International Journal of Applied Mathematics

Volume 38 No. 11s 2025,

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

MDLBA-LORA : A MULTIDIMENSIONAL LEARNING-BASED LIGHTWEIGHT ROUTING PROTOCOL FOR SECURE AND EFFICIENT COMMUNICATION IN LORAWAN.

Mrs. Nilofar S. Hunnargi[1], Dr. Ajay D. Jadhav[2]

[1].Assistant Professor, E&TC Engineering Department ATS's SBGI Miraj, Sangli, Maharashtra, India

Email: nilofar.hunnargi@gmail.com

[2.]Principal, Dnyanshree Institute of Engineering and Technology Satara,Maharashtra, India

Email: profajayjadhav@gmail.com

Abstract

LoRa WAN deployments still suffer from unreliable routing, energy constraints, and other vulnerabilities to DoS, injection, jamming, and Man-in-the-Middle attacks. Against this backdrop, this work proposes an intelligent and secure routing framework called MDLBA-LoRa (Multidimensional Learning Based Algorithm for LoRa), which is developed upon lightweight fuzzy logic, a BRNN-inspired anomaly detector, cluster-based priority scheduling, and symmetric encryption with AES-128. MDLBA-LoRa incorporates dynamic reconfiguration through continuous fuzzy trust updates, real-time attacker list management, priority-based queue reordering, and adaptive routing that avoids malicious or low-trust nodes based on evolving network conditions. In this paper, the system is implemented in NS-2, utilizing an LoRa - specific agent that emulates sensor nodes, gateways, and network-server operations. Neighbor trust is evaluated based on real-time metrics such as RSSI, queue length, bandwidth usage, and processing delay using rule-based fuzzy scoring. In this regard, a bidirectional temporal evaluator classifies the traffic as either legitimate or malicious. On the other hand, online clustering identifies high-priority packets for immediate encrypted forwarding, buffering normal traffic for scheduled transmission. Duty-cycle emulation and priority-aware queueing are implemented to ensure realistic energy and delay behavior. Through experimental evaluation against multiple attack scenarios, it significantly outperforms the baseline DLBA, RLLoRa, and DLBA-LoRa frameworks. Packet delivery ratio reaches approximately 87.84%, throughput reaches up to 84 kbps, delay goes down to about 1.28 seconds, and energy consumption reduces to 0.083 J. The accuracy of intrusion detection is over 99.06%. Strong precision, recall, and F1 values are demonstrated. MDLBA-LoRa effectively ensures secure, reliable, and energy-efficient communication for large-scale IoT networks.

Keywords-*IDS, IoT Security, LoRa WAN, Fuzzy Logic, Data Clustering, AES*

Received: August 02, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Encryption, Anomaly Detection

I. Introduction

LoRa WAN has become the leading LPWAN technology in large-scale IoT deployments because of its long range, energy efficiency, and low infrastructure cost. However, open wireless channels and constrained end-devices expose it to several critical security threats such as DDoS, replay, selective forwarding, jamming, and injection attacks. In such an environment, conventional cryptographic methods alone remain insufficient, since they cannot detect compromised nodes or adapt dynamically to rapidly changing network behavior. Learning-based security solutions have also been explored in addressing these challenges. While there are deep learning systems like Deep Defense [1] that show strong anomaly detection accuracy, the required large datasets and the GPU-level computation make them unsuitable for LoRa WAN nodes. Reinforcement Learning lightweight models as studied in [2] offer responses adaptable only to simple threshold updates without considering network factors such as trust, congestion, RSSI More significantly, no previous studies have described real-time attacker isolation, secure routing, or autonomous reconfiguration. To bridge these limitations, earlier work such as DLBA-LoRa introduced trust- and priority-based gateway reconfiguration, improving routing reliability under attack. However, it supports limited dynamic adaptation. This paper presents an enhanced, multi-dimensional security framework for LoRa WAN called MDLBA-LoRa. The system integrates lightweight fuzzy logic for attacker likelihood estimation, lightweight BRNN for anomaly detection, and cluster-based prioritization for efficient data delivery. MDLBA-LoRa performs multi-layer dynamic reconfiguration by updating fuzzy trust scores, isolating malicious nodes through an attacker list, reorganizing packets into priority-based clusters, and adapting routing paths based on real-time neighbour behaviour and temporal deviations. Experimental results illustrate that MDLBA-LoRa significantly reduces delay and energy consumption, and enhances PDR and detection accuracy compared to existing learning-based methods. Its lightweight design makes it a practical and effective security solution in real-world IoT-LoRa WAN deployments. The research paper is organized as follows: I. Introduction II Literature Review, III. Methodology, detailing the proposed framework and implementation workflow. IV. Simulation environment, V. Results and Discussion, analyzing experimental outcomes and performance; VI. Conclusion, summarizing key findings and contributions.

II. Literature Review

A wide variety of research works in the context of IoT security have been performed using machine learning, deep learning, trust models, and blockchain-based mechanisms; however, most of these are still unsuitable for resource-constrained LPWAN contexts such as LoRa WAN. Heavy deep learning systems such as Deep Defense [1] provide very high anomaly detection accuracy but rely on large datasets and computation at the GPU level, thus limiting practical deployments. On the other hand, lightweight approaches such as Reinforcement-Learning-based anomaly detection [2] offer adaptive behavior but rely

Received: August 02, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

only on threshold tuning, with complete neglect of essential network layer factors including trust, congestion, RSSI, or routing security. DLBA-LoRa [3] enhances reliability through trust- and priority-based gateway switching yet has limited reconfiguration mechanism. Further IDS solutions based on GRU models [4], unsupervised ensemble learning [5], CNN image-based detection [10], and autoencoder/SVM/CNN hybrids [11], [12] show promising accuracy but suffer from dataset limitations, poor generalization, high overhead, or limited real-world validation. SDN-based models [6] and blockchain trust frameworks [9] address specific threats but face scalability and deployment constraints. Comparative studies focused on IoT protocols [14], traditional IDS such as Snort [15], and encrypted-traffic detection such as HMMED [16] underline the always present challenges of dataset imbalance, robustness, and applicability to constrained devices. Overall, existing methods fail to integrate attack detection, trust evaluation, fuzzy reasoning, clustering, and secure routing within a unified framework. LoRa WAN still lacks adaptive, node-level IDS mechanisms capable of reconfiguration during ongoing attacks. No integrated framework exists that combines learning, trust, fuzzy logic, and neural IDS for LoRa WAN. In light of the above gap, the proposed MDLBA-LoRa protocol offers a multidimensional adaptive architecture that integrates lightweight fuzzy logic–based attacker detection, BRNN inspired packet classification, clustering-based transmission prioritization, and comprehensive dynamic reconfiguration into one protocol. Hence, a lightweight yet highly effective security solution is achieved for LoRa WAN-based IoT networks.

III. Methodology

Proposed MDLBA-LoRa Framework

The proposed MDLBA–LoRa protocol integrates intelligent decision layers within a realistic LoRa WAN network simulated in NS-2. Fig.1 shows MDLBA-LoRa framework. A lightweight fuzzy-logic module first evaluates neighbors using RSSI, queue length, bandwidth, and delay to prevent malicious participation. Verified packets are examined by a lightweight Bidirectional Recurrent Neural Network (BRNN) inspired algorithm for anomaly detection. Legitimate data are clustered into priority groups through threshold-based similarity analysis, enabling high-priority packets to be transmitted first. All packets undergo AES-128 symmetric encryption before transmission, ensuring confidentiality and integrity. The simulation replicates real LoRa WAN behavior, producing secure, energy-efficient, and high-throughput communication suitable for large-scale IoT networks. Fig. 2 and 3 illustrates the MDLBA-LoRa Flowchart and algorithm implemented in this study respectively, detailing all stages from neighbor assessment to priority-aware secure transmission.

Received: August 02, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

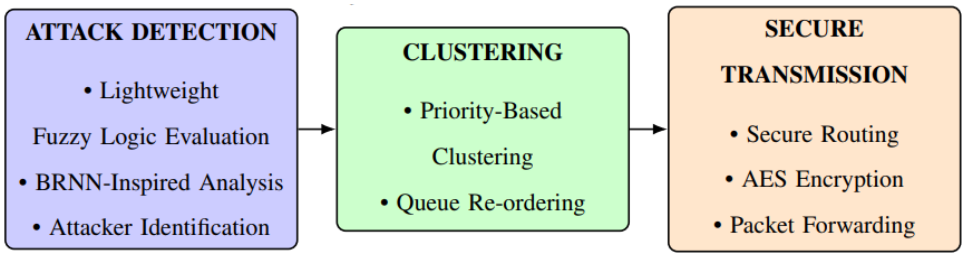


Fig.1 MDLBA-LoRa framework

MDLBA-LoRa addresses the dual challenges of network security and performance. The network optimizes the performance of the nodes with respect to energy consumption and packet delivery. The nodes use the physical layer LoRa for communication and follow the particular features of LoRa WAN, including low data rates, long-range communication, and low power consumption. The data set used in the research work is generated primarily through simulations in the NS-2 environment, reflecting a realistic LoRa

Algorithm MDLBA-LoRa

Deploy N nodes in $X \times Y$ area
Initialize each node with E_0 (initial energy)
Define communication range R_t and LoRa physical parameters (SF, BW, TxPower)
Measure: RSSI, Queue Length (q), Processing Delay (d), Bandwidth usage
Apply lightweight fuzzy rule-based neighbor assessment to compute trust score T
Apply BRNN-inspired bidirectional temporal detector to classify packet/neighbor as legitimate or malicious
if $T < \tau$ **or** packet is malicious **then**
    Mark as attacker / drop packet
else
    Mark as normal node / legitimate packet
end if
Apply threshold-based priority grouping:
    High Priority if $(q \geq \theta_q)$ or $(d \geq \theta_d)$
    Normal Priority otherwise
Encrypt high-priority packets immediately using AES
Encrypt normal-priority packets at dispatch time before transmission
Forward packets according to scheduler and duty-cycle constraints

Received: August 02, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

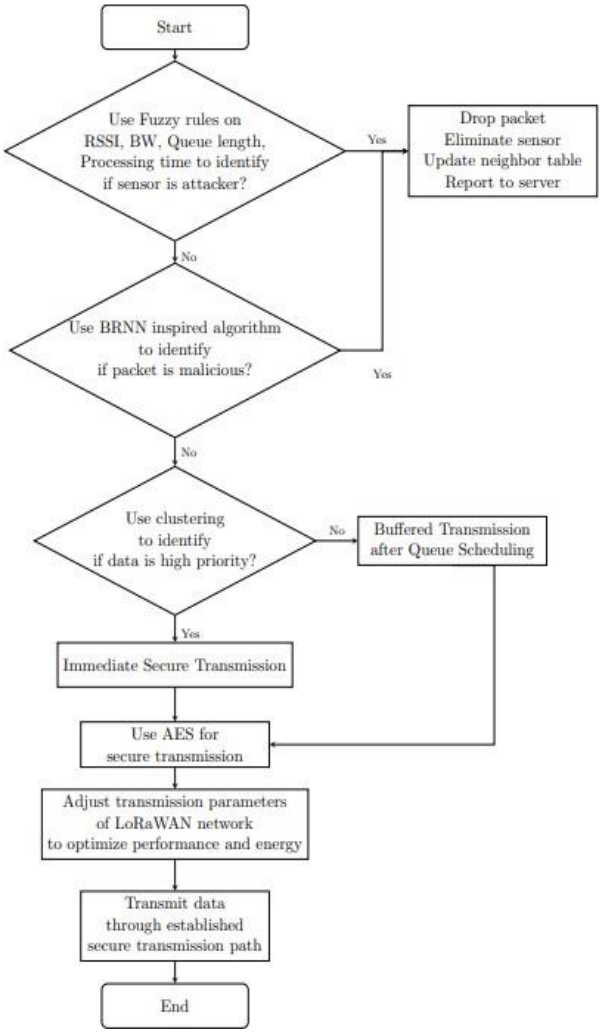


Fig. 2: MDLBA-LoRa Flowchart

Fig.3 MDLBA LoRa algorithm

WAN network scenario. The setup includes various LoRa WAN-specific parameters, such as energy models, transmission power, and modulation schemes, that are critical to mimicking the behavior of real LoRa WAN networks. Every node in the network is configured to use a customized LORA agent developed in NS-2 that emulates key MAC-layer behaviors of packet scheduling, providing realistic node-to-node communication.

The network is subjected to various attack scenarios such as DDoS, injection, zero-day, Jamming, and man-in-the-middle attacks that frequently occur in real-world IoT networks. This simulated attack offers a true representation of possible vulnerabilities in LoRa WAN networks. Network events such as packet transmissions, receptions, energy consumption, and delays are recorded during the simulation. This allows for a tailored environment to simulate specific conditions, such as network congestion and attacks, which provides more flexibility than pre-existing datasets. It allows evaluating protocol, attack detection, AES encryption, and data clustering, providing better control of network parameters with accurate, real-world insights, which standard data sets cannot provide.

Received: August 02, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

1.Attack Detection Layer

The intelligent, adaptive protection in the Attack Detection Layer can be achieved by the combination of lightweight fuzzy logic and machine learning in order to identify and isolate malicious nodes in real time. Fuzzy logic continuously assesses neighbors based on bandwidth, queue length, processing delay, and RSSI to compute trust values that enable early detection and removal of suspicious nodes before routing. In the subsequent process, a BRNN analyzes packet sequences to classify the traffic as either normal or malicious, drops harmful packets, and updates lists of attackers dynamically. This integrated fuzzy-ML approach therefore is capable of enabling real-time and online learning and adaptive anomaly detection that strengthens accuracy, while reducing false alarms, thereby ensuring robust IoT network security under the MDLBA-LoRa framework.

A. Fuzzy Logic–Based Neighbor Assessment

The proposed system incorporates a lightweight fuzzy-logic neighbor evaluation mechanism to ensure reliable route formation and early attacker filtering. In the implementation, each neighboring node is assessed using four real-time indicators—RSSI, queue length, bandwidth usage, and processing delay extracted directly within the LoRa agent. Instead of a full fuzzy inference engine, the system uses simple rule-based mapping to classify each parameter as good, moderate, or poor. These mapped values are then combined into a trust score that reflects the stability and behavior of the neighbor. Nodes with low trust scores are immediately excluded from the routing table and their packets are ignored, preventing unstable or malicious nodes from influencing route discovery. This lightweight fuzzy assessment significantly reduces packet loss and retransmissions, while maintaining very low computational overhead suitable for IoT-class LoRa devices.

B. BRNN Inspired algorithm

The lightweight Bidirectional Recurrent Neural Network (BRNN) integrated into the proposed MDLBA–LoRa protocol as shown in Fig.4.It serves as an embedded, lightweight decision engine for intrusion detection in IoT–LoRa networks. Unlike traditional neural networks that perform gradient-based backpropagation and parameter tuning, this implementation employs rule-driven temporal reasoning using sequential feature analysis in both forward and backward directions. The model continuously monitors each node's behavior over time and classifies its activity as normal or malicious based on dynamic threshold evaluation. The BRNN architecture, within the MDLBA-LoRa protocol, is depicted in Fig. 4.

i. Input Feature Representation

At each simulation interval, four real-time features as Bandwidth Utilization (BW_t), Queue Length (QL_t), Processing Delay (PD_t), Received Signal Strength Indicator ($RSSI_t$) are extracted that describe the operational state of every node. These values are normalized to a unit scale and combined into a feature vector:

$$X_t = [BW_t, QL_t\ PD_t, RSSI_t,] \qquad [1]$$

Each x_t represents the node's behavior at a specific time t.

Received: August 02, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

ii. Forward Temporal Evaluation

The forward operation of the lightweight BRNN analyses how the current node behavior evolves from its previous states. Instead of numerical weights, fixed thresholds are used to evaluate deviations between consecutive feature values. The forward response function is defined as:

$$F_t = f(x_t, x_{t-1}) = \begin{cases} 1, & |x_{t-} \ x_{t-1}| > \theta f, \\ 0, & otherwise \end{cases} \quad [2]$$

where θ_f is a predefined threshold vector for each feature dimension. A large variation indicates abnormal temporal change such as sudden bandwidth rise or sharp drop in RSSI, signaling possible malicious behavior.

iii. Backward Temporal Evaluation

Simultaneously, the backward evaluation examines the impact of upcoming states on the current observation, thereby adding predictive intelligence:

$$B_t = (x_t, x_{t+1}) = \begin{cases} 1, & |x_{t+1} \ - x_t| > \theta b, \\ 0, & otherwise \end{cases} \quad [3]$$

This computation allows the model to interpret early symptoms of an attack pattern by inspecting future traffic variations. Together, the forward and backward evaluations provide a bidirectional temporal context for every node.

iv. Decision Integration

The two directional evaluations are then combined to form a composite decision score:

$$D_t = \alpha F_t + \beta B_t \quad [4]$$

where α and β are influence factors that control the relative weight of historical and predictive observations. The final classification decision is obtained by comparing D_t with a detection threshold δ:

$$y_t = \begin{cases} 1, & if \ D_t \geq \delta \ (Malicious), \\ 0, & if \ D_t < \delta \ (Legitimate) \end{cases} \quad [5]$$

If the output y_t equals 1, the corresponding node identifier is added to the attacker-list and its packets are discarded. Otherwise, the packets are forwarded to the clustering and encryption modules for secure delivery.

v. Adaptive Temporal Reasoning

Although no backpropagation or numerical weight adjustment is performed, the model achieves adaptivity by continuously updating feature values with each simulation step. Newly observed parameters replace previous states:

$$x_{t-1} \leftarrow x_t, \quad x_{t+1} \text{ (predicted)} \leftarrow \text{next measured state.}$$

This maintains a dynamic rolling window of temporal context, enabling online adjustment of decisions according to real-time network fluctuations.

Received: August 02, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

vi. Operational Flow for Intrusion Detection

The operational flow of the BRNN-based intrusion detection can be represented as:

$$x_{t-1},\ x_t,\ x_{t+1} \rightarrow (F_t,\ B_t) \rightarrow D_t \rightarrow y_t \rightarrow \text{Decision (Drop / Forward)}.$$

Through this process, the model correlates past, present, and future feature patterns to detect anomalies such as Denial-of-Service (DoS), injection, or jamming attacks in real time. This implementation ensures high detection accuracy while remaining computationally efficient for IoT devices with limited processing capability.

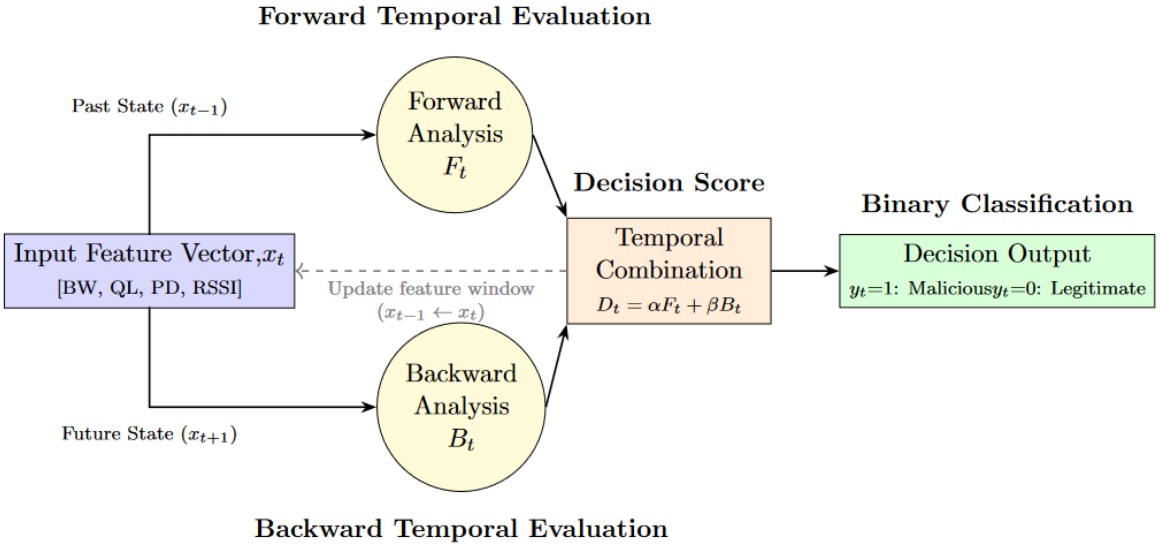


Fig. 4: Lightweight BRNN implemented in the MDLBA-LoRa.

2. Clustering and Adaptive Detection

In addition to enhancing detection precision, the procedure includes clustering as shown in Fig.5 for bundling patterned data. The output of the clustering is used to implement packet prioritization essential data are delivered first, thus maintaining network stability even when under attack. The combination of lightweight fuzzy logic, BRNN, and clustering converts the Attack Detection Layer into a multi-tier adaptive security mechanism. It automatically adapts to changing threats, reduces misclassification, and isolates compromised nodes in a timely manner. The layer offers comprehensive protection against DoS, Jamming, Injection, MiM, and Zero-day attacks, ensuring operation under practical IoT deployment conditions.

i. Clustering and Prioritization Layer

The proposed system utilizes threshold-based clustering mechanism that categorizes packets into high- and normal-priority groups based on processing delay, queue length, and BRNN legitimacy output as shown in Fig.5. Instead

Received: August 02, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

of computationally intensive K-means iterations or centroid updates, the implementation applies simple rule-based thresholds to determine packet criticality, ensuring constant-time operation suitable for low-power LoRa nodes. High-priority packets will be immediately encrypted and forwarded to minimize delay, while normal packets will be buffered and transmitted in the next duty-cycle window, in order to reduce congestion and energy usage.

Let each incoming packet be represented by a feature vector

$$x_i = [d_i, q_i, s_i] \quad [6]$$

$$G(X_i) = \begin{cases} 1, & if\ d_i \geq \theta_d\ or\ q_i\ \geq \theta_q, \\ 0, & otherwise \end{cases} \quad [7]$$

Where, G (x_i)= 1 indicates high-priority group, G (x_i)= 0 indicates normal-priority group and θ_d, θ_q are predefined thresholds. Thus, grouping becomes a deterministic classification problem driven by operational limits rather than iterative clustering. High-priority packets: $x_i \in C_1 \iff G(x_i) = 1$ and Normal-priority packets: $x_i \in C_2 \iff G(x_i) = 0$ .The final forwarding decision ensures that high-priority packets are encrypted and transmitted immediately, while normal-priority packets are buffered and only encrypted at their scheduled dispatch time before being forwarded.

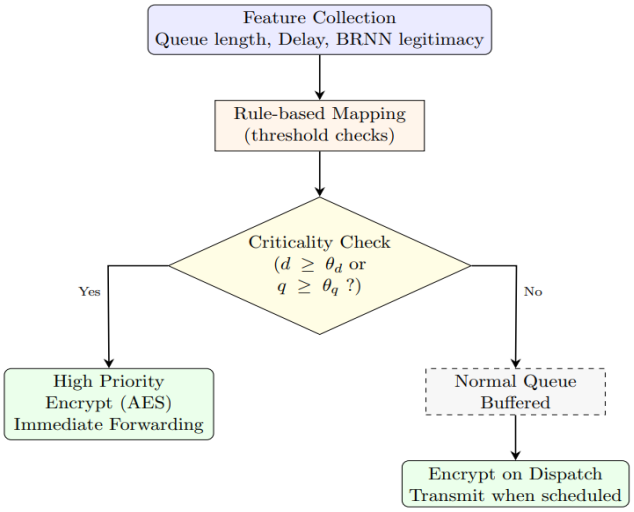


Fig. 5: Process flow of clustering, encryption, and transmission in the MDLBA–LoRa protocol.

The process flow encompassing clustering, encryption, and transmission phases within the proposed MDLBA–LoRa protocol is illustrated in Fig. 5.This simplified design meets the practical objective of clustering-distinguishing traffic based on urgency-while avoiding the computational burden of full clustering algorithms. This approach is realistic for IoT

Received: August 02, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

constraints and achieves the performance benefits of a priority-aware traffic separation without exceeding the processing limitations of LoRa devices.

3. Secure Transmission and Encryption Layer

Once the packets are classified and prioritized through clustering, the final stage of the proposed system ensures secure transmission of legitimate data. This layer integrates a lightweight symmetric encryption mechanism with adaptive scheduling to guarantee both data confidentiality and network efficiency. The approach is designed to complement the preceding fuzzy and BRNN layers, which detect and filter malicious traffic, ensuring that only verified packets enter the secure transmission path.

i. AES-Based Encryption Process

Each authenticated node in the LoRa WAN network maintains a locally stored symmetric key that is generated during initialization and used for all subsequent encryptions. When a valid packet reaches the transmission layer, its payload is encrypted using the Advanced Encryption Standard (AES), a block cipher well suited for constrained IoT devices due to its balance between cryptographic strength and computational efficiency. AES transforms the plaintext payload P into ciphertext C as:

$$C = E_K(P),$$

where $E_K(\cdot)$ denotes the encryption operation with symmetric key K. Decryption at the receiver end applies the inverse function:

$$P = D_K(C).$$

This symmetric encryption ensures confidentiality without the computational overhead of public-key algorithms such as ECC, which, although stronger for dynamic key generation, are less suitable for lightweight LoRa nodes operating under strict energy and memory constraints.

In the implemented system, AES encryption is applied differently depending on the packet's priority. Packets identified as critical are encrypted immediately after clustering, whereas packets classified as normal are buffered and encrypted just before their scheduled transmission. This design ensures that every packet leaving a node is encrypted, while still giving preference to urgent data without increasing overall delay.

ii. Priority-Aware Secure Transmission

The routing and scheduling layer integrates the results of clustering and encryption readiness to decide when and how each packet should be transmitted. Let x_i represent a packet, and C_1 and C_2 be the high and normal priority clusters respectively. The priority-based encryption and transmission operation can be represented as:

$$T(X_i) = \begin{cases} E_K(xi) & xi \ \epsilon \ C1 \\ Q_{(Xi)\rightarrow} E_{K(Xi),,} & xi \in C2 \end{cases} \quad [8]$$

Received: August 02, 2025

International Journal of Applied Mathematics

Volume 38 No. 11s 2025,

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

where $Q(x_i)$ represents buffering and scheduling in the routing queue. This formulation highlights how high-priority packets are immediately encrypted and forwarded, while normal packets undergo AES encryption later in the transmission cycle. Such priority-driven encryption ensures that time-sensitive data are not delayed, whereas routine data are transmitted securely with optimized resource usage.

The use of symmetric encryption also simplifies the transmission process, avoiding time-consuming key exchanges or negotiation steps, which can otherwise increase latency and computation overhead in large-scale IoT networks. By embedding encryption within the packet-handling routine of the LoRa routing agent, the system guarantees that no packet can bypass the security layer, even in the presence of compromised intermediary nodes.

The use of static symmetric keys instead of complex key-exchange procedures is also justified in this context. Real-world LoRa WAN end devices commonly rely on pre-shared keys for joining and data session establishment, making the implemented approach both realistic and computationally efficient. This design choice supports secure data transmission while maintaining minimal energy overhead, an essential factor for IoT nodes expected to operate for years on limited battery power.

IV. Simulation Environment

For a fair comparison, the proposed MDLBA-LoRa protocol is contrasted with the re-implementation and simulation of the baseline methods DLBA (Deep Learning based algorithm) [1] and RLLoRa (Reinforcement Learning algorithm for LoRa) [2] in the same NS-2 environment as shown in Fig.6. In addition, DLBA-LoRa (Dynamic Learning Based Algorithm for LoRa), representing our prior work [3], has been simulated under the same conditions to assess the incremental enhancement brought about by the proposed model. Identical simulation setups are maintained for all works, including node density, topology, traffic generation, and identical attack scenarios (DDoS, zero day, MiTM, and injection). LoRa physical and MAC parameters are kept constant to avoid configuration bias. The NS-2 trace outputs for each referenced baseline [1], [2] and our previous work [3] have been processed using AWK scripts to compute throughput, delay, packet delivery ratio, and energy consumption. This establishes DLBA [1], RLLoRa [2], and our prior DLBA-LoRa [3] as good benchmarks for proving the achieved performance enhancement using the proposed MDLBA-LoRa.

The choice to simulate LoRa WAN in NS-2 rather than using raw analytical models allows the system to incorporate realistic propagation delays, packet collisions, and channel contention that directly affect throughput and reliability. This is crucial because, in real LoRa WAN networks, environmental interfer- ence and gateway placement have significant impacts on performance. By modeling these effects, the proposed architecture produces results that can be generalized to practical scenarios.

While the encryption, clustering, and detection algorithms are embedded at higher layers, their execution adheres to the timing and duty-cycle constraints of the LoRa WAN MAC layer. This ensures that the proposed modifications do not violate regulatory transmission limits or unrealistically inflate node capabilities. The selection of AES encryption, directly mirrors LoRa WAN's own frame security mechanism, making the simulation

Received: August 02, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

cryptographically consistent with commercial LoRa modules.The network topology employed in simulations is depicted in Fig. 6, which was implemented and evaluated using the NS-2 simulator.

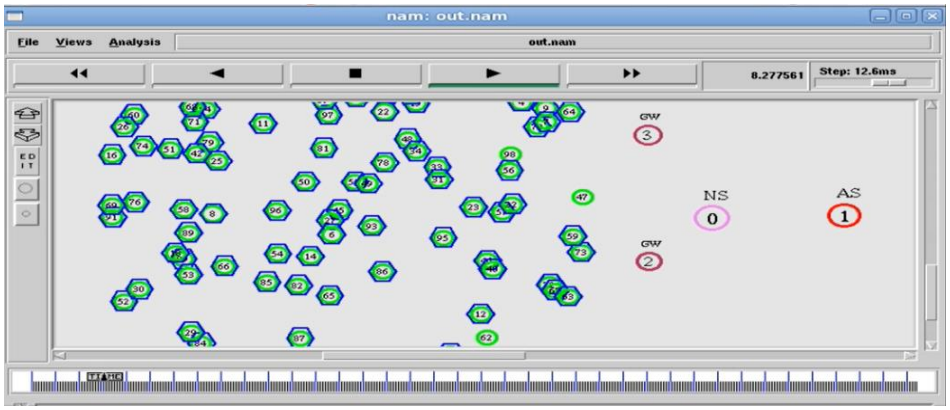
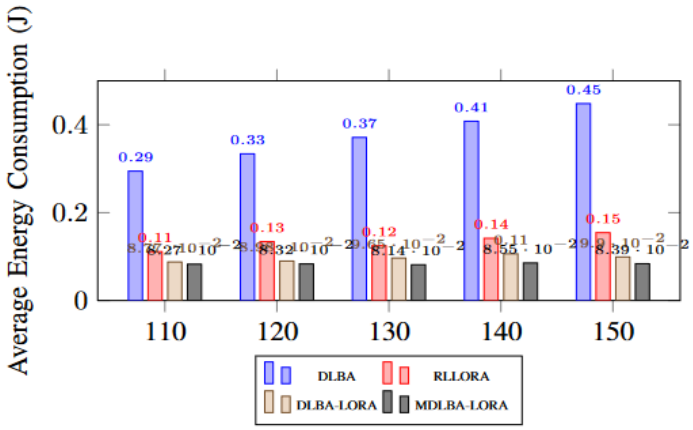


Fig.6. Network simulated in NS2

V. Results & Discussion

The protocols discussed in [1], [2], and [3] collectively represent the existing body of research on learning-driven security enhancement in IoT and LoRaWAN environments. DLBA [1] introduces an early static learning approach that highlights the limitations of non-adaptive routing under adversarial conditions. RLLoRa [2] advances this line of work by incorporating reinforcement-learning–based decision strategies that have been extensively applied for IoT anomaly detection, illustrating how adaptive intelligence can improve resilience. DLBA-LoRa [3], our previous contribution, integrates trust metrics and priority-based gateway reconfiguration, demonstrating the benefits of partial dynamic control in improving network robustness. Together, these studies reflect the evolution of learning-based security mechanisms—from static models to adaptive reinforcement learning and then to trust-aware reconfiguration—and thus form the existing landscape against which the proposed MDLBA-LoRa framework extends the state of the art.



Received: August 02, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

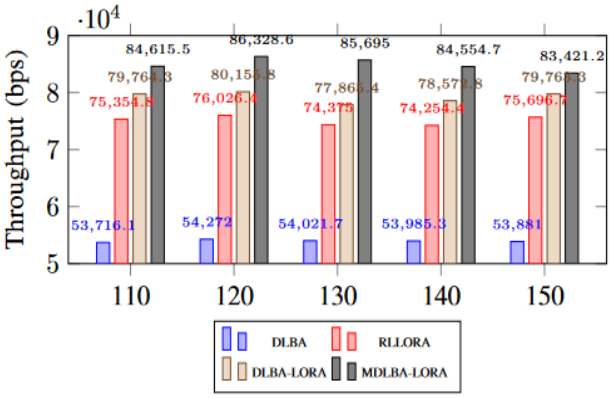


Fig. 7: Average Energy Consumption vs Simulation Time Fig. 8: Throughput vs Simulation Time

Fig. 7 shows the energy consumption results, which indicate that the lowest energy usage around 0.083 J among all four models is achieved by the proposed MDLBA-LoRa. Where DLBA and RLLoRa depict higher consumptions due to static or partially adaptive routing that leads to frequent retransmissions and collisions, DLBA-LoRa reduces some of the overhead through trust-based reconfiguration. In contrast, MDLBA-LoRa minimizes energy consumption by isolating attackers early and preventing repeated forwarding attempts, besides assuring stable routes through fuzzy–BRNN filtering. It maintains its lead as the most energy-efficient protocol despite the addition of extra security layers since it does not have unnecessary packet retries nor congestion or malicious node avoidance.

Throughput performance shown in Fig. 8 further attests to the superiority of MDLBA-LoRa. Combining clustering-based priority transmission, dynamic routing, and early attacker removal, the network sustains a much higher throughput exceeding 84 kbps compared to DLBA, RLLoRa, and DLBA-LoRa. The baseline DLBA suffers from severe throughput degradation under various attacks. RLLoRa enhances performance only in normal conditions. DLBA-LoRa maintains a moderate throughput by making improved decisions at the gateway, yet, it still suffers from packet drops. In contrast, MDLBA-LoRa maintains maximum throughput even during DDoS, and injection attacks.

Similarly, Fig. 9 depicts the packet delivery ratio. The PDR of the proposed protocol is 87.84% the highest among protocols compared here. This stems from the fact that its fuzzy logic, along with the BRNN-inspired temporal deviation evaluator, jointly removes malicious pathways, stabilizes routing, and hence ensures reliable transmission of both priority and normal packets. DLBA and RL LoRa fail when there is an attack due to their static or incomplete decision-making, whereas DLBA-LoRa performs moderately better since it utilizes trust evaluation. However, in MDLBA-LoRa, the combination of detection, clustering, and reconfiguration yields the most resilient PDR performance.

The delay performance highlighted in Fig. 10 illustrates that MDLBA-LoRa achieves the minimum end-to-end delay of 1.28 s despite having multiple intelligent

Received: August 02, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

modules in operation. This counterintuitive advantage is gained because the system reduces retransmissions, removes attack-induced congestion, and selectively forwards critical packets via secure priority queues. The purely topology-driven baseline DLBA reflects maximum delay, while RLLoRa only marginally reduces delay. DLBA-LoRa improves delay based on selective gateway switching; however, MDLBA-LoRa significantly outperforms all the baselines by utilizing dynamically optimized and attack-free routes.

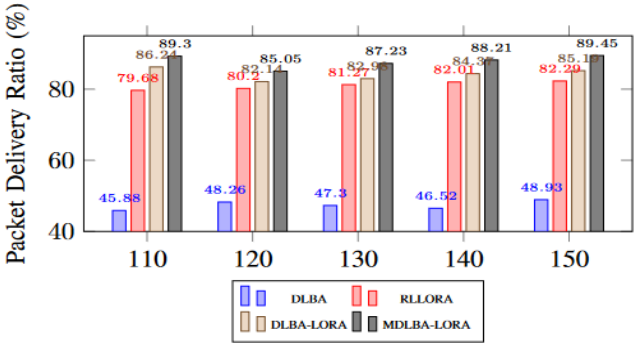


Fig. 9: Packet Delivery Ratio vs Simulation Time

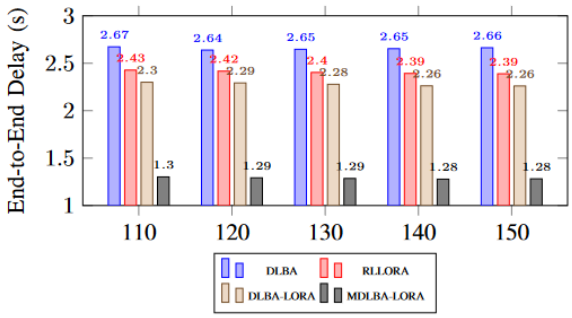


Fig. 10: End-to-End Delay vs Simulation Time

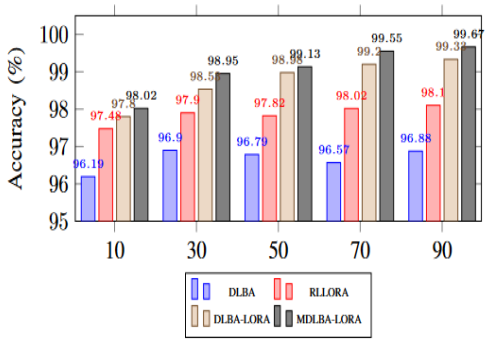


Figure 11: Accuracy vs Window Size

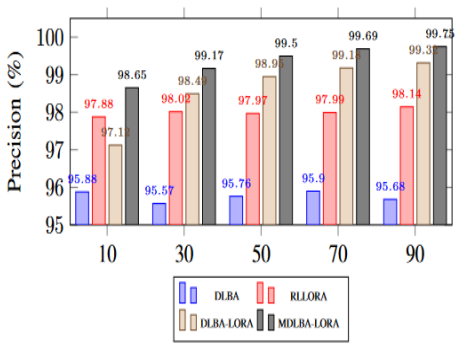


Figure 12: Precision vs Window Size

Received: August 02, 2025

International Journal of Applied Mathematics
Volume 38 No. 11s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

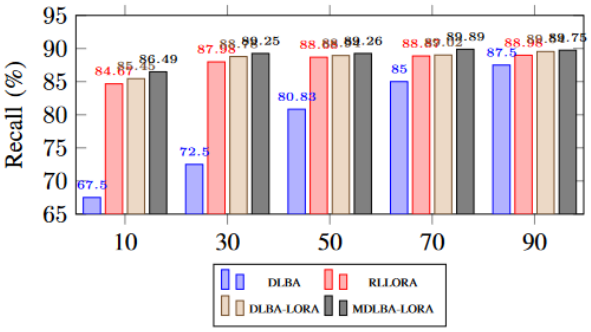


Figure 13: Recall vs Window Size

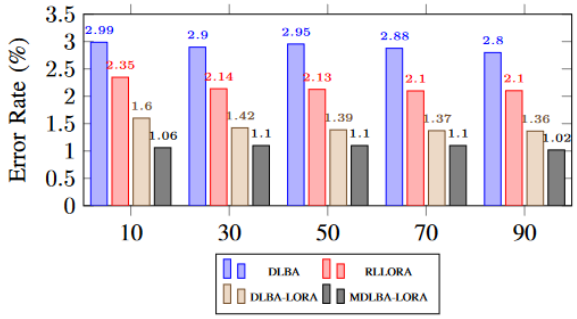


Figure 14: Error Rate vs Window Size

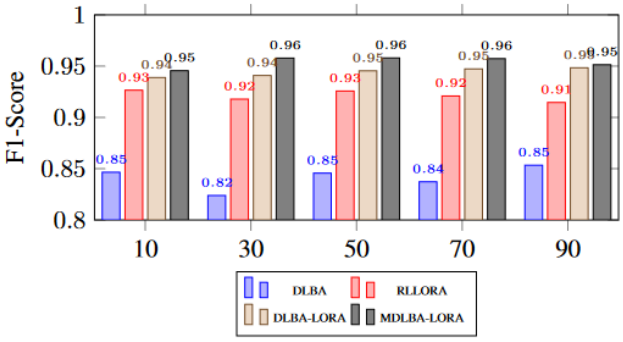


Figure 15: F1-Score vs Window Size

Accuracy results given in Fig. 11 outline that MDLBA-LoRa reaches near-perfect accuracy of 99.06% since the fuzzy engine captures the abnormal pattern of RSSI, packet delay, and queuing, while the BRNN verifies the temporal attack signatures. The precision is also high, close to 99.35% as depicted in Fig. 12, which proves that few normal packets are misclassified as malicious. This is further supported by strong recall values above 88.9% depicted in Fig. 13, which confirms that the majority of the attacks, including DDoS, MiTM, and zero-day variants, are detected with good timeliness. The low error rate close to 1% depicted in Fig. 14 further supports the reliability of the detection mechanism under different sizes of windows. Finally, the

Received: August 02, 2025

Volume 38 No. 11s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

F1-score around 0.95 shown in Fig. 15 shows a balanced precision and recall, which further justifies that MDLBA-LoRa performs consistently with no bias to false positives or false negatives. In summary, the results confirm that the MDLBA-LoRa outperforms DLBA, RLLoRa, and DLBA-LoRa in all performance metrics. Due to the integration of lightweight fuzzy logic, BRNN-based IDS, clustering priorities, AES encryption, and dynamic reconfiguration, it guarantees an effective and lightweight security solution for real-world LoRa WAN deployments, with higher throughput and lower delay, reduced energy consumption, and highly accurate attack detection.

However, these improvements come at the price of a minor increase in computational overhead and memory usage since nodes perform additional fuzzy inference, clustering, and BRNN-based decision layers. This minimal increase in processing time is acceptable considering the resilience, energy efficiency, and security improvements obtained. Altogether, MDLBA-LoRa shows that node-level light intelligence can significantly strengthen LoRa WAN networks without compromising their low-power operational objectives.

VI. Conclusion

The results highlighted that MDLBA-LoRa not only provides superior security but also optimizes resource utilization, making it an effective solution for modern IoT deployments. The protocol outperforms existing IDS approaches by integrating lightweight fuzzy logic and a BRNN-inspired anomaly evaluator for adaptive node-level intrusion detection in LoRaWAN networks. Unlike conventional methods, MDLBA-LoRa incorporates priority-based packet handling, AES-enabled secure forwarding, and dynamic reconfiguration through trust updates, attacker isolation, queue reordering, and adaptive routing. Together, these mechanisms enable energy-efficient, low-latency, and secure communication, presenting a practical and deployable security framework for IoT applications.

References

[1] X. Yuan, C. Li, X. Li, *DeepDefense: Identifying DDoS attack via deep learning*, IEEE International Conference on Communications (ICC), Paris (2017).

[2] P. Kamble, A. Gawade, *Digitalization of healthcare with IoT and cryptographic encryption against DoS attacks*, International Conference on Contemporary Computing and Informatics (IC3I), (2019) 69–73.

[3] N. S. Hunnargi, A. D. Jadhav, *Comprehensive approach to IoT network security: Integrating machine learning and LoRaWAN for enhanced attack detection*, Indian Journal of Technical Education, 48(S1) (2025) 269–275.

[4] G. R. Mode, P. Calyam, K. A. Hoque, *False data injection attacks in Internet of Things and deep learning enabled predictive analytics*, (2019).

Received: August 02, 2025

Volume 38 No. 11s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[5] M. Roopak, S. Parkinson, G. Y. Tian, Y. Ran, S. Khan, B. Chandrasekaran, *An unsupervised approach for detection of zero-day DDoS attacks in IoT networks*, IET Research Journals (2015).

[6] E. Christensson, *Man-in-the-middle attacks on software defined networks*, (2023).

[7] M. A. Khatun, S. F. Memon, C. Eising, L. L. Dhirani, *Machine learning for healthcare-IoT security: A review and risk mitigation*, IEEE (2023).

[8] M. Z. Khan, O. H. Alhazmi, M. A. Javed, H. Ghandorh, K. S. Aloufi, *Reliable Internet of Things: Challenges and future trends*, (2021).

[9] K. V. Sharma, C. Sarada, M. Vasavi, K. Ambika, *Securing IoT devices from DDoS attacks through blockchain and multi-code trust framework*, (2024).

[10] M. Hamidouche, E. Popko, B. Ouni, *Enhancing IoT security via automatic network traffic analysis: The transition from machine learning to deep learning*, (2023).

[11] S. SakthiMurugan, A. S. Kumaar, V. Vignesh, P. Santhi, *Assessment of zero-day vulnerability using machine learning approach*, EAI Endorsed Transactions (2024).

[12] B. I. Hairab, H. K. Aslan, M. S. Elsayed, A. D. Jurcut, M. A. Azer, *Anomaly detection of zero-day attacks based on CNN and regularization techniques*, (2023).

[13] S. T. Arzo, C. Naiga, F. Granelli, R. Bassoli, M. Devetsikiotis, F. H. P. Fitzek, *A theoretical discussion and survey of network automation for IoT: Challenges and opportunities*, IEEE (2021).

[14] J. P. S. Sundaram, W. Du, Z. Zhao, *A survey on LoRa networking: Research problems, current solutions and open issues*, (2019).

[15] M. Schrotter, A. Niemann, B. Schnor, *A comparison of neural-network-based intrusion detection against signature-based detection in IoT networks*, (2024).

[16] P. Xiao, Y. Yan, J. Hu, Z. Zhang, *HMMED: A multimodal model with separate head and payload processing for malicious encrypted traffic detection*, Security and Communication Networks (2024).

[17] R. Gurbani, *IoT: Ongoing challenges and opportunities in mobile technology*, International Journal of Electrical, Electronics and Computers, 6(3) (2021).

[18] A. Kumar, *Internet of Things (IoT): Challenges and future directions*, International Journal of Advanced Research and Development, 3(2) (2018).

[19] M. N. B. C. Kamarudin, A. B. Ayob, A. B. Husain, S. Ansari, M. G. M. Abdolrasol, M. H. B. M. Saad, *Review of LoRaWAN: Performance, key issues, and future perspectives*, (2024).

[20] P. Shama, N. Bansal, *Internet of Things: Application and challenges*, Journal of Critical Reviews (2021).

[21] D. C. Ngyen, M. Ding, P. N. Pathirana, A. Seneviratne, J. Li, H. V. Poor, *Federated learning for Internet of Things: A comprehensive survey*, IEEE Communications Surveys & Tutorials (2021).

Received: August 02, 2025

Volume 38 No. 11s 2025,
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[22] C. Wheelus, X. Zhu, *IoT network security: Threats, risks, and a data-driven defense framework*, (2020).

[23] S. Sarkar, *Communication security challenges of IoT*, International Journal of Novel Research and Development, 8(9) (2023).

[24] S. Sharan, P. Bansal, S. Kumar, *Security concerns and major challenges in IoT: A review*, Journal of Data Science and Cyber Security, 1(1) (2023).

[25] F. Kuntke, L. Baumgartner, C. Reuter, *Rural communication in outage scenarios: Disruption-tolerant networking via LoRaWAN setups*, (2023).

[26] A. Srhir, T. Mazri, M. Benbrahim, *Security in the IoT: State-of-the-art, issues, solutions, and challenges*, International Journal of Advanced Computer Science and Applications, 14(5) (2023).

[27] M. Alipio, M. Bures, *Current testing and performance evaluation methodologies of LoRa and LoRaWAN in IoT applications: Classification, issues, and future directives*, (2023).

[28] B. Liertz, J. Andre, L. Seidlitz, *LoRaWAN – Current state, challenges, and chances*, (2024).

Received: August 02, 2025