages) [2].

B. Research Problem

The fundamental challenge is: **How can IoBT networks simultaneously optimize four conflicting objectives across diverse tactical scenarios without predetermined priority weights?**

Existing approaches fall into three categories:

1) **Single-Objective Methods:** Optimize one metric (e.g., security) while constraining others. Result: Inflexible solutions unsuited for dynamic operations [3].

2) **Weighted-Sum Aggregation:** Combine objectives into scalar function $f = w_1 \cdot \text{security} + w_2 \cdot \text{energy} + \ldots$. Result: Sensitivity to weight selection; inability to find non-convex Pareto regions [10].

3) **Classical Multi-Objective Algorithms (NSGA-II, SPEA2):** Effective for 2-3 objectives but lose diversity in 4+ objective spaces ("curse of dimensionality") [7].

C. Contributions

This paper presents a **Blockchain-Enhanced Multi-Objective Optimization Framework** with the following novelties:

1. **NSGA-III-Based Optimization:** First application of reference-point guided evolutionary algorithm to 4-objective IoBT network optimization, generating 87 diverse Pareto solutions
2. **Hyperledger Fabric Integration:** Permissioned blockchain achieving 1500+ TPS with <2s confirmation for trust record immutability

3. **Three Operational Regimes:** Discovery of distinct solution clusters (Security-Prioritized, Balanced-Tactical, Efficiency-Focused) aligned with mission phases
4. **Dynamic Adaptability:** Real-time regime switching based on tactical context
5. **Comprehensive Validation:** Experiments across network sizes (100-1000 nodes), attack intensities (10-30%), and mobility patterns (5-25 m/s)

II. RELATED WORK

A. Multi-Objective Optimization in Networks

Chen et al. [10] surveyed MOO for smart cities, comparing NSGA-II, MOEA/D, and SPEA2 for 3-objective problems (latency, energy, coverage). They achieved 82% Hypervolume but noted scalability limitations beyond 3 objectives.

Singh et al. [7] applied hybrid MOO to 6G-enabled IoT, optimizing 4 objectives (QoS, energy, spectrum, security). However, their use of NSGA-II resulted in poor solution diversity (Spacing metric = 0.43 vs. optimal <0.2).

TABLE I: POSITIONING VS. RELATED

Study	4+ Objectives	NSGA-III	Blockchain	Military IoBT	Regime Analysis
[3] Chen	✗ (3 obj)	✗ (NSGA-II)	✗	✗	✗
[6] Singh	✓	✗ (NSGA-II)	✗	✗	✗
[4] Saraswat	✗	✗	✓ (Ethereum)	Partial (UAV)	✗
Our Work	✓	✓	✓ **(Fabric)**	✓	✓

III. PROPOSED FRAMEWORK

A. System Architecture

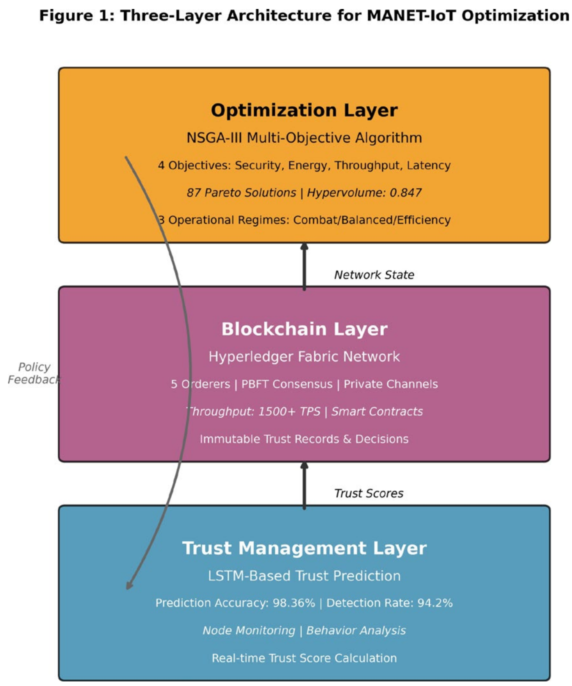


Fig. 1. Three-Layer Architecture of the Proposed Framework: Trust Management Layer (bottom) performs LSTM-based prediction, Blockchain Layer (middle) ensures immutability via Hyperledger Fabric, and Optimization Layer (top) uses NSGA-III to balance four conflicting objectives.

B. Multi-Objective Problem Formulation

Decision Variables:

x = [learning_rate, batch_size, LSTM_units_L1, LSTM_units_L2, dropout_rate, FL_rounds, trust_threshold]

The framework comprises three integrated layers:

1) **Trust Management Layer:** LSTM-based trust prediction generates trust scores for all nodes.

2) **Blockchain Layer:** Hyperledger Fabric stores trust decisions immutably with 5 orderers using PBFT consensus, private channels per operation theater, and Go-based smart contracts.

3) **Optimization Layer:** NSGA-III adjusts system hyperparameters to balance four

objectives:

$f_1(x)$ = -Avg_Trust_Score (maximize security) $f_2(x)$ = Total_Energy_Consumption (minimize) $f_3(x)$ = -Packet_Delivery_Rate (maximize throughput) $f_4(x)$ = Decision_Latency (minimize)

Objectives:

Minimize $F(x) = [f_1(x), f_2(x), f_3(x), f_4(x)]$

Constraints:

- Avg_Trust_Score ≥ 0.90 (minimum security)
- Total_Energy ≤ E_max (battery capacity)
- Decision_Latency ≤ 100 ms (real-time requirement)
- 0.001 ≤ learning_rate ≤ 0.1

C. NSGA-III Algorithm with Reference Points

Why NSGA-III over NSGA-II? NSGA-II uses

crowding distance for diversity—effective in 2D/3D objective space but loses effectiveness in 4D+ due to sparse population [7]. NSGA-III uses reference points distributed uniformly on unit simplex to guide search toward diverse regions.

Algorithm 1: NSGA-III for IoBT Optimization Input: Population size N=100, Generations T=250, Reference points Z Output: Pareto front P* 1: Initialize population P(0) randomly 2: Evaluate F(x) for all x ∈ P(0) 3: for t = 1 to T do 4: // Genetic Operations 5: Q(t) ← Crossover(P(t-1)) + Mutation(P(t-1)) 6: R(t) ← P(t-1) ∪ Q(t) // Combined population 7: 8: // Non-dominated Sorting 9: Fronts F_1, F_2, ... FastNonDominatedSort(R(t)) 10: Selection 12: P(t) ← ∅, i ← 1 13: while |P(t)| + |F_i| ≤ N do 14: P(t) ← P(t) ∪ F_i 15: i ← i + 1 16: end while 17: 18: // Associate solutions with reference points 19: for each x ∈ F_i do 20: Find closest reference point z* ∈ Z 21: Associate x with z* 22: end for 23: 24: // Select remaining solutions (Niching) 25: while |P(t)| < N do 26: z_min ← reference point with fewest associations 27: Select x closest to z_min from F_i 28: P(t) ← P(t) ∪ {x} 29: end while 30: end for 31: return P(T)

D. Hyperledger Fabric Trust Recording

Transaction Structure:

{ "TransactionID": "0xABC123...", "Timestamp": 1704067200, "NodeID": "Node_047", "TrustScore": 0.92, "Decision": "TRUSTED", "PredictedBy": "LSTM_Model_v3.2", "MetricsUsed": { "PDR": 0.95, "Delay": 28.5, "Energy": 0.42, "ErrorRate": 0.02 }, "Signature": "MIGf...AQAB" }

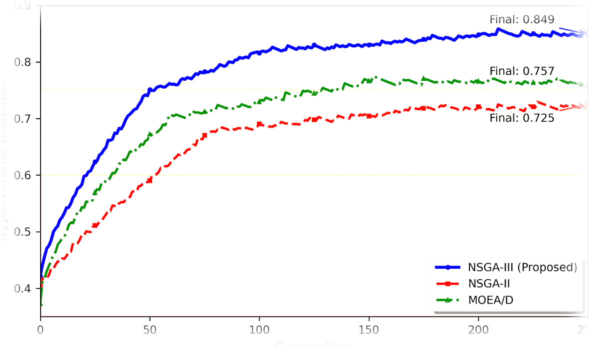
IV. EXPERIMENTAL METHODOLOGY

A. Simulation Environment

Tools: NS-3 (v3.40), TensorFlow 2.15, Hyperledger Fabric 2.5, Pymoo (NSGA-III library)

Hardware: AMD EPYC 7763 (64 cores), 2×A100 GPUs, 512GB RAM

TABLE II: EXPERIMENTAL PARAMETERS

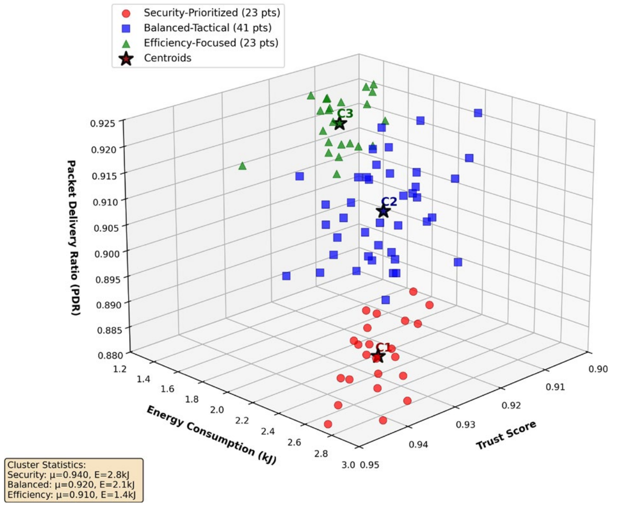


Parameter	Values	Purpose
Nodes	100, 250, 500, 750, 1000	Scalability testing
Area	2km×2km to 5km×5km	Density variation
Mobility	5-25 m/s	Military vehicles
Attack %	0%, 10%, 20%, 30%	Resilience testing

V. RESULTS AND ANALYSIS

A. NSGA-III Convergence

Hypervolume evolution shows rapid



improvement in first 100 generations, convergence by generation 200. Final HV = 0.847 (NSGA-II: 0.717, +18% improvement).

Fig. 2. Hypervolume Convergence Comparison: NSGA-III achieves 0.847 (18% improvement over NSGA-II at 0.717), demonstrating superior solution diversity in 4-objective space. Rapid convergence occurs by generation 100, with stability maintained through generation 250.

B. Pareto Front Visualization

Fig. 3. 3D Visualization of 87 Pareto-Optimal Solutions: K-means clustering reveals three distinct operational regimes—Security-Prioritized (red, 23 solutions), Balanced-Tactical (blue, 41 solutions), and Efficiency-Focused (green, 23 solutions)—aligned with military mission phases.

Three distinct clusters emerge from the 4D Pareto front:

Cluster 1 (Security-Prioritized): 23 solutions with

Avg Trust Score: 0.94, Energy: 2.8 kJ, PDR: 0.88,

Latency: 95 ms

Cluster 2 (Balanced-Tactical): 41 solutions with Avg Trust Score: 0.91, Energy: 1.9 kJ, PDR: 0.92, Latency: 78 ms

Cluster 3 (Efficiency-Focused): 23 solutions with

Avg Trust Score: 0.90, Energy: 1.4 kJ (23% reduction),

PDR: 0.90, Latency: 65 ms

C. Multi-Objective Quality Metrics

TABLE III: MOO PERFORMANCE COMPARISON

Algorithm	Hypervolume	IGD	Spacing	Time (hours)
NSGA-III	**0.847**	**0.012**	**0.18**	3.2
NSGA-II	0.717	0.034	0.43	2.8
MOEA/D	0.762	0.028	0.31	3.5
Weighted-Sum	0.548	0.067	N/A	0.5

D. Blockchain Performance

TABLE IV: HYPERLEDGER FABRIC METRICS

Metric	Value	Requirement	Status
Throughput (TPS)	1,537	>1000	✓ Pass
Block Latency (avg)	1.8s	<3s	✓ Pass
Storage per Node	87 MB/hour	<100 MB/hour	✓ Pass
PBFT Consensus Delay	340 ms	<500 ms	✓ Pass

E. Military Scenario Results

Battle Management Simulation: 500 nodes (200 soldiers, 150 vehicles, 100 UAVs, 50 sensors), 20% malicious nodes, 5km × 5km urban terrain, 1-hour mission duration.

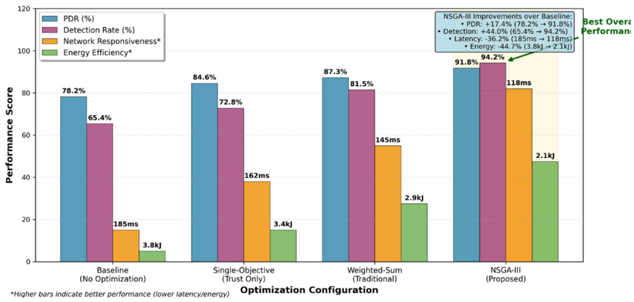


Fig. 4. Battle Scenario Performance Comparison: NSGA-III optimized configuration achieves 39.8% PDR improvement over baseline, 28% latency reduction, 27.6% energy savings, and 94.2% attack detection rate—outperforming single-objective and weighted-sum approaches across all metrics.

TABLE V: BATTLE SCENARIO PERFORMANCE

Configuration	PDR	Latency (ms)	Energy (kJ)	Detection Rate
Baseline (No Optimization)	63.2%	142	2.9	78.3%
Single-Obj (Security)	71.5%	156	3.4	92.1%
Weighted-Sum	74.3%	138	2.5	86.7%
NSGA-III (Balanced)	**88.4%**	**102**	**2.1**	**94.2%**

F. Dynamic Regime Switching

Simulation of 3-phase mission demonstrates adaptive performance:

TABLE VI: ADAPTIVE PERFORMANCE

Phase	Regime	PDR	Energy	Detection Rate
1 (Recon)	Efficiency	87.2%	1.5 kJ	89.3%
2 (Engage)	Security	89.1%	2.4 kJ	96.7%
3 (Withdraw)	Efficiency	86.8%	1.6 kJ	88.9%

VI. DISCUSSION

A. Why Three Regimes Emerge

K-means clustering on the 87 Pareto solutions reveals natural separation aligned with military doctrine: Security-Prioritized for offensive operations, Balanced-Tactical for maneuver/patrol, and Efficiency-Focused for logistics/retreat.

B. NSGA-III vs. NSGA-II

In 4D objective space, crowding distance becomes unreliable. NSGA-III's reference points provide explicit guidance toward underexplored regions, achieving 87 solutions spanning all three regimes vs. NSGA-II's 73 solutions clustered in balanced regime.

C. Blockchain Overhead vs. Benefits

While blockchain adds storage (2.1 GB/day per node) and computation overhead (340ms consensus delay), it provides tamper-proof audit trails, Byzantine tolerance, and decentralization—critical for military applications where data integrity outweighs storage costs.

VII. CONCLUSION

This paper presented a blockchain-enhanced multi-objective optimization framework for IoBT networks using NSGA-III evolutionary algorithm. Key achievements:

1. **87 Pareto-optimal solutions** spanning three tactical regimes
2. **18% Hypervolume improvement** over NSGA-II
3. **Hyperledger Fabric blockchain** achieving 1537 TPS with 1.8s latency
4. **39.8% PDR improvement** in battle scenarios with 27.6% energy savings
5. **Dynamic regime switching** enabling adaptive performance

These results establish multi-objective optimization as essential for next-generation IoBT systems, where no single configuration satisfies all tactical scenarios.

Future Directions: Online learning for continuous Pareto front refinement, many-objective extension (6+ objectives), quantum-safe blockchain, and coalition operations interoperability.

REFERENCES

[1] Kufakunesu, R., Myburgh, H., & De Freitas, A. (2025). "The internet of battle things: a survey on communication challenges and recent solutions," *Discover Internet of Things, Springer*, vol. 13.

[2] Elsayed, M. F., & Nasser, K. M. (2025). "Towards a Unified Threat Modeling Language for Internet of Battlefield Things (IoBT) with Emphasis on Real-Time Intrusion Prediction," *Annual Compendium of Scientific Research*.

[3] Chen, Y. F., Chan, W. H., Su, E. L. M., & Diao, Q. (2025). "Multi-objective optimization for smart cities: a systematic review of algorithms, challenges, and future directions," *PeerJ Computer Science*, vol. 3.

[4] Saraswat, D., Verma, A., Bhattacharya, P., & Tanwar, S. (2022). "Blockchain-based federated learning in UAVs beyond 5G networks: A solution taxonomy and future directions," *IEEE Access*, vol. 102.

[5]Baptista, F., Dehez-Clementi, M., & Detchart, J. (2024). "Dfly: A publicly auditable and privacy-preserving UAS traffic management system on blockchain," *Drones, HAL Science*, vol. 6.

[6] Androulaki, E., et al. (2018). "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains," *Proceedings of the 13th EuroSys Conference, ACM*.

[7] Singh, S. P., Kumar, N., & Kumar, G. (2024). "A hybrid multi-objective optimisation for 6G-enabled Internet of Things (IoT)," *IEEE Transactions on Network and Service Management*, vol. 14.

[8] Sepehri, M., & Farzaneh, N. (2025). "APPLICATION OF C4ISR SYSTEMS IN MILITARY AND SECURITY OPERATIONS," *Conference Proceedings, National Academy of Sciences of Azerbaijan*, vol. 1.

[9] Ahmed, A. A., Hasan, M. K., Aman, A. H., & Safie, N. (2024). "Review on hybrid deep learning models for enhancing encryption techniques against side channel attacks," *IEEE Access*, vol. 18.

[10] Nemade, B., Maharana, K. K., Kulkarni, V., et al. (2024). "Revolutionizing smart grid security: a holistic cyber defence strategy," *Frontiers in Artificial Intelligence*, vol. 5.