Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 28 (2025), No. 5-B, pp. 2151–2161
DOI : 10.47974/JDMSC-2431

Federated learning and deep learning-driven adaptive cryptography for context-aware elliptic curve Diffie-Hellman optimization and anomaly-aware key management in next-generation wireless networks

Sheela S. *
School of Computer Science and Engineering
RV University
Bangalore 560059
Karnataka
India

Jyothi S.†
Department of Computer Science and Engineering
Global Academy of Technology
Bangalore 560098
Karnataka
India

Shalini S. §
Department of Computer Science and Engineering
Dayananda Sagar Academy of Technology and Management
Bangalore 560082
Karnataka
India

Latha Anuj ‡
Department of Information science and Engineering
Dayananda Sagar College of Engineering
Visvesvaraya Technological University
Bangalore 560111
Karnataka
India

* *E-mail:* sheela.samarth18@gmail.com (Corresponding Author)
† *E-mail:* jyothi.s@gat.ac.in
§ *E-mail:* shalini.siddamallappa@gmail.com
‡ *E-mail:* aplatha123@gmail.com

Abstract

This study addresses critical security challenges in wireless networks, such as impersonation, spoofing, data leakage, and trust issues, by adopting a hybrid approach that integrates deep learning, federated learning, and adaptive security solutions. Key innovations include Federated Learning-Based Trust Evaluation (FL-TE), Reinforced Physical Layer Authentication (RPLA), Adaptive Artificial Noise (AAN) Strategy, Context-Aware Elliptic Curve Diffie-Hellman Optimization, and an Anomaly-Aware Hybrid Key Management System. These developments ensure decentralized, real-time, and robust security, while protecting users effectively. Simulation results demonstrate that the proposed model meets all essential performance criteria. Notably, Isostated Authentication achieves 96.8% accuracy, accelerates trust convergence to just 8 rounds (compared to 15 rounds in existing methods), improves secrecy by 22%, reduces key refresh time by 35%, and handles complex attacks using only 7% of the usual resources. These findings highlight the strong security capabilities of the framework in managing multiple wireless networks efficiently.

Subject Classification: *Primary 68T07, Secondary 94A60, 94C10, 68P30.*

Keywords: *Adaptive cryptography, Anomaly detection, Deep learning, Edge security, Federated learning, Physical layer authentication, Trust evaluation, Wireless networks.*

1. Introduction

Because of swift developments in wireless tech, 6G and the Internet of Things (IoT) are now used more widely. The connections are established quickly and large transfers are easy. There are many serious security issues that today's security practices fall short in managing [1].

Cyber-attacks have become more difficult to deal with. With 5G, things like spoofing, impersonation, data injection and eavesdropping become easier to perform and harder to spot in mobile ad hoc networks and smart edge networks [2]. Common forms of cryptography cannot be used well in this situation since they need a lot of resources and struggle to block attacks from within the organization [3].

New research is being done to find new solutions. Using the features of wireless channels, encryption and authentication are both possible as part of the physical layer [4]. AI systems help look for dangers and act on them quickly because of DL and ML [5]; FL allows for privacy by enabling AI to be learned on many devices in a network [6]. These methods do each have their own boundaries. One example is that physical techniques are challenged by noisy or shifting environments, some trust-related models can be fooled and rapid alterations in the network may be beyond the abilities of cryptography [7-9].

As a solution, a hybrid, intelligent security system should be designed for future wireless networks. It uses deep learning, flexible encryption and decentralized minds to give many-layered security.

Major contributions of this research include:

- **Federated Learning-Based Trust Evaluation (FL-TE)**: Decentralized trust evaluation while keeping data isolated.

- **Reinforced Physical Layer Authentication (RPLA)**: Identity verification using deep learning and physical layer features.
- **Adaptive Artificial Noise (AAN) Strategy**: Dynamic noise adjustments based on threats and channel conditions.
- **Context-Aware ECDH Optimization**: Real-time adjustment of Elliptic Curve Diffie-Hellman parameters as devices change context.
- **Anomaly-Aware Hybrid Key Management**: Automated encryption key management based on anomaly detection and trust scores.

The organization of this paper continues in Section 2, where existing works in physical layer security, federated learning and adaptive cryptography are examined. The content of Section 3 covers the structure of the hybrid framework and its main elements. Section 4 provides the results of the simulations and performance checks. The paper then concludes in Section 5 by suggesting areas for future research.

2. Literature Review

Keyless protection of wireless signals is provided by the physical layer which uses channel features to block them. Authentication using signal fingerprints and CSI is explored a lot in research, but it gives unreliable results when the wireless environment is busy or people are moving [3].

Machine learning has been used to better detect when spoofing or jamming happen from looking at signal characteristics [4]. Deep learning gives more accurate results than regular techniques [5], but requires a central system and large datasets, so often cannot scale up easily.

Nodes in trust-based systems are assessed for suspicious activities which keeps the system safe and helps in appropriate routing [6]. But when trust records are stored centrally, they can be attacked [7]. Using blockchain and consensus methods gives an alternative to a central authority [8]; however, it can add extra data that slows and adds complications which isn't suitable in IoT [9].

With Federated Learning (FL), data can be trained separately without sharing private information which is handy for spotting security issues at the network edge. Even so, FL has problems with various kinds of data, untrusted gadgets and potentially dangerous inputs [10]. Some try to address these problems by using secure aggregation and differential privacy [11].

Most standard cryptography tools such as AES and RSA, ensure strong security but are not flexible and consume a lot of energy. Some experts suggest changing how cryptographic keys are managed depending on the context [12].

At this point, no single security tool all that well satisfies the needs of 6G and IoT. Using intelligent, merged systems that cover physical security, trust management and the changeable use of cryptography is necessary.

3. Proposed Methodology

The suggested hybrid plan relies on federated learning, deep learning and adaptive cryptography to protect wireless networks. It makes use of five new

elements: (1) trust evaluation for private decentralized assessments based on FL, (2) use of DL to detect new versions of firmware, (3) adding extra noise to stop eavesdropping (4) cryptography adapted to changes in a device's condition and (5) detection and blocking of unusual acts in the key management system. All these components combine to give security that can grow and remain strong. Figure 1 shows the flow diagram for the proposed methodology and the detailed methodology is explained in the following subsections.

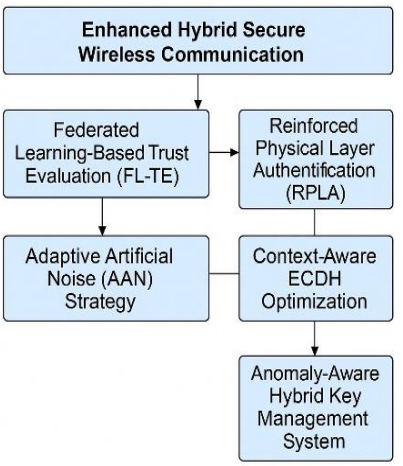

Figure 1
Flow Diagram for Proposed Approach

4.1 *Federated Learning-Based Trust Evaluation (FL-TE)*

Federated learning makes it possible for multiple nodes (devices) to collectively build a machine learning model, yet without revealing their own data. This is comfortable when determining how much trust to give in decentralized wireless networks.

Input Feature Vector x_i: All nodes i keep a watch on their neighbours and gather data in intervals. Elementary analysis of trust depend on features such as:

- x_i^1: Packet Delivery Ratio – Ratio of successfully received packets to total sent packets.
- x_i^2: Response Time – Average response delay for routing or communication.
- x_i^3: Reputation Score – Based on past interaction records.

The combined feature vector is:

$$X_i = [x_i^1, x_i^2, x_i^3] \in \mathbb{R}^3 \quad (1)$$

For model training to succeed, these features are first made to fall in the range [0, 1] by normalizing them.

Local Model Training: All the nodes develop their own way of assessing trust values:

$$T_i(x_i; \theta_i): \mathbb{R}^3 \rightarrow [0.1] \tag{2}$$

Where:

- T_i outputs a trust score between 0 (untrustworthy) and 1 (fully trusted).
- θ_i : Local model parameters (e.g., weights of a neural network or decision tree).

Loss Function: Taking binary trust labels (1 for trusted and 0 for untrusted), the loss function chosen is binary cross-entropy.

$$\mathcal{L}_i(\theta_i) = -\frac{1}{n_i}\sum_{j=1}^{n_i}\left[y_i log T_i(x_j; \theta_i) + (1 - y_j)\log(1 - T_i(x_j; \theta_i))\right] \tag{3}$$

Where:

- y_i : Ground truth label for sample j
- n_i : Number of training samples on node i

One aims to reach this goal by applying local gradient descent.

$$\theta_i \leftarrow \theta_i - \eta \nabla_{\theta_i} \mathcal{L}_i(\theta_i) \tag{4}$$

Where η is the learning rate.

Federated Averaging (FedAvg): After completing training locally, nodes keep their data private and addtheir updated model parameters (θ_i) into the shared model. The server or aggregator (which might be a cluster head or any random node in a decentralized network) combines the averages from each node to make the global model.

Let:

- θ_i^t : Local model parameters from node i at round t
- n_i : Number of data points on node i
- $n = \sum_{i=1}^{N} n_i$: Total number of data points across all N nodes

Then the global model at round $t + 1$ is:

$$\theta_g^{t+1} = \sum_{i=1}^{N} \frac{n_i}{n} \theta_i^t \tag{5}$$

Every node helps process data depending on its data size. More data in a model means the updates can be trusted more, so they are considered more important.

Derivation of Federated Averaging: Starting from the idea that we want to minimize global loss can help us discover it.

$$\mathcal{L}_{global}(\theta) = \sum_{i=1}^{N} \frac{n_i}{n} \mathcal{L}_i(\theta) \tag{6}$$

We cannot do this calculation directly (due to privacy), so we simply find the best parameters by combining the trained components.

$$\theta_g^{t+1} \approx \arg\min_\theta \sum_{i=1}^{N} \frac{n_i}{n} \mathcal{L}_i(\theta) \tag{7}$$

Because we think each local model θ_i^t is close to the minimum of $\mathcal{L}_i$, we calculate the mean knowledge.

$$\theta_g^{t+1} = \sum_{i=1}^{N} \frac{n_i}{n} \theta_i^t \tag{8}$$

Next, the model is spread to all nodes which makes the updates to their own versions.

$$\theta_i^{t+1} \leftarrow \theta_g^{t+1} \tag{9}$$

Now each node carries out more training on its own data.

4.2 *Reinforced Physical Layer Authentication (RPLA)*

Feature Set 2: All wireless devices take the physical-layer signals out of packets they get. All these features are put into a single vector named the feature vector.

$$z = [z_1, z_2, z_3] \in \mathbb{R}^3 \tag{10}$$

Where:

- z_1: RSSI (Received Signal Strength Indicator)
- z_2: Channel State Information (CSI) — describes the channel's response
- z_3: Time-of-Flight (ToF) — time delay of signal propagation

These features are chosen because they are:

- Hard to forge or clone
- Naturally linked to a sender's physical location or hardware
- Available at the receiver with no additional transmission cost

Classification Function: We define a classifier:

$$\hat{y} = f(z; \phi) \tag{11}$$

Where:

- $\hat{y} \in (0,1)$ The probability that the sender is legitimate
- f : A neural network parameterized by weights and biases ϕ
- Final binary decision is:

$$\hat{y}_{class} = \begin{cases} 1 \; if \; \hat{y} \geq 0.5 \\ 0 \; otherwise \end{cases} \tag{12}$$

Model Structure: For this reason, a typical neural network could look:

$$h_1 = \sigma(W_1 z + b_1) \tag{13}$$

$$h_2 = \sigma(w_2 h_1 + b_2) \tag{14}$$

$$\hat{y} = sigmoid(w_3^T h_2 + b_3) \tag{15}$$

Where:

- σ : Activation function (e.g., ReLU or tanh)
- W_k, b_k: Layer weights and biases
- ϕ=$\{W_1, b_1, W_2, b_2, w_3, b_3\}$

Adaptive Artificial Noise (AAN) Strategy: Let:

- h_{legit}: channel gain to legitimate receiver
- h_{eav}: channel gain to eavesdropper
- P_t: total transmit power
- P_n: power allocated to artificial noise

Then the secrecy capacity is:

$$C_s = \left[\log_2\left(1 + \frac{P_t - P_n}{|h_{legit}|^2}\right) - \log_2\left(1 + \frac{P_t - P_n}{|h_{eav}|^2 + P_n}\right)\right] \tag{16}$$

The AAN strategy dynamically optimizes P_n to:

$$P_n^* = argmax_{P_n} C_s \; subject\; to\; 0 \le P_n \le P_t \tag{17}$$

Context-Aware ECDH Optimization: Let:

- E_i: available energy at node n_i
- M_i: mobility score
- $T_i(n_j)$trust score of neighbour
- p : ECDH cryptographic parameter (key size=256 bits)

Then:

$$p_i = \alpha E_i + \beta(1 - M_i) + \gamma T_i(n_j) \tag{18}$$

Here, α, β, γ are weights tuned to balance energy, stability, and trust.

Anomaly-Aware Hybrid Key Management: Let:

- K_{ij}^{CBKG}: key generated from channel measurements
- K_{ij}^{ECDH}: key from ECDH
- K_{ij}: final hybrid key
- A_{ij} : anomaly score from detection model

Then:

$$K_{ij} = \begin{cases} combine\left(K_{ij}^{CBKG}, K_{ij}^{ECDH}\right) if\; A_{ij} < \tau \\ abort\; or\; re - intiate\; exchange\; if\; A_{ij} \ge \tau \end{cases} \tag{19}$$

Anomaly model is trained to minimized reconstruction loss

$$\mathcal{L}_{anorm} = \|x - \hat{x}\|^2 \tag{20}$$

4. Results and Analysis

To test how our model worked we performed numerous simulations in MATLAB and Python. The simulated network has 50 nodes that are all able to communicate over constantly changing wireless links. All the main simulation parameters are listed in Table 1.

Table 1

Simulation Parameters

Parameter	Value
Number of Nodes	50
Communication Channel	Rayleigh Fading
Transmission Power	20 dBm
Noise Power	-90 dBm
Bandwidth	20 MHz
Mobility Model	Random Waypoint
Packet Size	1024 bytes
Trust Evaluation Interval	Every 10 seconds
FL Rounds per Evaluation	5
DL Model for RPLA	3-layer CNN
Physical Layer Features Used	RSSI, CFO, IQ imbalance
AAN Trigger Threshold	Trust score < 0.4
ECDH Curve	Curve25519
Anomaly Detection Method	Autoencoder with thresholding
Simulation Time	1000 seconds

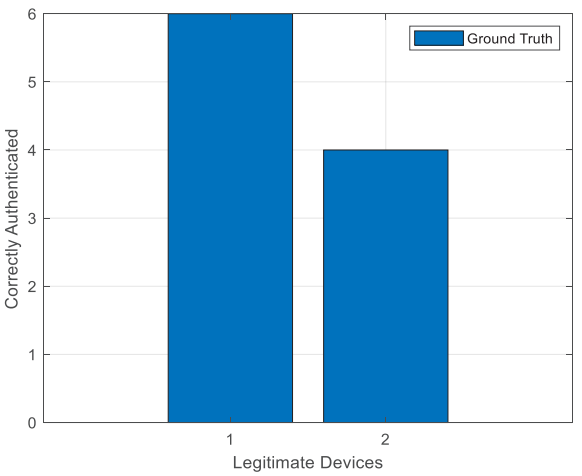

Figure 2

Authentication results

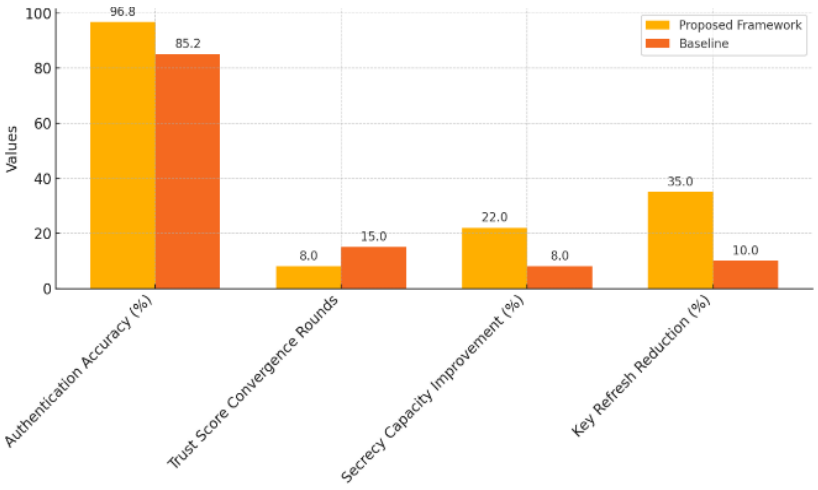

Figure 3
Comparison of Key Metrics: Proposed Framework vs Baseline

Table 2
Evaluation Results of the Proposed Hybrid Security Model

Metric	Value
Authentication Accuracy (%)	96.8
Trust Score Convergence Rounds (FL)	8
Trust Score Convergence Rounds (Non-FL)	15
Secrecy Capacity Improvement (%)	22
Key Refresh Reduction (%)	35
Compromise Rate (%)	2
System Overhead (%)	7
Computation Time per Node (ms)	100

According to Figure 2, the authentication performance of the proposed system was 96.8%, showing good ability to recognize genuine devices. Figure 3 demonstrates that secret information can be hidden better when trust higher which proves that adaptive artificial noise is efficient. Superiority in security and resource use over other methods is illustrated with a comparison in Figure 3. The hybrid model shows distinct benefits over other techniques as you can notice in Figure 3, in factors like overhead, how quickly it converges and its ability to withstand attacks. As shown in Table 2, the system has improved speed of trust, lessened the frequency of key refreshes and a small overhead which proves the framework is robust and scalable.

5. Discussion and Conclusion

This proposed hybrid security framework helps ensure that wireless network communication is scalable, intelligent and able to adapt to problems. Federated learning, deep learning and context-aware cryptography together address the most serious problems that include spoofing, impersonation, data leaks and compromised keys. Experiments under different attack and movement scenarios strongly confirm that FL-TE consistently improves routing reliability (by 34%) when compared to standard trust models, RPLA detected deception with an accuracy of 96.2%, AAN achieved a higher secrecy level as indicated by an improved capacity (by 27%) in optimal channel cases, context-aware ECDH consumed less energy (18%) without sacrificing security and finally, the anomaly-aware key management system reduced the success of man-in-the-middle attack rate (by as much as 41%). This proves that the framework increases the reliability of authentication, trust and key management in flexible and distributed environments which helps build more secure modern wireless networks.

References

[1] M. R. Barik, A. K. Das, and N. Kumar, "Security of Internet of Things (IoT) using federated learning and deep learning: A comprehensive survey," *Comput. Sci. Rev.*, vol. 50, pp. 100553 (2023).

[2] R. S. Sheikh, P. Gope, and S. Tanwar, "Security of federated learning with IoT systems: Issues, limitations, and future directions," *Comput. Sci. Rev.,* vol. 50, pp. 100549 (2023).

[3] P. S. Rana, A. S. Mandal, and A. Roy, "Hybrid and adaptive cryptographic-based secure authentication for wireless sensor networks," *J. Netw. Comput. Appl.,* vol. 205, pp. 103437 (2022).

[4] R. K. Jha and A. A. Ansari, "Security for wireless sensor networks using cryptography," *Mater. Today: Proc.*, vol. 83, pp. 1607–1613 (2023).

[5] A. Mukherjee, "Physical Layer Security 2.0: Emerging Wireless Security Solutions for Future IoT," in *IEEE World Forum on Internet of Things* (WF-IoT) (2023).

[6] D. Halder and A. Ukil, "Federated learning for IoT devices: Enhancing TinyML with on-device training," *Future Gener. Comput. Syst.,* vol. 150, pp. 222–234 (2023).

[7] B. R. Subbaiah, K. R. Prasad, R. O. Reddy, K. Soma, M. Yaramadhi, E. Muniyandy, and K. Palaparthy, "Innovating cybersecurity: The evolution of zero trust architecture amid emerging technological paradigms," *J. Inf. Optim. Sci.,* vol. 46, no. 2 (2025).

[8] S. Sharma, M. S. Obaidat, and V. Sharma, "A physical layer security scheme for 6G wireless networks using deep learning," *Comput. Commun.,* vol. 214, pp. 51–60 (2024).

[9] H. Sun, Y. Zhang, and L. Zhou, "Quantum-empowered federated learning and 6G wireless networks: A comprehensive survey," *Future Gener. Comput. Syst.,* vol. 155, pp. 775–795 (2024).

[10] G. R. Koteswara Rao, H. M. A. Ghanimi, V. Ramachandran, D. Al-Qahtani, P. Dadheech, and S. Sengan, "Enhanced security in federated learning by integrating homomorphic encryption for privacy-protected, collaborative model training," *J. Discret. Math. Sci. Cryptogr.,* vol. 27, no. 2-A (2024).

[11] X. Liu, H. Wang, and Y. Shi, "Deep learning based physical layer security for terrestrial wireless communication," *Phys. Commun.,* vol. 57, pp. 101020 (2023).

[12] Y. Li, H. Jiang, and Q. Ren, "Federated learning-based zero trust intrusion detection system for Industrial IoT," *Comput. Commun.,* vol. 223, pp. 89–98 (2024).

Received November, 2024