International Journal of Applied Mathematics
Volume 38 No. 6s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

ML-PLSR: AN INTEGRATED LIGHTWEIGHT PHYSICAL LAYER SECURED ROUTING ALGORITHM FOR MULTI-HOP WIRELESS NETWORKS INSPIRED BY RANDOM FOREST AND CNN-LSTM

Mrs. Sana Firoz Amin[1*], Dr. Ajay D. Jadhav[2]

Corresponding Author [1]Department of E&TC Engineering, D.Y. Patil School of Engg. & Management, Kasba Bawda, Kolhapur, India Email: sana.mulla@gmail.com

[2]Department Principal, Dnyanshree Inst. of Engg. & Tech.

Satara, Maharashtra, India, Email: profajayjadhav@gmail.com

Abstract

Multi-hop wireless networks, critical to Intelligent Transport Systems, IoT, and industrial automation, face significant security threats like DDoS, jamming, and eavesdropping due to their open and dynamic nature. Existing frameworks often lack real-time adaptability and scalability. This paper introduces ML-PLSR (Machine Learning Based Physical Layer Secured Routing Algorithm), a lightweight, integrated framework for real-time attack detection, intelligent routing, and secure data transmission. Utilizing Random Forest-inspired decision trees for detecting DDoS and jamming via live metrics (PDR, SINR), a Convolutional Neural Networks and Long Short-Term Memory (CNN-LSTM) inspired model for reliable forwarder selection based on spatio-temporal features, and ECC for end-to-end encryption, ML-PLSR ensures robust security and performance. Implemented in NS2 and evaluated across WSN, VANET, and Zigbee, it achieves up to 26.65% higher secrecy capacity, over 92.8% packet delivery ratio, and 98% detection accuracy, offering an efficient solution for securing next-generation wireless networks.

Keywords *— Multi-hop Wireless Networks, Intrusion Detection, Random Forest, CNN-LSTM, ECC, Physical Layer Security, Secure Routing, VANET, WSN, Zigbee, Lightweight Security, Machine Learning.*

I. Introduction

The Modern wireless networks, including Zigbee, Wireless Sensor Networks (WSNs), and Vehicular Ad Hoc Networks (VANETs), face escalating security threats like eavesdropping, jamming, and Distributed Denial of Service (DDoS) attacks due to their open, dynamic nature. Traditional intrusion detection and cryptographic methods are often static, centralized, and ill-suited for rapidly evolving network conditions or sophisticated multi-vector attacks. Many machine learning-based security models rely on offline training, limiting their adaptability to real-time wireless environments where attack patterns and topologies change unpredictably.

Effective security in such networks requires lightweight, adaptive, cross-layer frameworks that coordinate detection, routing, and encryption across physical, network, and application layers. Single-layer solutions often miss critical interdependencies, while heavyweight models are impractical for resource-constrained devices. Recent ML advancements enable

Received: August 10, 2025

International Journal of Applied Mathematics
Volume 38 No. 6s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

dynamic threat adaptation, but most existing solutions treat attack detection, routing, and data protection separately, reducing efficiency.

This work proposes ML-PLSR (Machine Learning Based Physical Layer Secured Routing Algorithm), a unified, lightweight framework for multihop full-duplex wireless networks. It integrates Elliptic Curve Cryptography (ECC) for encryption, Random Forest-inspired decision trees for real-time attack detection, and CNN-LSTM-inspired models for adaptive routing. ML-PLSR ensures scalable, low-latency, energy-efficient protection against layered threats in dynamic wireless environments.

II. Literature Survey

Multi-hop wireless networks, including Zigbee, WSNs, and VANETs, are vulnerable to attacks like jamming, eavesdropping, and DDoS due to open radio propagation and dynamic topologies. Traditional static intrusion detection systems struggle to adapt to evolving threats, prompting the use of machine learning (ML) techniques like Random Forest and CNN-LSTM for real-time solutions. However, most existing studies rely on offline-trained models with static datasets, limiting adaptability to dynamic attack patterns and network mobility.

Al-Abadi et al. (2023) [1] achieved 99.845% accuracy in detecting DDoS in IoMT using K-means and Random Forest, but simulations limit real-world applicability. Buczak and Guven (2016) [2] reported 98.5% accuracy with Decision Trees, though outdated datasets reduce relevance. Priyadarshani et al. (2024) [3] detected jamming in mmWave/THz with 97.5% accuracy, but terahertz security research remains limited. Nguyen and Hoang (2024) [4] applied ML for VANET attack detection, struggling with complex mobility. Wang et al. (2021) [5] used SVM for Zigbee-WiFi spoofing detection (98.67% accuracy), limited by indoor testing. Salmi and Oughdir (2022) [6] achieved 94.4% accuracy against WSN DoS using CNN-LSTM, but computational overhead persists. Alam et al. (2024) [7] detected IoT botnets with 99.87% accuracy, constrained by dataset dependency. Al-Haija et al. (2024) [8] reported 99.92% accuracy with ELMs, limited by dataset reliance. Mohamed (2023) [9] explored ECC for IoT security, lacking practical validation.

In WSNs, Salmi and Oughdir (2022) [6] and Al-Haija et al. (2024) achieved 94.4% and 93.8% accuracy, respectively, but faced challenges with simulated datasets and computational complexity. For Zigbee, Wang et al. (2021) [5] and Alam et al. (2024) [7] showed high accuracy (98.67% and 99.87%), but indoor testing and traffic complexity limit generalization. These studies highlight ML's potential but underscore challenges in scalability, dataset dependency, and real-time deployment.

The ML-PLSR framework addresses these gaps by integrating Random Forest inspired attack detection, CNN-LSTM for forwarder selection, and ECC for encryption. Evaluated on WSN, VANET, and Zigbee networks using NS2, ML-PLSR achieves a secrecy capacity gain of 13.38%–26.65%, packet delivery ratios up to 95.5%, and spectral efficiency of 3.75–4.75 bps/Hz, outperforming traditional PLSR and demonstrating superior security and efficiency.

III. ML-PLSR Framework

The ML-PLSR framework enhances physical layer security in multi-hop wireless networks

Received: August 10, 2025

International Journal of Applied Mathematics
Volume 38 No. 6s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

(e.g., WSN, VANET, Zigbee) by integrating CNN-LSTM for optimal forwarder selection, Random Forest for real-time threat detection (e.g., DDoS, jamming), and ECC for lightweight encryption. It combines secure routing, attack detection, prevention, and data protection for scalability and robustness.

The ML-PLSR Algorithm operates as a distributed system for resource-constrained devices, validated via network simulation. Its workflow includes:

1. Neighbor discovery and topology update.

2. Malicious node detection using node-local decision trees inspired by Random Forest principles.

3. CNN-LSTM-based forwarder selection.

4. ECC-based packet encryption.

5. Real-time routing adaptation to exclude threats.

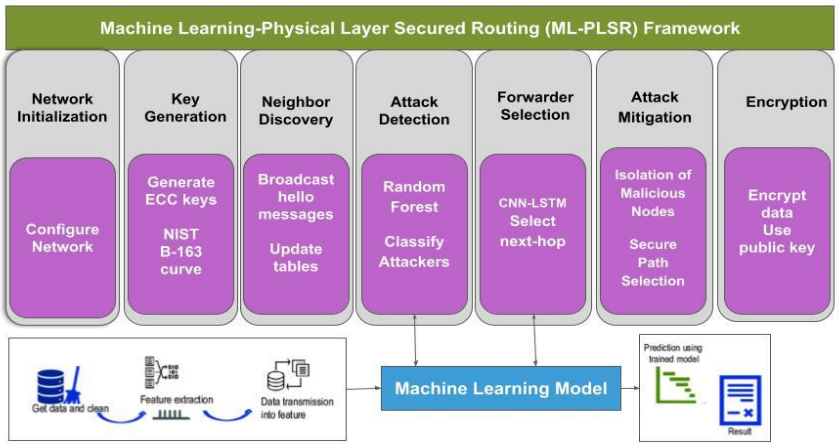

Fig. (1): ML-PLSR Framework

A. Algorithm and Flowchart of ML-PLSR

(i) Data Collection: Real-time physical layer metrics such as node energy, inter-node distance, and SINR (Signal-to-Interference-plus-Noise Ratio) are collected and stored in local buffers.

(iii) Threat Detection: Each node constructs a lightweight, locally maintained decision tree inspired by Random Forest principles. These trees use live packet features to identify malicious behaviors, such as jamming, eavesdropping, and DDoS. Detected nodes are dynamically added to a local blacklist.

(iv) Routing: A CNN-LSTM model processes spatio-temporal traffic features to identify reliable next-hop forwarders, improving routing resilience under adversarial conditions.

(v) Data Protection: Elliptic Curve Cryptography (ECC) is used for lightweight encryption of packets at the physical layer, ensuring data confidentiality and low computational overhead.

Received: August 10, 2025

International Journal of Applied Mathematics
Volume 38 No. 6s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

(vi) Evaluation: NS2 simulation trace files are used to compute key performance metrics such as packet delivery ratio, average latency, secrecy capacity, and real-time detection accuracy.

Algorithm 1 ML-PLSR Protocol

Input: Node ID i, incoming packet p, neighbor set N_i, features $X_i = [e_i, d_i, s_i]$
Output: Forwarded packet or threat response
Initialize data buffers and local blacklist B
while network is active **do**
    Collect features X_i from current transmission context
    if p is a data packet **then**
        Perform threat detection using node-local decision tree (Random Forest-inspired)
        if malicious behavior detected **then**
            Add suspected node to blacklist B
        end if
        Use CNN-LSTM model to select optimal next-hop $j^* \in N_i \setminus B$
        Encrypt payload of p using ECC
        Forward packet p to node j^*
    else if p is a control packet **then**
        Update neighbor set N_i and link cost information
    end if
    Log event to NS2 trace file
end while
Post-simulation: extract performance metrics from trace file

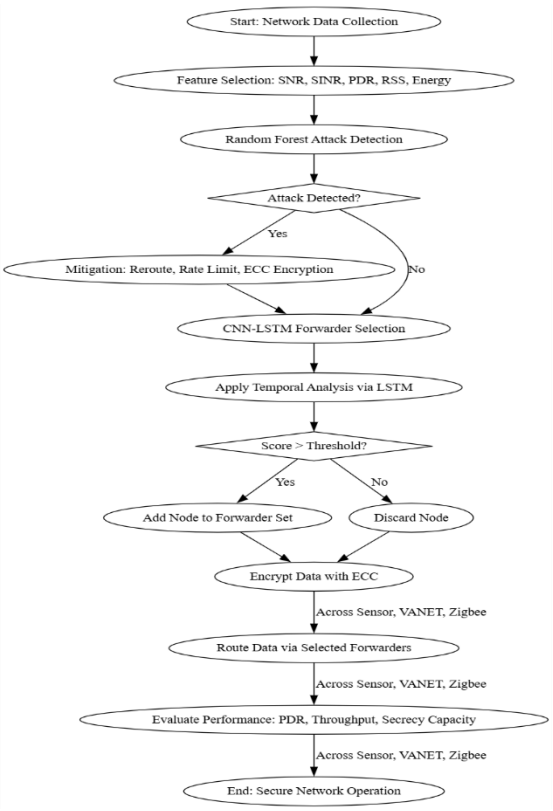

Fig. (2): Algorithm and Flowchart of ML-PLSR

Received: August 10, 2025

International Journal of Applied Mathematics
Volume 38 No. 6s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

IV. Methodology

The ML-PLSR algorithm integrates lightweight machine learning and Elliptic Curve Cryptography (ECC) for secure, adaptive routing in wireless sensor networks (WSNs). It combines secure path establishment, attack detection, intelligent forwarder selection, and efficient encryption for resource-constrained environments.

A. Secure Routing and Cost Evaluation

ML-PLSR uses proactive neighbor discovery with periodic control messages to maintain topology. Nodes evaluate link quality using Packet Delivery Ratio (PDR) and Signal-to-Interference-plus-Noise Ratio (SINR). The path cost is determined as a weighted function of distance and link quality, where higher weights correspond to poor connectivity or increased transmission distance.

$$C(\pi) = \sum_{(i,j)\epsilon\pi} (w_1 . d_{ij} + w_2 . (1 - q_{ij})) \quad (1)$$

Where d_{ij} is the distance, q_{ij} is link quality, and w_1, w_2 are weights.

B. Random Forest-Inspired Attack Detection

The ML-PLSR framework incorporates a lightweight, distributed attacker detection mechanism inspired by the Random Forest algorithm. Unlike traditional ensemble-based approaches, each node maintains a single optimized decision tree constructed from real-time packet observations. This design ensures fast, localized decision-making suitable for dynamic and resource-constrained environments like WSNs and VANETs.

(i) Data Collection: Each node monitors packet-level attributes such as Packet Delivery Ratio (PDR), routing path node IDs, and signal anomalies during transmission.

(ii) Feature Evaluation: The key metric for detection is PDR. A threshold value is applied for binary classification into malicious or benign behavior.

(iii) Tree Construction and Detection: The decision tree minimizes Gini impurity to identify the optimal splits:

$$G = 1 - \sum_{i=1}^{G} p_i^2 \quad (2)$$

$$G_{total} = \frac{n_{left}}{n} G_{left} + \frac{n_{right}}{n} G_{right} \quad (3)$$

Nodes consistently associated with low PDR are flagged as malicious based on majority voting across the node's packet history. This single-tree, Gini-based model provides real-time, scalable detection without the overhead of ensemble forests.

Where p_i is the probability of class i, and n_{left} , n_{right} represent the sample counts.

Received: August 10, 2025

International Journal of Applied Mathematics
Volume 38 No. 6s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

C. Attack Mitigation Strategy

Once an attacker is identified, adaptive mitigation techniques are applied:

(i) Jamming: Nodes monitor SINR fluctuations to detect potential jamming. Affected routes are bypassed by selecting alternative paths through high-SINR neighbors.

(ii) DDoS: To prevent overload from traffic spikes, a rate-limiting mechanism is triggered. Incoming traffic is capped by a predefined threshold to avoid congestion and maintain stability.

$R_L = \min(R_{incoming,} R_{thresh})$

where $R_{incoming}$ is the observed traffic rate and R_{thresh} is the safe upper bound.

(iii) Eavesdropping: ECC-based encryption ensures that even if transmission is intercepted, the payload remains confidential. Detected attackers are removed from routing tables, and neighboring nodes are notified through secure broadcast to reroute traffic.

D. CNN-LSTM-Inspired Forwarder Selection

The ML-PLSR framework employs a CNN-LSTM-inspired heuristic for selecting the optimal forwarder based on spatio-temporal parameters. While full CNN and LSTM models are not trained, the system approximates their behavior through real-time scoring of node features such as energy, distance, and SINR.

(i) Feature Collection: Each node measures residual energy, distance to destination (d_i), and SINR (s_i).

(ii) Feature Aggregation: A composite score is calculated by combining energy, distance, and SINR values.

$$x_i = e_i + d_i + s_i \quad (4)$$

A ReLU activation is applied to normalize scores.

$$ReLU(x) = \max(0, x) \quad (5)$$

(iii) **Heuristic Scoring:** A lightweight update rule models LSTM-style adaptation by adjusting the node score based on recent behavior and output from the activation layer.

$$s_i = s_i + \frac{o}{s_i + o} \quad (6)$$

Where o represents output from the activation layer based on recent node behavior.

(iv) **Forwarder Selection:** The node with the highest score among neighbors not in the blacklist is selected as the next hop. This approach provides real-time, resource-efficient routing decisions that adapt to both mobility and attack conditions without requiring offline model training.

E. ECC-Based Cryptographic Protection

To ensure end-to-end data confidentiality, ML-PLSR integrates Elliptic Curve Cryptography

Received: August 10, 2025

International Journal of Applied Mathematics
Volume 38 No. 6s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

(ECC) at the physical layer. ECC offers high security with minimal computational cost, making it ideal for energy-constrained multihop networks.

(i) Private Key Generation: Each node generates a private key derived from its unique ID using a secure hash function.

$$d = OS2IP\big(SHA1(ID)\big) \quad (7)$$

where d is the node's private key derived from its ID.

(ii) Public Key Computation: The public key is computed by multiplying the private key with a base point on the NIST B-163 curve.

$$Q = d.G \quad (8)$$

where G is a base point on the NIST B-163 curve.

Encryption Process: The sender encrypts the data using the receiver's public key. A random ephemeral key is used to compute cipher components, ensuring data confidentiality even if intercepted.

$$C_1 = k.G, C_{2=} Data + xkQ_B \quad (9)$$

where k is a randomly selected ephemeral key.

Decryption Process: The receiver uses their private key to reconstruct the shared secret and retrieve the original data. Only the intended recipient can decrypt the message, ensuring secure communication. This makes ECC a practical choice for securing lightweight multihop communication.

$$kQ_B = d_B.C_{1,} \quad Data = C_2 - xkQ_B \quad (10)$$

Where C_1 is the ephemeral key component, C_2 is the encrypted data, ,G is the elliptic curve base point, Q_B is the receiver's public key, d_B is the receiver's private key, kQ_B is the shared secret, and xkQ_B is the x-coordinate of the shared secret.

V. Implementation and Simulation Setup

The ML-PLSR algorithm was evaluated through simulations in Wireless Sensor Networks (WSNs), Zigbee networks, and Vehicular Ad Hoc Networks (VANETs), selected for their distinct characteristics: static, resource-constrained nodes in WSNs, low-power IEEE 802.15.4 in Zigbee, and high-mobility, dynamic topologies in VANETs. This diversity ensures a robust assessment of ML-PLSR's adaptability across real-world scenarios.

ML-PLSR was compared against a baseline PLSR (Physical Layer Secured Routing) algorithm without machine learning, both employing ECC encryption and threshold-based detection for fair evaluation. The algorithm was implemented in NS2, with adaptations to meet the MAC and physical layer requirements of each network. The following subsections detail the simulation environment and algorithmic modifications.

A. Simulation Environment

NS2 simulations compared ML-PLSR and PLSR across WSN, Zigbee, and VANET

Received: August 10, 2025

International Journal of Applied Mathematics
Volume 38 No. 6s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

scenarios. WSN and Zigbee setups used 100 nodes in a 500 × 500 m area with IEEE 802.15.4. VANETs were simulated in a 1000 × 1000 m area using IEEE 802.11p to model dynamic topologies. Attacker models (jammers, eavesdroppers) tested security. Key metrics included throughput, packet delivery ratio (PDR), delay, and secrecy capacity. Trace file analysis confirmed ML-PLSR's superior detection rates and security under diverse attack scenarios compared to PLSR.

dynamic road environments.

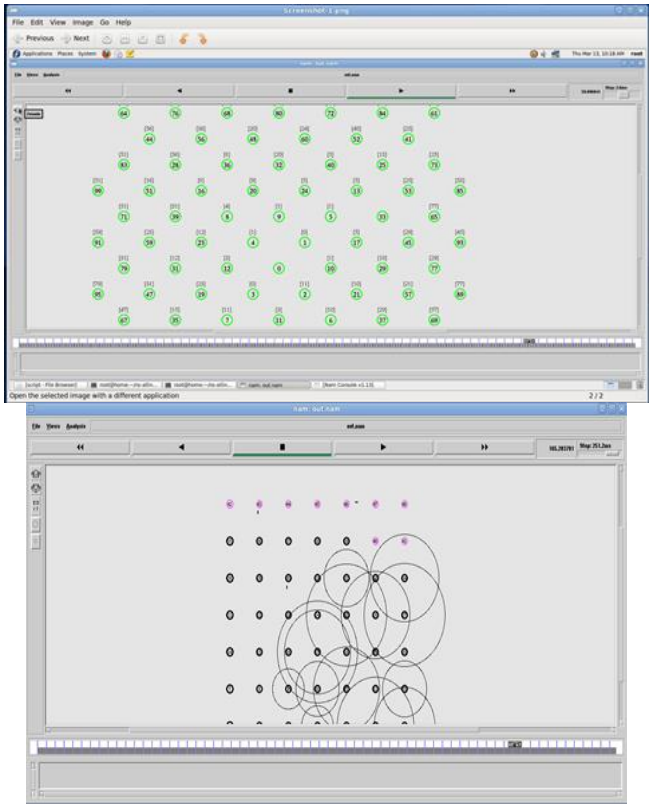

Fig. (3): Network Simulation in NS2

B. Implementation of ML-PLSR in VANET Networks

For highly dynamic environments, ML-PLSR was implemented in Vehicular Ad Hoc Networks (VANETs) using the IEEE 802.11p MAC protocol. In VANETs, ML-PLSR uses Round Trip Time, Traffic Volume, Energy Consumption, Channel Occupancy, SNR, and PDR. Random Forest detects attacks, while adaptive strategies mitigate threats. Simulations in a 1000 × 1000 m area with IEEE 802.11p model vehicular dynamics. ML-PLSR outperforms PLSR in PDR and secrecy capacity, ensuring connectivity and resilience.

C. Implementation of ML-PLSR in Zigbee Networks

ML-PLSR was adapted for Zigbee networks using IEEE 802.15.4 MAC and PHY layers, suitable for low-power, low-bandwidth, energy-constrained IoT environments. NS2's Zigbee module was modified to incorporate ML-PLSR's components: CNN-LSTM for node scoring, Random Forest for attack detection, and ECC for packet encryption. The routing layer was

Received: August 10, 2025

International Journal of Applied Mathematics
Volume 38 No. 6s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

tailored to Zigbee's cluster-tree topology. Simulation parameters included reduced transmission power, smaller packet sizes, and sleep scheduling to emulate Zigbee device behavior. In a 500 × 500 m area, ML-PLSR improved throughput, secrecy capacity, and detection accuracy, enhancing Zigbee's scalability for IoT and industrial applications.

Algorithm 2 ML-PLSR for VANETs

Input: Packet p, RF data RF, sensed S, threshold T
Output: Next hop N, attacker list A
Collect S, init ECC keys K (NIST B-163), update neighbor table
if RF.count $< Threshold$ **then return**
end if
for feature f **do**
    Compute Gini for split at $T_f \in [30, 40]$; update T if Gini improves
end for
for node n in p **do**
    if $\text{PDR}_n \leq T$ or Jamming(p) **then** add n to A
    end if
end for
Run CNN-LSTM on S: $S_n = \sigma(\text{LSTM}(\text{ReLU}(\text{Conv}(S))))$
if $S_n \geq T$ **then** set $N = n$
end if
Encrypt $D_e = D + K$; route via N avoiding A
return N, A

Algorithm 3 ML-PLSR on Zigbee

Input: Packet p, RF RF, sensed S, threshold T
Output: Forwarder F, attacker list A
Collect S, init ECC keys K, update RF
if RF.count $< Threshold$ **then return**
end if
for feature f **do**
    Evaluate Gini for $T_f \in [30, 40]$; update T if improved
end for
for node n in p **do**
    if $\text{PDR}_n \leq T$ or Jamming(p) **then** add n to A
    end if
end for
Run CNN-LSTM on S: $S_n = \sigma(\text{LSTM}(\text{ReLU}(\text{Conv}(S))))$
if $Sificent \geq T$ **then** set $F = n$
end if
Encrypt $D_e = D + K$; route via F avoiding A
return F, A

Fig. (4): Algorithm of ML-PLSR on VANET and Zigbee Network

D. Physical Layer Secured Routing (PLSR)

PLSR is a baseline framework using similarity metrics (Jaccard Coefficient, Cosine Similarity, and Levenshtein Distance) for neighbor validation and attack detection (e.g., eavesdropping, DDoS, and jamming), with ECC for lightweight encryption. Its low computational complexity makes it ideal for comparison with ML-PLSR, showcasing the latter's enhanced attack detection, routing resilience, and efficiency.

Received: August 10, 2025

International Journal of Applied Mathematics
Volume 38 No. 6s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Algorithm 4 PLSR Algorithm

Input: Network data D, neighbors N, threshold T
Output: Path P, attacker list A
Collect D, generate ECC keys K (NIST B-163)
for $n \in N$ **do**
    if $d(n) \leq R$ **then** keep n
    end if
end for
Compute Jaccard J, Cosine C, Levenshtein L
if $J < T$ or $C < T$ or $L > T$ **then** add n to A
end if
Encrypt $D_e = D + K$, compute P excluding A
Monitor jamming; update A if count ≥ 5
return P, A

Fig. (5): Algorithm of PLSR

VI. Results and Discussion

A. Evaluation of ML-PLSR with Existing Work

This subsection compares ML-PLSR with the NIDS-CNN-LSTM model by Du et al. (2023)[10], a deep learning-based intrusion detection system using a similar CNN-LSTM structure for DDoS attack detection. Performance was evaluated on the CICIDS2017 dataset using accuracy, F1-score, recall, and precision. ML-PLSR outperformed NIDS-CNNLSTM, achieving 96.94% accuracy and 95.62% F1-score compared to 96.17% and 95.87%, respectively. ML-PLSR's recall (96.94%) surpassed NIDS-CNNLSTM's (95.50%), indicating superior attack detection. However, NIDS-CNNLSTM's precision (95.80%) slightly exceeded ML-PLSR's (94.33%). Figure 4 illustrates these results.

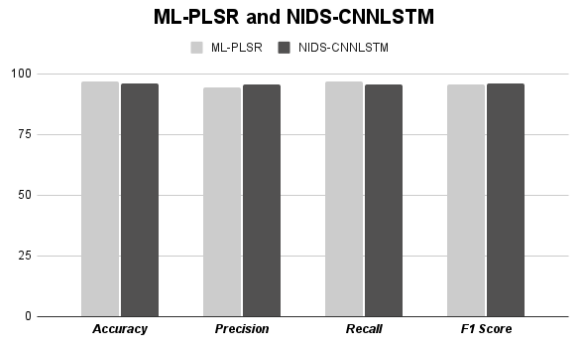

Figure (6): ML-PLSR Vs NIDS-CNNLSTM

B. Evaluation of ML-PLSR with PLSR

This subsection compares ML-PLSR with the non-machine learning Physical Layer Secured Routing (PLSR) algorithm, tracking packet delivery ratio (PDR), throughput, secrecy capacity, communication cost, and secrecy outage probability, as shown in Figures 7(a to e). ML-PLSR outperformed PLSR across Sensor, VANET, and Zigbee networks. In Sensor networks, ML-PLSR achieved a PDR of 91.48% and throughput of 76.60 kbps, compared to

Received: August 10, 2025

International Journal of Applied Mathematics
Volume 38 No. 6s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

PLSR's 85.02% PDR and 67.41 kbps throughput. ML-PLSR's Random Forest and CNN-LSTM models enabled robust detection of DDoS, eavesdropping, and jamming, with adaptive routing ensuring resilience to evolving threats, demonstrating its superiority over PLSR.

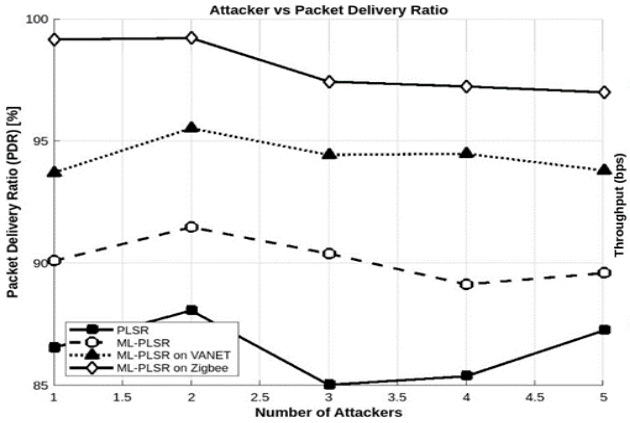

Figure 7a: Packet Delivery Ratio

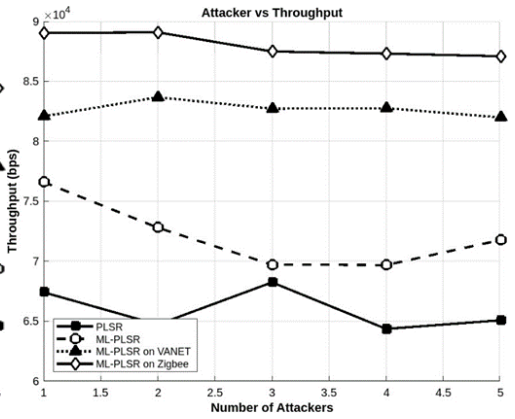

Figure 7b: Throughput

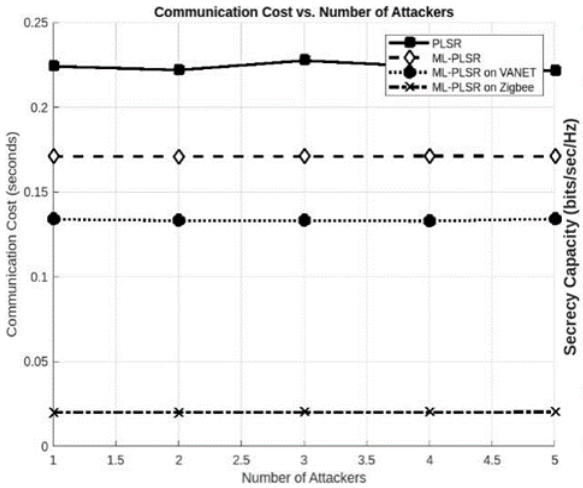

Figure 7c: Communication Cost

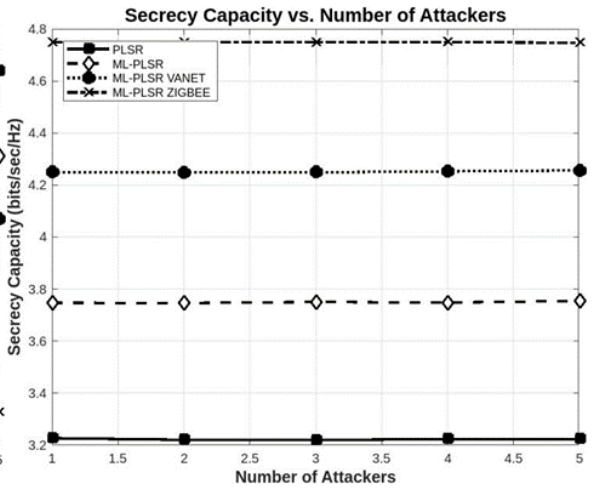

Figure 7d: Secrecy Capacity

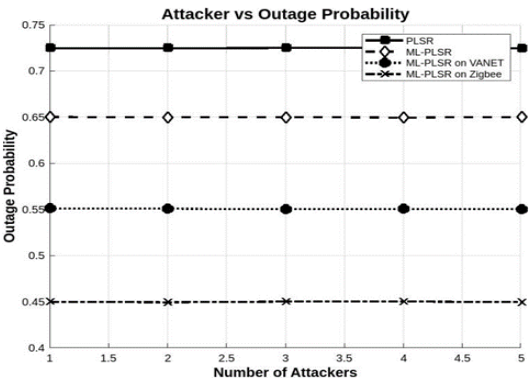

Figure 7e: Outage Probability

Received: August 10, 2025

International Journal of Applied Mathematics
Volume 38 No. 6s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

C. Evaluation of ML-PLSR QoS Metrics in Diverse Wireless Environments

Figures 7(a to e) plot PDR, throughput, communication cost, secrecy capacity, and secrecy outage probability against 1–5 attackers. In Sensor networks, ML-PLSR achieved a PDR of 91.48%, throughput of 76.60 kbps, communication cost of 0.17 ms, and accuracy of 96.73–96.94%, suitable for resource-constrained wireless applications. In Zigbee, ML-PLSR excelled with a PDR of 99.2%, throughput of 76.60 kbps, secrecy capacity of 4.74 bps/Hz, communication cost of 0.02 ms, secrecy outage probability of 0.4499, and accuracy of 98.85–99.06%, ideal for low-power IoT applications like smart homes and healthcare. In VANETs, ML-PLSR achieved a PDR of 95.53%, throughput of 83.68 kbps, communication cost of 0.13 ms, secrecy outage probability of 0.5502, and accuracy of 97.33–98.14%, supporting safety-critical applications like autonomous driving. ML-PLSR Zigbee offered the highest efficiency, VANET provided the highest throughput, and Sensor networks balanced performance, demonstrating ML-PLSR's versatility across diverse wireless networks.

D. Evaluation of ML-PLSR Classification Metrics in Diverse Wireless Environments

This subsection evaluates ML-PLSR's attack detection performance across Sensor, VANET, and Zigbee networks, analyzing accuracy, precision, recall, F1-score, and error rate under 1–5 attackers. ML-PLSR achieved peak accuracies of 96.95% (Sensor), 99.07% (Zigbee), and 98.14% (VANET), as shown in Figure 8a. Precision reached 94.33% (Sensor), 98.51% (Zigbee), and 98.76% (VANET), minimizing false positives (Figure 8b). Recall was 96.95% (Sensor), 99.01% (Zigbee), and 98.14% (VANET), ensuring robust threat detection (Figure 8c). F1-scores were 95.62% (Sensor), 98.85% (Zigbee), and 98.45% (VANET), balancing precision and recall (Figure 8d). Error rates remained low at 2.96% (Sensor), 0.93% (Zigbee), and 1.86% (VANET), with slight increases as attackers grew (Figure 8e). ML-PLSR excelled in Zigbee's low-power environment, achieving optimal PDR, secrecy capacity, and communication cost for IoT applications (e.g., smart homes, healthcare). In VANETs, it ensured high throughput and low outage probability, supporting safety-critical applications like autonomous driving, demonstrating versatility across dynamic wireless environments.

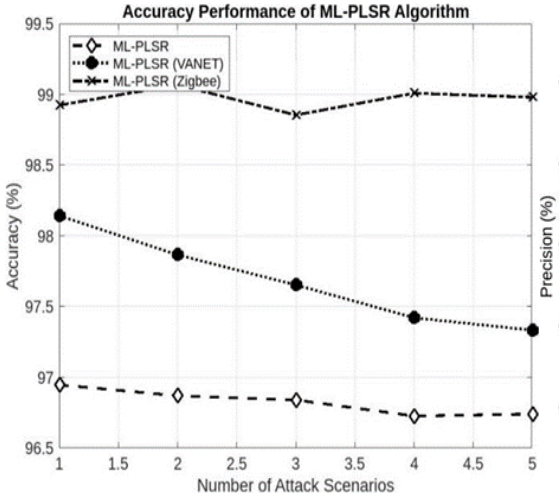

Figure 8a: Accuracy

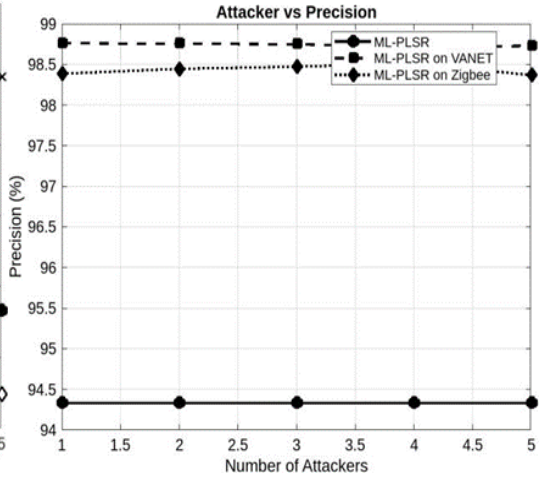

Figure 8b: Precision

Received: August 10, 2025

International Journal of Applied Mathematics
Volume 38 No. 6s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

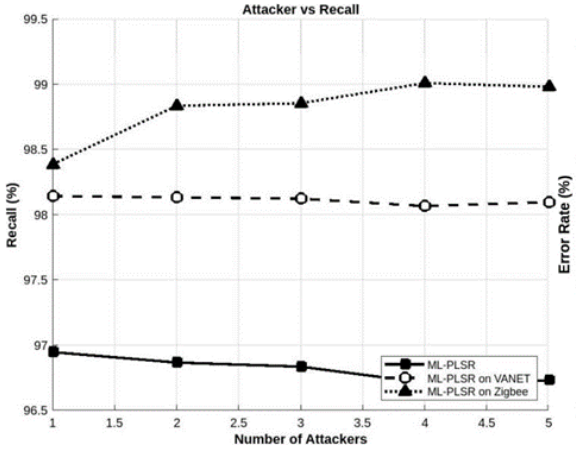

Figure 8c: Recall

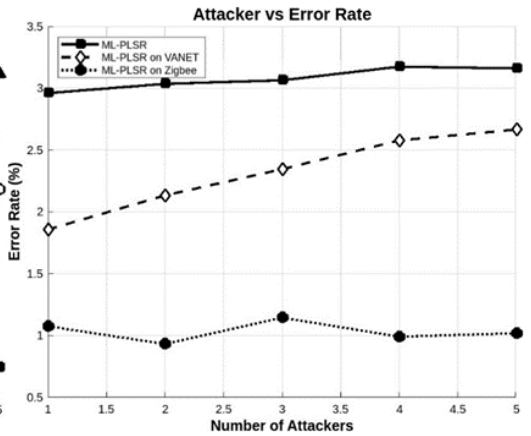

Figure 8d: Error Rate

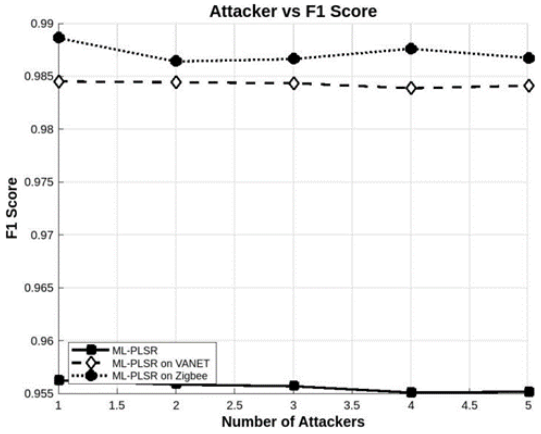

Figure 8e: F1-Score

VII. Conclusion

This study presents two key comparisons. The first evaluates ML-PLSR against a baseline non-ML PLSR algorithm to assess the impact of integrating machine learning-inspired techniques on network security and performance. The second examines ML-PLSR across Sensor, VANET, and Zigbee networks to evaluate its versatility and suitability for different wireless environments. Together, these comparisons demonstrate that ML-PLSR not only improves resilience and attack detection but also adapts effectively to varied network conditions and constraints. In Sensor networks, ML-PLSR achieved a packet delivery ratio (PDR) of 91.48–99.2%, throughput of 76.60–83.68 kbps, and attack detection accuracy ranging from 96.72% to 99.06%. These values significantly exceeded the baseline PLSR's 85.02% PDR, 67.41 kbps throughput, and 0.7248 secrecy outage probability. When compared to recent models such as NIDS-CNNLSTM (Du et al., 2023)[10], ML-PLSR delivered superior accuracy and F1-scores (95–98%), emphasizing its effectiveness in wireless environments. Among the evaluated topologies, Zigbee exhibited the highest PDR (99.2%), while VANET and sensor networks demonstrated strong performance in vehicular and resource-constrained applications, respectively. These findings open the door for future researchers to explore more advanced, trainable, and distributed learning models, including transformer-based architectures. Further research should also address computational overhead

Received: August 10, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

and generalization challenges by optimizing the model for real-world deployments and large-scale scenarios. Overall, the results highlight ML-PLSR's versatility and underscore the transformative potential of machine learning in enhancing wireless network security.

References

[1] A. Al-Abadi, M. Mohamed, and A. Fakhfakh, "Enhanced random forest classifier with k-means clustering (erf-kmc) for detecting and preventing distributed-denial-of-service and man-in-the-middle attacks in internet-of-medical-things networks," Computers, vol. 12, no. 12, p. 262, 2023.

[2] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," IEEE Communications Surveys Tutorials, vol. 18, no. 2, pp. 1153–1176, 2016.

[3] R. Priyadarshani, K.-H. Park, Y. Ata, and M.-S. Alouini, "Jamming intrusions in extreme bandwidth communication: A comprehensive overview," 2024. [Online]. Available: https://arxiv.org/abs/2403.19868

[4] T. Nguyen and X. Hoang, "Machine learning-based malicious vehicle detection for security threats and attacks in vehicle ad-hoc network (vanet) communications," 2024, arXiv preprint.

[5] X. Wang, L. Gao, S. Mao, and S. Pandey, "Spoofing attack detection using machine learning in cross-technology communication," Wireless Communications and Mobile Computing, 2021.

[6] S. Salmi and L. Oughdir, "CNN-LSTM based approach for dos attacks detection in wireless sensor networks," International Journal of Advanced Computer Science and Applications, vol. 13, no. 4, pp. 830–837, 2022.

[7] F. Alam, M. Siddique, M. Hossain, and K. Andersson, "Botnet attack detection in iot network using CNN-LSTM," International Journal of Intelligent Systems and Applications in Engineering, vol. 12, no. 2, pp. 82–89, 2024.

[8] Q. Abu Al-Haija, S. Al-Tamimi, and M. Alwadi, "Analysis of extreme learning machines (ELMS) for intelligent intrusion detection systems: A survey," Expert Systems with Applications, vol. 253, p. 124317, 2024.

[9] W. A. Mohamed, "Elliptic curve implementation and its applications: A review," Iraqi Journal of Intelligent Computing and Informatics (IJICI),2023.

[10] J. Du, K. Yang, Y. Hu, and L. Jiang, "NIDS-CNNLSTM: Networkintrusion detection classification model based on deep learning,"IEEE Access, vol. 11, pp. 24 808–24 821, 2023. [Online]. Available: http://doi.org/10.1109/ACCESS.2023.3254915

[11] T.-T. Nguyen, J.-H. Lee, M.-T. Nguyen, and Y.-H. Kim, "Machine learning-based relay selection for secure transmission in multi-hop df relay networks," Electronics, vol. 8, no. 9, p. 949, 2019.

[12] H. H. Bosman, G. Iacca, A. Tejada, H. J. W¨ortche, and A. Liotta, "Spatial anomaly

Received: August 10, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

detection in sensor networks using neighborhood information," Information Fusion, vol. 33, pp. 41–56, 2017.

[13] X. Liu, Y. Yuan, J. Xiao, W. Zheng, and Z. H. Ling, "A novel kalman filter based shilling attack detection algorithm," Mathematical Biosciences and Engineering, 2020.

[14] R. Kareliya, N. Mokal, P. Shah, H. U. Solanki, and S. Shingare, "ML-based network anomaly detection," International Journal of Research Publication and Reviews, 2024.

[15] E. Mohammed and B. E. Ouahidi, "A survey on vanet intrusion detection systems," Journal of Applied Mathematics Informatics, vol. 15, pp. 43–46, 2021.

[16] J. Zhang et al., "A random forest based network intrusion detection system," Journal of Network and Computer Applications, vol. 133, pp.30–41, 2019.

[17] P. A. A. Resende and A. C. Drummond, "A survey of random forest based methods for intrusion detection systems," ACM Computing Surveys, vol. 51, no. 3, pp. 1–36, 2018.

[18] L. Breiman, "Random forests," Machine Learning, vol. 45, no. 1, pp. 5–32, 2001.

[19] W. Lu, J. Li, Y. Li, A. Sun, and J. Wang, "A CNN-LSTM-based model to forecast stock prices," Complexity, vol. 2020, pp. 1–10, 2020. [Online]. Available: https://doi.org/10.1155/2020/6622927

[20] Y. K. Saheed, A. I. Omole, and M. O. Sabit, "Ga-madam-iiot: A new lightweight threats detection in the industrial IoT via genetic algorithm with attention mechanism and LSTM on multivariate time series sensor data," Sensors International, vol. 6, p. 100297, 2025.[Online]. Available: https://doi.org/10.1016/j.sintl.2025.100297

[21] A. W. Khan, M. A. Khan, J. A. Khan, A. Ahmad, and K. A. Abuhasel, "A novel weighted clustering based secure data transmission protocol for wireless sensor networks," IEEE Access, vol. 8, pp. 204 563–204 575, 2020. [Online]. Available: https://doi.org/10.1109/ACCESS.2020.3036412

[22] J. Haseeb, T. H. Im, I. U. Din, A. Almogren, and M. Shafiq, "Secure and energy aware routing protocol using elliptic curve cryptography in wireless sensor networks," Sensors, vol. 21, no. 17, p. 5898, 2021. [Online]. Available: https://doi.org/10.3390/s21175898

[23] I. Ullah, N. U. Amin, M. J. Khan, and H. Khattak, "A lightweight and secure key management scheme for iot networks," Sensors, vol. 23, no. 6, p. 3142, 2023. [Online]. Available: https://doi.org/10.3390/s23063142

Received: August 10, 2025