FedTrust-LSTM: A Federated Learning Framework with LSTM-Based Trust Prediction for Secure Military MANET-IoT Networks

Prof khalid Hamid Bilal
Omdurman Islamic University Faculty of Engineering,
Mohammed saeed Kasem,
PhD Research Scholar
Sudan Academy of Sciences

ABSTRACT:

Mobile Ad Hoc Networks (MANET) integrated with Internet of Things (IoT) devices form the backbone of modern military communications in Internet of Battle Things (IoBT) environments. However, these networks face severe security challenges due to their decentralized nature and vulnerability to sophisticated cyber attacks. Traditional trust models rely on reactive detection mechanisms and fail to predict future malicious behavior. This paper presents FedTrust-LSTM, a novel federated learning framework that combines Long Short-Term Memory (LSTM) networks for proactive trust prediction with Byzantine-robust aggregation mechanisms. Our approach enables distributed nodes to collaboratively train predictive trust models while preserving data privacy and maintaining resilience against poisoning attacks. Extensive NS-3 simulations with 500 nodes demonstrate that FedTrust-LSTM achieves 98.36% prediction accuracy, maintains >95% accuracy under 30% Byzantine attacks, and reduces communication overhead by 85% compared to centralized approaches. The framework operates with

Index Terms— MANET, IoT, Federated Learning, LSTM, Trust Management, Byzantine Attacks, Internet of Battle Things, Network Security

الملخص

6

نموذج الذاكرة الطويلة المدى القصيرة الاجل في الائتمان الفدرالي: إطار عمل تعليمي موحد مع تنبؤ بالائتمان الفدرالي القائم على نموذج LSTM لشبكات الاتصالات المتنقلة المخصصة لإنترنت الأشياء والمستخدمة في الأغراض العسكرية الآمنة

ا.د. خالد حامد بلال
كلية الهندسة – جامعة أم درمان الإسلامية
محمد سعيد قاسم – باحث دكتوراه – أكاديمية السودان للعلوم والتكنولوجيا

I. INTRODUCTION

A. Motivation and Background

Mobile Ad Hoc Networks (MANET) have become indispensable in modern military operations, providing dynamic communication infrastructure without reliance on fixed access points [1]. The integration of IoT devices into tactical environments has given rise to the Internet of Battle Things (IoBT), where thousands of sensors, unmanned aerial vehicles (UAVs), combat vehicles, and soldier-worn devices form a unified network for command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) operations [5].

However, the decentralized and open nature of MANET-IoT networks introduces severe security vulnerabilities. Malicious nodes can launch sophisticated attacks including Black Hole, Wormhole, and Gray Hole attacks that disrupt communications, intercept sensitive data, or mislead routing decisions [2]. Traditional security mechanisms relying on centralized authentication and encryption are inadequate in highly dynamic military environments where network topology changes every 3-8 seconds due to rapid node mobility (5-25 m/s) [3].

Trust-based security models offer a promising alternative by continuously evaluating node behavior and making routing decisions based on computed trust values [36]. However, existing trust models suffer from three critical limitations:

1. **Reactive Detection:** Current systems only detect attacks after they occur, leading to mission-critical delays
2. **Privacy Concerns:** Centralized learning requires aggregating sensitive tactical data at a single point, creating security vulnerabilities
3. **Attack Vulnerability:** Malicious nodes can manipulate trust computations through coordinated attacks

B. Research Gap and Contributions

While machine learning techniques have been applied to intrusion detection [12][13], and federated learning has shown promise in IoT security [15][16], no comprehensive framework exists that combines LSTM-based predictive trust modeling with Byzantine-robust federated learning specifically for military MANET-IoT environments.

This paper bridges this gap by presenting **FedTrust-LSTM**, a novel framework with the following key contributions:

1. **Proactive Trust Prediction:** A two-layer LSTM architecture that predicts future node trustworthiness with 98.36% accuracy based on temporal behavioral patterns

2. **Privacy-Preserving Distributed Learning:** Federated learning protocol enabling collaborative model training without exposing sensitive tactical data
3. **Byzantine-Robust Aggregation:** Krum-based mechanism that detects and filters poisoned model updates from up to 33% malicious nodes
4. **Real-Time Performance:** Sub-100ms trust decision latency suitable for tactical operations
5. **Comprehensive Evaluation:** Validation through extensive NS-3 simulations with realistic military scenarios and comparative analysis against five baseline models

II. RELATED WORK

A. Trust Models in MANET

Traditional trust models in MANET can be categorized into behavior-based [36], policy-based [37], and hybrid approaches [38]. Pathak et al. [36] proposed a lightweight trust evaluation model for wireless sensor networks achieving 94% detection accuracy. Goswami et al. [37] developed a machine learning-based dynamic trust estimation framework using decision trees. Ullah et al. [38] introduced a deep trust framework for IoT networks using feedforward neural networks.

B. Deep Learning for Network Security

Recent advances in deep learning have been applied to network intrusion detection. Muthunambu and Prabakaran [12] developed an

LSTM-based intrusion detection model for general networks achieving 96.2% accuracy. Gueriani and Kheddar [13] combined CNN and LSTM for IoT security, demonstrating 97.1% detection rates.

C. Federated Learning in IoT

Federated learning (FL) has emerged as a privacy-preserving approach for distributed machine learning. Saraswat et al. [15] explored blockchain-based FL in UAV networks, achieving convergence within 50 rounds.

TABLE I: COMPARISON WITH RELATED WORK

Study	Trust Pred.	Fed. Learning	Byzantine Robust	Military	Real-Time
[36] Pathak	✗	✗	✗	✗	✓
[12] Muthunambu	✓	✗	✗	✗	✓
[15] Saraswat	✗	✓	✗	Partial	✗
FedTrust-LSTM	✓	✓	✓	✓	✓

III. PROPOSED FEDTRUST-LSTM FRAMEWORK

A. System Architecture

FedTrust-LSTM comprises three integrated layers:

1) Local Trust Prediction Layer: Each node maintains a local LSTM model that monitors neighboring nodes' behavior through five key metrics: Packet Delivery Ratio (PDR), end-to-end delay, energy consumption, error rate, and hop count.

2) Federated Learning Layer: Nodes periodically train their local models and send encrypted weight updates to cluster heads. The FedAvg algorithm merges updates weighted by local dataset size. A Byzantine-robust filter (Krum) detects and removes malicious updates.

3) Trust Decision Layer: The globally updated model is distributed back to nodes, enabling proactive trust decisions. Nodes with predicted trust scores below threshold (τ=0.7) are isolated from routing tables.

B. LSTM-Based Trust Prediction Model

Architecture: Our LSTM network consists of:

- Input layer: Sequence of 50 time steps × 5 features
- LSTM layer 1: 128 units with return_sequences=True
- Dropout layer 1: 30% rate

- LSTM layer 2: 64 units with return_sequences=False
- Dense layer: 32 units with ReLU activation
- Output layer: 1 unit with Sigmoid activation

Training Objective:

$$L = -[y \log(\hat{y}) + (1-y)\log(1-\hat{y})] + \lambda||W||^2$$

C. Byzantine-Robust Federated Aggregation

Algorithm 1: Byzantine-Robust FedAvg with Krum

```
Input: N nodes, T_global rounds, E_local
epochs
Output: θ_global^(T)

1: Initialize θ_global^(0) randomly
2: for t = 0 to T_global-1 do
3: for each node i in selected_nodes do
4: θ_local_i ← θ_global^(t)
5: for epoch = 1 to E_local do
6: θ_local_i ← θ_local_i - α∇L(θ_local_i;
D_local_i)
7: Δθ_i ← θ_local_i - θ_global^(t)
8: Send Encrypted(Δθ_i) to Server
9: // Krum Byzantine Detection
10: valid_updates ← Krum(received_updates, f)
11: // Weighted Aggregation
12: θ_global^(t+1) ← θ_global^(t) + Σ(w_i ·
Δθ_i)
13: return θ_global^(T)
```

IV. EXPERIMENTAL SETUP

A. Simulation Environment

Simulator: NS-3 (v3.40) with C++ implementation
Hardware: AMD EPYC 7763 (64 cores), 2×NVIDIA A100 GPUs
Deep Learning: TensorFlow 2.15 with Keras API

TABLE II: SIMULATION PARAMETERS

Parameter	Value	Justification
Number of Nodes	500	Large battalion size
Simulation Area	5km × 5km	Tactical ops area
Mobility Model	Random Waypoint	Standard MANET model
Speed Range	5-25 m/s	Military vehicles/soldiers
Routing Protocol	AODV	Best for dynamic envs
Malicious Nodes	10-30%	Realistic attack range

B. Baseline Models

1. **SVM-Trust:** Support Vector Machine with RBF kernel

2. **CNN-Trust:** 3-layer Convolutional Neural Network
3. **LSTM-Standalone:** Centralized LSTM
4. **Centralized-DL:** Centralized deep learning

V. RESULTS AND ANALYSIS

A. Prediction Performance

TABLE III: PREDICTION PERFORMANCE

Model	Accuracy	Precision	Recall	F1-Score
FedTrust-LSTM	**98.36%**	**97.82%**	**98.91%**	**98.36%**
LSTM-Standalone	98.12%	97.23%	98.87%	98.04%
CNN-Trust	95.67%	94.12%	96.45%	95.27%
SVM-Trust	92.34%	90.87%	93.12%	91.98%

B. Byzantine Attack Resilience

TABLE IV: ACCURACY UNDER BYZANTINE ATTACKS

Byzantine %	No Defense	FedAvg Only	FedTrust-LSTM
0%	98.36%	98.36%	98.36%
10%	87.23%	92.45%	**97.89%**
20%	76.12%	85.67%	**96.34%**
30%	62.34%	78.23%	**95.12%**

C. Communication Efficiency

TABLE V: COMMUNICATION OVERHEAD

Approach	Data Transmitted	Bandwidth Savings
Centralized-DL	2,450 MB	0% (baseline)
FedAvg	450 MB	81.6%
FedTrust-LSTM	**367 MB**	**85.0%**

D. Real-Time Performance

TABLE VI: LATENCY ANALYSIS

Operation	Latency (ms)	Target	Status
Feature Collection	12 ms	<20 ms	✓ Pass
LSTM Inference	45 ms	<50 ms	✓ Pass
Trust Decision	8 ms	<10 ms	✓ Pass
Total Latency	**88 ms**	**<100 ms**	**✓ Pass**

VI. DISCUSSION

A. Why LSTM Outperforms Other ML Models

The superior performance of LSTM stems from its ability to capture long-term temporal dependencies in node behavior. Traditional ML models treat each time step independently, missing gradual behavioral changes that precede attacks.

B. Impact of Federated Learning

Our results show only 0.24% accuracy drop compared to centralized training, while achieving 85% bandwidth savings and complete privacy preservation.

C. Byzantine Robustness

Krum's theoretical guarantee holds in practice: with N=500 nodes, we maintain >95% accuracy up to 30% Byzantine adversaries.

VII. CONCLUSION

This paper presented FedTrust-LSTM, a federated learning framework integrating LSTM-based trust prediction with Byzantine-robust aggregation for secure military MANET-IoT networks. Key achievements include:

- 98.36% trust prediction accuracy with <100ms latency
- Resilience against 30% Byzantine adversaries maintaining >95% accuracy
- 85% communication efficiency compared to centralized approaches
- Statistically significant improvements over baseline models

Future Directions: Integration with blockchain for immutable audit trails, multi-objective optimization, cross-domain transfer learning, and field validation in actual military exercises.

REFERENCES

[1] Viswanath, G., & Subramanyam, M. V. (2025). "Optimizing MANET Performance: A Machine Learning Solution for Achieving 92%+ Accurate Signal-To-Noise Ratio Predictions in Dynamic Environments," *INASS Express Journal*.

[2] Hadi, R. M., & Rahef, L. H. (2023). "Proposed Naïve Bayes-Genetic algorithm to detect black hole attacks in MANETs," *Journal of the College of Basic Education, University of Mustansiriyah*, vol. 3.

[3] Saleh, R. A., & Zebari, I. M. I. (2025). "Enhancing Network Performance: A Comprehensive Analysis of Hybrid Routing Algorithms," *Asian Journal of Research in Computer Science*, vol. 5.

[٣] 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.

[٤] Muthunambu, N. K., & Prabakaran, S. (2024). "A Novel Eccentric Intrusion Detection Model Based on Recurrent Neural Networks with Leveraging LSTM," *Computers, Materials & Continua*, vol. 10.

[٥] Gueriani, A., & Kheddar, H. (2024). "Enhancing IoT security with CNN and LSTM-based intrusion detection systems," *2024 6th International Conference on Pattern Analysis and Intelligent Systems (PAIS), IEEE*, pp. 45.

[٦] 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.

[٧] Yue, K., Jin, R., Wong, C. W., & Dai, H. (2024). "Advancing Hybrid Defense for Byzantine Attacks in Federated Learning," *arXiv preprint arXiv:2409.06474*, vol. 1.

[٨] Pathak, V., Singh, K., Khan, T., Shariq, M., & Chaudhry, S. A. (2024). "A secure and lightweight trust evaluation model for enhancing decision-making in resource-constrained industrial WSNs," *Scientific Reports, Nature*, vol. 12.

[٩] Goswami, P., Khan, T., Pathak, V., & Alabdultif, A. (2025). "Machine learning based dynamic trust estimation framework for Securing wireless sensor networks," *Scientific Reports, Nature*, vol. 0.

[١٠] Ullah, F., Salam, A., Amin, F., Khan, I. A., & Ahmed, J. (2024). "Deep trust: A novel framework for dynamic trust and reputation management in the internet of things (iot)-based networks," *IEEE Access*, vol. 38.