International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(11s) 2026 pp. 306-326
https://doi.org/10.70917/ijcisim-2026-3755
Article

Linear Projective Statistical Regressive Mamba Deep Learning for Multifactor Node Authentication in WSN

A. Saravanan[1], S. Sampath[2]

[1]Department of Computer Science, P K R Arts College For Women, Gobichettipalayam, Tamilnadu, India.
Email: **asnpcemca@gmail.com**
[2] Department of Computer Science, P K R Arts College for Women, Gobichettipalayam, Tamilnadu, India.

Abstract: A Wireless Sensor Network (WSN) is a network consists of numerous small electronic devices called sensor nodes that are distributed within the environments to collect, monitor, and transmit data wirelessly. These sensors transmit the collected data to a central system or sink nodes for analysis. As the data is transmitted over an insecure channel, they are vulnerable to a variety of attacks, and hence the network security plays an important part in the WSN. Thus, a secure authentication protocol is necessary to avoid security issues within WSNs. Moreover, the authentication process validates and identifies devices before transmitting the data. In this paper, a novel Linear Projective Statistical Regressive Mamba Deep Learning (LiPSR-MDL) model is developed for efficient node authentication to perform secure data environmental data transmission in WSN. In Mamba Deep Learning architecture, number of sensor nodes is collected as an input. After that, multiple characteristics of sensor nodes such as residual energy, trust level, cooperative score is calculated in convolutional layer. Followed by, Mamba architecture utilizes the Structured State Space Sequence (SSM) model to effectively analyze the multifactor characteristics of the sensor nodes by using statistical kitchen sink regressive analysis. Based on the regression analysis, normal and malicious sensor nodes are authenticated using sigmoid activation function. The output layers display the node authentication results in an accurate manner. Finally, secure environmental data transmission is carried out between the normal sensor nodes and sink nodes. Experimental analysis is carried out with metrics authentication accuracy, authentication time, energy efficiency, transmission success ratio, data drop rate and jitter with respect to different number of environmental data packets and sensor nodes. The overall simulation analyses illustrate that the proposed LiPSR-MDL model improves the authentication accuracy, transmission success ratio, energy efficiency, and minimizes the data drop rate and jitter when compared to conventional methods.
Keywords: WSN, Environmental data transmission, sensor node authentication, Mamba Deep Learning, Structured State Space Sequence (SSM) model, statistical kitchen sink regressive analysis, sigmoid activation function

1. Introduction

An automated wireless sensor network (WSN) consists of massive numbers of autonomous and resource-constrained sensor nodes working in dynamic environments. WSN have been organized in various applications such as healthcare, military, transportation and home automation to gather data and transfer it to remote sensor nodes for further processing. Due to open communication channels, data transmissions are vulnerable to different threats. Therefore, various resource-constrained lightweight authentications schemes have been developed to address these challenges. Lightweight cryptographic key agreement mutual authentication protocol (LCKAMAP) was introduced in [1] for secure data transmission by using Deep gradient descent multi-layer Marquardt vector algorithm. The designed model increases the attack detection accuracy and minimizing the latency. However, the technique did not address trust -aware data transmission to minimize data loss rate. A novel trust based system called Minimum Rank with Hysteresis Objective Function Routing Protocol Low Power and Non-Local (MRHOF-RPL) framework was introduced in [2] with the aim of detecting and classifying malware within the network. The framework reduces the packet loss but the performance of delay reduction remains major issues.

Trusted Energy-Aware Hierarchical Routing (TEAHR) approach was developed in [3] for enhancing the security level. However, the delay aware secure routing remained major issues.

Dual Level Node Authentication Model was developed in [4] depends on node behavior analysis for accurate intrusion detection. However, it failed to incorporate lightweight methods to train distributed model for accurate authentication depending on trust and mobility-aware dynamic sensor environments. Secure Machine learning- based Adaptive Reliable Trust (SMART) model was developed in [5] for accurate prediction of misbehavior nodes. The designed SMART model provides enhanced security and accuracy. However, more advanced machine learning algorithms were not employed for time anomaly detection and trust assessment to enhance the robustness and reliability. A Lightweight MobileNet and Gated Recurrent Unit (GRU) model were developed in [6] to improve the security of network model with low computational demands. However, security and efficiency were challenging task. A novel Deep Learning-Enhanced Hybrid Trust (DLEHT) model was developed in [7] to enhance the packet delivery by minimizing the packet drop. However, DLEHT model failed to focus on improving the energy efficiency of the network.

Energy aware and secure routing (EASR) method was developed in [8] to select secure optimal CH and trust based routing by resisting the routing attacks for establishing trustworthy. However, machine learning techniques were not developed to analyze comprehensive trust value. Energy-Efficient Elliptic Diffie Clustering Technique (3EDCT) method was introduced in [9] to balance security robustness with minimal energy usage. But the model did not minimize the communication delays and energy overhead. A new trust entropy model approach was developed in [10] using machine learning to significantly enhance the network security. The approach achieves high detection accuracy, but delay-aware transmission remains a challenging issue.

Trusted Head Node for Node Behavior Analysis for Malicious Node Detection (THN-NBA-MND) framework was developed in [11] based on node behavior analysis and improve the data transmission. However, the system did not integrate the advanced deep learning methods to improve the performance of malicious node detection. An innovative Elliptic Curve Cryptography and Triple-Layer Authentication Framework (ECC-TLAF) was developed in [12] to enhances the security of while improving energy efficiency and reducing latency. However, the framework failed to improve the scalability of threat detection. Centralized Energy Efficient Clustering Routing Protocol was introduced in [13] to find an optimal path for multi-hop communication. However, the protocol did not consider the trust factors for secure data communication. An AI-driven security system was developed in [14] based on dynamic Trust Management System to increase the security and reliability. However, the trust computation model was not optimized to large-scale and heterogeneous environment. Provably secure two-factor authentication protocol was developed in [15] to enhance security and also improves authentication efficiency. However, the protocol was not efficient to enhance data security.

1.1 Key contribution of the paper

The main aim of this paper is to propose a LiPSR-MDL model for node authentication to enhance secure data transmission in WSN. The major contribution of the LiPSR-MDL model is summarized as follows,

- A novel LiPSR-MDL model is developed to improve the node authentication for ensuring the secure data transmission in WSN.
- To increase the authentication accuracy, LiPSR-MDL model utilizes the **M**amba **D**eep **L**earning architecture for categorizing the sensor nodes as normal or intruders based on residual energy, trust and cooperative score with statistical kitchen sink regressive analysis
- To improve the transmission success ratio in WSN, LiPSR-MDL model utilizes the normal sensor nodes for transmitting the data packets from source to sink node. This process reduces data loss caused by misbehaving nodes during transmission.
- Finally, a extensive simulation is carried out to assess the performance of LiPSR-MDL model and other works.

1.2 Organization of the paper:

The remainder of this paper is organized into six sections. Section 2 presents a review of the related literature. Section 3 describes the proposed LiPSR-MDL model and its architectural structure. Section 4 details the simulation setup and analyzes the results. Section 5 compares the proposed LiPSR-MDL model with existing methods using various performance metrics. Finally, Section 6 summarizes the key findings and concludes the paper.

2. Related works

Secure two-factor authentication scheme was introduced in [16] to provide forward secrecy, and improve the efficiency and security. However, computation overhead, communication overhead, and energy consumption performance evaluation remained unaddressed. Lightweight Trust Management based on Bayesian and Entropy (LTMBE) model was developed in [17] for detecting and mitigating malicious sensor nodes. But a novel trust

evaluation framework was not employed to minimize the data loss. Two-factor authentication (2FA) approach was introduced in [18] for secure communication between users and sensor nodes. However, approach failed to enhance the scalability and compatibility. A trust -aware Software Defined Wireless Sensor Network (SDWSN) framework was introduced in [19] to optimize the energy, delay, trust, while simultaneously ensuring confidentiality. However, mobility-aware trust models and AI-driven predictive optimization were not employed for secure and energy-efficient data transmission. Server–Client Machine Learning Intrusion Detection System (SC-MLIDS) was developed in [20] aimed to enhance security. However, the system failed to optimize energy consumption for evolving security threats.

An opportunistic sensor-based authentication method was introduced in [21] for achieving high identification accuracy. However, it failed to focus on exploring the trade-offs between the cost, power consumption, and security. A novel authentication technique was designed in [22] for achieving an effective and secure data communication. However it failed to focus on developing better security and data communication while maintaining high-performance and security. A Randomized Bi-Phase Authentication Scheme (RBAS) was introduced in [23] to strengthen both external and internal network security and energy efficiency. However, the computational overhead was not minimized. Light Weight authentication protocol was designed in [24] to ensure the security. However, the designed authentication protocol did not lead to an improvement in the successful transmission rate. Lightweight authentication protocols were developed in [25] for minimizing the computation, communication and storage complexities. However, the trust based authentication was not employed to minimize the packet loss.

A strong Two- Factor authentication (2FA) technique was designed in [26] for susceptibility of different types of attacks. However, the technique was not considered the strong security features against potential threats. An Improved Type-2 Fuzzy Logic System (IT2FLS) was introduced in [27] for secure and energy-efficient routing with minimal power consumption. However, failed minimize the network complexity and security threats. Four-factor authentication protocol was developed in [28] to improve the security level of data communications. However, the efficient method was not employed to attain a strong performance rate. Multi-Level Trust Based Secure Routing (MLTSR-BC) method was designed in [29] to analyze the trust and select the secure route. However, method did not make improvement in network security for making secure environments. Machine learning (ML) algorithms were developed in [30] for accurate intrusion detection with higher accuracy and minimal time consumption. However, deep learning models were not employed to further improve the accuracy of the model.

3. Proposal methodology

Wireless Sensor Networks (WSNs) consist of small tiny sensor nodes that are distinguished by limited energy, memory, transmission range, communication and processing power. These sensors are employed to determine environmental physical conditions in fields such as the industry, health, environment, military, commerce, transportation and home automation. The sensor nodes often distributed in open environments, they are susceptible to a variety of security threats such as unauthorized access. Therefore, sensor node authentication plays a vital role in ensuring that only genuine sensor nodes contribute in the network data transmission. Therefore, an effective machine learning or deep learning node authentication technique are essential for securing WSN and enabling secure and reliable data transmission. To address these challenges in WSN, a novel deep learning model based node authentication called LiPSR-MDL is employed in this paper for secure and reliable data transmission.

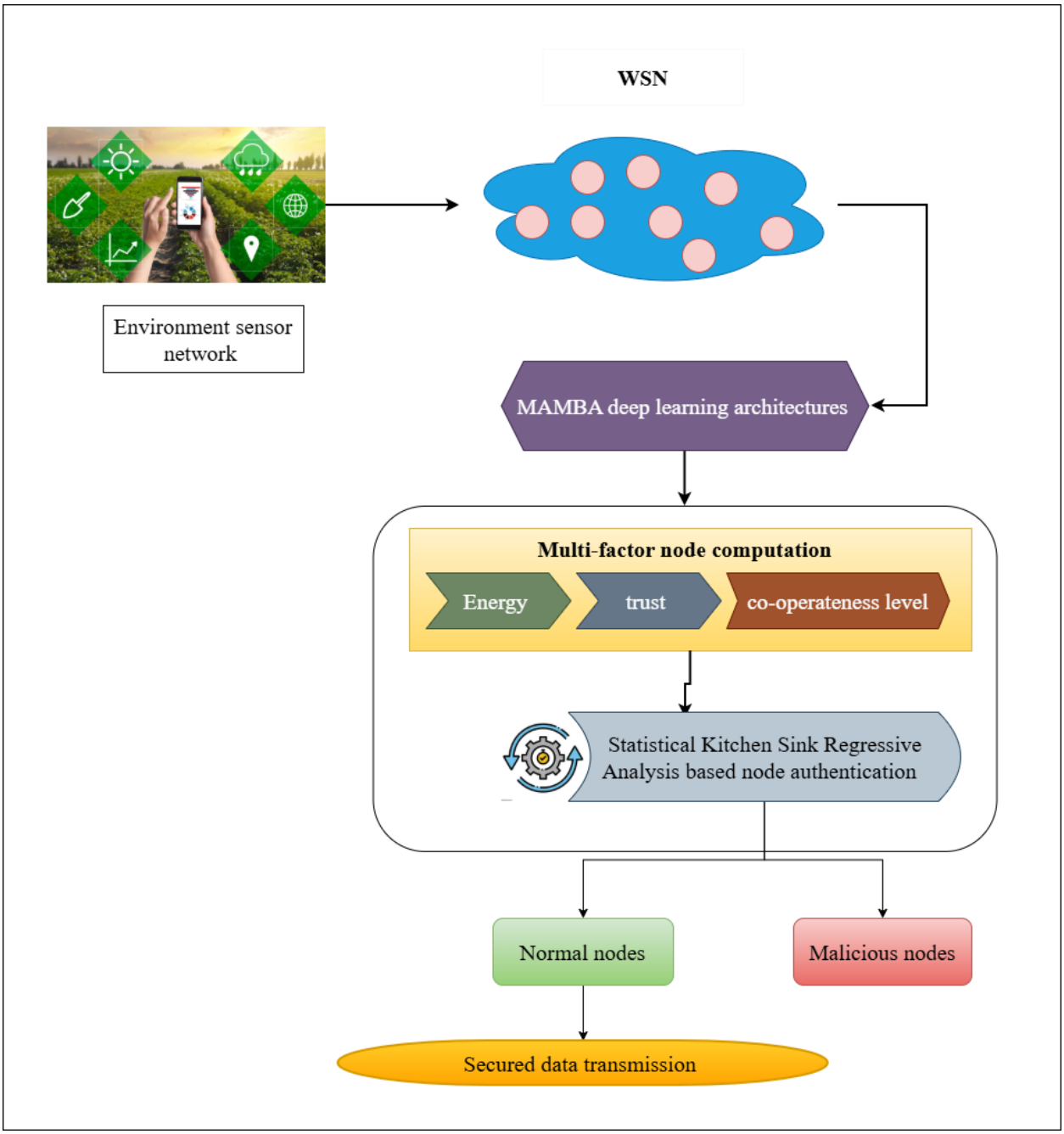

Figure 1 Architecture of proposed LiPSR-MDL

Figure 1 illustrates the architecture of the proposed LiPSR-MDL model planed to facilitate node authentication for secure data communication in WSNs. The proposed model utilizes the Mamba advanced deep learning architecture specifically designed for node authentication in WSN. In the initial stage, the Mamba advanced deep learning architecture computes the multiple factors of the sensor nodes that possess sufficient residual energy, trust and cooperativeness level Followed by, Statistical Kitchen Sink Regressive Analysis in Mamba is employed to analyzes the multifactor's of the sensor nodes and distinguishes into two classes namely normal or malicious or unauthorized . With the normal sensor nodes, secure data transmission is performed to achieve high data delivery and minimal delay in WSN. The detailed process of proposed LiPSR-MDL model with various stages is explained in the subsequent sections.

3.1 Network model

The considered network model is a Wireless Sensor Network (WSN) designed specifically for environmental analysis and monitoring applications. This model consists of a large number of low-power, energy-constrained sensor

nodes $SN_1, SN_2, SN_3 \ldots, SN_n$ that are spatially distributed over a geographical area to continuously monitor various environmental parameters such as Temperature, humidity, CO, liquid petroleum gas (LPG), smoke, light, and motion.

The proposed network model in a WSN is developed for secure environmental data transmission applications. In this network, a large number of low-power and energy-limited sensor nodes, represented as $SN_1, SN_2, SN_3 \ldots, SN_n$ are deployed across a specific geographical region. These sensor nodes collaboratively aggregating the environmental parameters may include temperature, humidity, carbon monoxide (CO), liquid petroleum gas (LPG), smoke, light intensity, and motion and so on. The collected data is then aggregated and transmitted to a remote base station for further processing, analysis, and monitoring. Before the data transmission, node authentication is an important security mechanism used to verify the identity of sensor nodes. It ensures that only legitimate and authorized nodes $SN_{authorized}$ can join the network and transmit data. By validating each node, the network is to prevent malicious $SN_{unauthorized}$ from disrupting communication. Node authentication process helps to maintain node authenticity based on numerous factors namely residual Energy (EN_{res} (SN_i)), trust ($TR\,(SN)$ and cooperativeness level (CO_s).

3.2 Enhanced Mamba Deep Learning

Mamba is a deep learning architecture for reliable secure data transmission through the sensor node authentication. Mamba is an advanced deep learning architecture specifically designed for effective sensor node authentication. On the contrary to traditional deep learning approaches, Mamba enhances efficiency and modeling performance, particularly when dealing with long sequential data. It also offers faster data processing and reduced memory consumption and better scalability compared to other deep learning models. As a result, the proposed LiPSR-MDL model incorporates the Mamba deep learning model for secure data transmission.

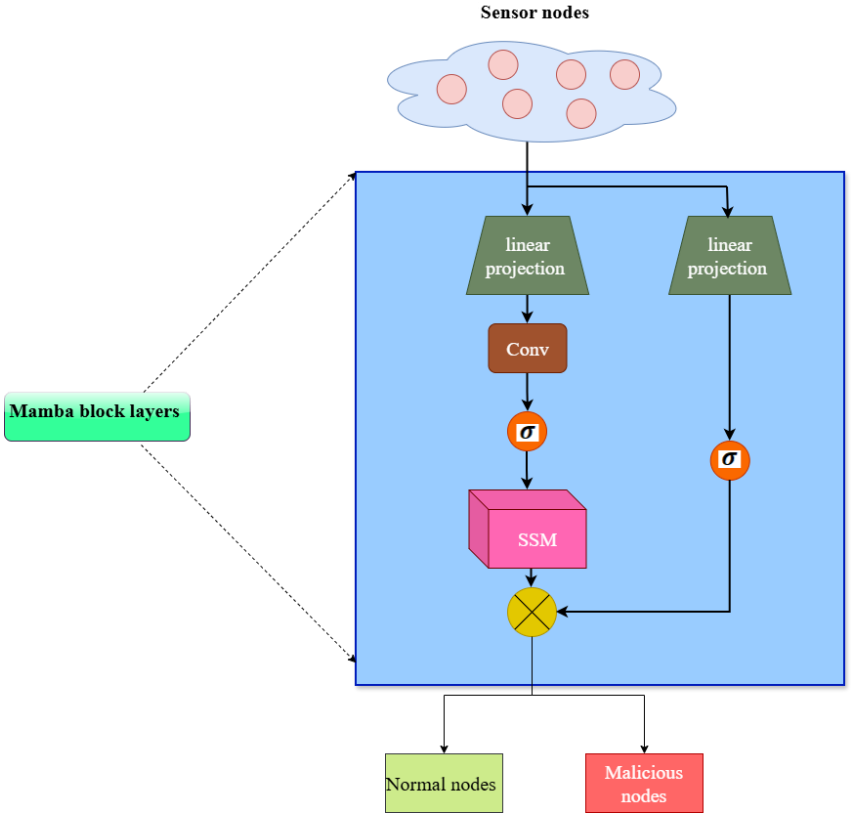

Figure 2 structure of MAMBA deep learning

Figure 2 demonstrates a structure of the MAMBA deep learning model used to obtain an accurate node authentication in WSN. The MAMBA deep learning architecture received the input as $\{X, Y\}$ where 'X' denotes a number of sensor nodes $SN_1, SN_2, SN_3 \ldots, SN_n$' and '$Y$ 'indicates the output of sensor node classification. First, the input is given to linear projection layer to project into a higher-dimensional space using a linear transformation. After that, the convolutional layer is employed for to extract the features of sensor nodes in the given input. As shown in figure 2, σ act as a gate mechanism that controls the flow of information through the Mamba block from one layer to another layer. After computing the node characteristics, the results are fed into a State Space Model (SSM), which acts as a dynamic decision mechanism. This model helps to estimate each input characteristics of sensor nodes based

on the regression results and selectively retains authorized sensor nodes while discarding unauthorized or malicious ones.

3.2.1 Linear projection layer

The sensor nodes are first given to linear projection of the Mamba architecture. It is a linear transformation of input, mathematically calculated by multiplying it with a weight matrix and bias. It efficiently projects input data from its original vector space into a high dimensional space. The linear projection of the input is represented as follows,

$$P_i = \sum_{i=1}^{n} (SN_i * \beta_i) + b \quad (1)$$

Where,P_i represents a linear projected output, β_i represents projection weight matrix allocated to input sensor nodes 'SN_i', b denotes a bias term. The projected output is given to a convolutional layer.

3.2.2 convolutional layer

In this convolutional layer, depthwise convolution process is employed for depthwise convolution to capture local patterns (i.e. characteristics) of the sensor nodes. In that layer, different characteristics of the sensor nodes are analyzed such as residual energy, trust and cooperativeness level.

In the beginning process, the entire sensor nodes have equivalent initial energy. But, it achieves sensing and observing operations, their energy levels decline over time. The total energy consumption of sensor nodes is computed as follows,

$$EN_T(SN_i) = EN_{Tr}(SN_i) + EN_{Rc}(SN_i) \quad (2)$$

Where, $EN_T(SN_i)$ represents a total energy of the i^{th} sensor node, $EN_{Tr}(SN_i)$ indicates an energy consumed during transmission of a data, $EN_{Rc}(SN_i)$ indicates an energy consumed during reception of a data. The term residual energy typically specifies the remaining energy in a sensor node after it performing the data communication, and processing.

$$EN_{res}(SN_i) = EN_T(SN_i) - EN_C(SN_i) \quad (3)$$

Where, $EN_{res}(SN_i)$ designates the residual energy of i^{th} sensor node,$EN_T(SN_i)$ symbolizes total energy of i^{th} sensor node, $EN_C(SN_i)$ designates energy consumed by the i^{th} sensor node.

Subsequently, the next behavior is a node trust to enhance the security, reliability, and for successful data communication within WSN. A lightweight trust assessment method is applied to measures the direct trust and indirect trust for detecting the sensor nodes as trusted or untrusted.

The direct trust value of a node is measured as the ratio of successful data transmissions to the total number of transmissions, which consist of both successful and failed attempts. This metric returns the reliability and trust level of the sensor node. The mathematical illustration of the direct trust value is expressed as follows,

$$TR(SN) = \left[\frac{Success_{DPT}}{Success_{DPT}+Unsuccess_{DT}}\right] \quad (4)$$

Where, $TR(SN)$ represents a trust of sensor nodes,$Success_{DPT}$ indicates a successful data transmission, $Unsuccess_{DT}$ represents an unsuccessful data transmission. Based on calculated trust value, the direct trust and indirect trust is mathematically calculated as follows.

$$DRT(SN) = N_c * \sum (w_1 * TR(SN)) \quad (5)$$

$$IRT(SN) = \sum (w_2 * DRT(SN)) \quad (6)$$

$$TTR(SN) = (w_3 * DRT(SN)) + (w_4 * IRT(SN)) \quad (7)$$

Where, $DRT(SN)$ represents a direct trust of the sensor node, $DRT(SN)$ indicates a indirect trust of the sensor node, N_c indicates a confidence or normalization factor that balances the overall trust value, w_1, w_2, w_3 and w_4 represents a weight allocated to each interaction, $TTR(SN)$ indicates a total trust rate of the sensor nodes.

The cooperativeness of a sensor node refers to its ability to actively connect in network operations such as forwarding data, maintaining routing processes, and distributing network resources with other nodes. On the contrary, malicious or attacker nodes normally avoid contributing in these cooperative behavior, which interrupt efficient communication within the network. Therefore, the cooperativeness of sensor nodes is measured by analyzing the communication or links created between nodes during a specific time interval.

The communication links among sensor nodes are identified through the sharing of two types of beacon messages. These beacon messages comprise a request (r_{eq}) message and a route reply (r_{ep}) message, which are distributed between neighboring sensor nodes. Initially, the sensor node SN_i transmits a request beacon message '(r_{eq})' to its neighboring nodes to begin and detect feasible communication links.

$$SN_i \; r_{eq} \Rightarrow \; SN_j \; (8)$$

Where, the sensor node SN_i transmits route request (r_{eq}) beacon message to other sensor nodes SN_j within the network. The node SN_j send back to the reply message 'r_{ep} 'back to the node SN_i .

$$SN_j \quad r_{ep} \Rightarrow \; SN_i \; (9)$$

Where, node SN_j transmits a reply message $r_{ep}$to the sensor node SN_i. For each sensor node, the cooperative score values is calculated depends on the received requests and responses.

$$CO_s = \left[\frac{r_{ep}\,(R)}{r_{eq}\,(S)}\right] \quad (10)$$

Where, CO_sdenotes a cooperative score of the each sensor node based on ratio of response received $r_{ep}\;(R)$ from its neighboring node and requests sends$r_{eq}\;(S)$. A cooperativeness value approaching 1 indicates that the sensor node reveals a high level of cooperation. This implies that the nodes consistently responds to requests from neighboring nodes, dynamically supports data forwarding, and efficiently contribute in network operations. Such nodes are regarded as trustworthy and are generally chosen for energy-efficient secure data transmission in WSN. The estimated characteristics of the sensor nodes are transferred to the SSM model through the gate mechanism.

3.2.3 SSM model

The Selective State Space Model (SSM) is the key part of the Mamba architecture, designed to efficiently analyze and maintain important information with linear complexity. On the contrary to traditional models, the SSM maintains a hidden state that changes over time, capturing relevant information efficiently. The State Space Model (SSM) acts as a dynamic decision mechanism that evaluates each input feature's relevance based on the Statistical Kitchen Sink Regressive Analysis and selectively analyzes the important features while discarding malicious users. This process helps improve model accuracy.

The block diagram of SSM model receives the input i.e. node features characteristics at time 't' and it transferred into the state evolution block called 'latent state' or hidden state. In this state, long-range relationship is measured between the sensor nodes and characteristics using structured and efficient linear operators and kitchen sink regression. The kitchen sink regression for forecasting the normal or abnormal sensor node has the following linear structure as follows,

$$z = \alpha + \sum_{i=1}^{n} \quad \gamma_i \; f(SN_i) + \varepsilon \quad (11)$$

Where, z denotes a regression outcomes, α represents constant parameters, γ denotes a regression coefficient, $f(SN_i)$ denotes a features or characteristics of sensor nodes such as energy, trust and cooperativeness level, ε represents the error term.

$$L\,(t) = p.z(t) + q.X(t) \quad (12)$$

Where, term $L(t)$ represents a latent state, factor p and q denotes evaluation parameters, $X(t)$ denotes input sensor nodes, $z(t)$ denotes a regression analysis of the node characteristics. In the projection state, the normal sensor nodes are retained.

$$M(t) = r.L(t) \; (13)$$

Where, $M(t)$ indicates an output of the SSM model, r denotes a projection parameter of the model, $L(t)$ denotes a latent state output. In this state, projection parameter finds and distinguishes the sensor nodes as normal or malicious are selected for secure data transmission. Therefore, the output of after the SSM is expressed as follows,

$$H = SSM \; \left(\sigma\big(Conv\,(P_1(SN_i))\big)\right) \; (14)$$

Where, H denotes a output after the SSM model, σ denotes a gate function, $Conv$ denotes a convolution layer output, $P_1(SN_i)$ denotes a one linear projection of sensor nodes. The output of the other linear projection is expressed as follows,

$$G = \sigma(P_2(SN_i)) \quad (15)$$

Where, G denotes an output second linear projection of sensor nodes '$P_2(SN_i$'), σ represents the gate function. Finally, the output of MAMBA is observed as follows,

$$Y = H \otimes G \quad (16)$$

Where, Y denotes an output of MAMBA which is the element-wise multiplication between the SSM output 'H' and the linear-projection gate 'G'. Finally, the sigmoid activation function is employed to distinguish the normal or malicious nodes.

$$F = \frac{1}{1+e^{-Y}} \quad (17)$$

Where, F denotes a sigmoid activation function which provides the output from 0 to 1.

$$F = \{1 \; ; \quad Normal\ nodes \quad 0 \; ; \quad malicious\ nodes \quad (18)$$

From the above equation, activation function 'F' provides the output ranges from 0 to 1. where '1' indicates the normal sensor nodes are and '0' indicates malicious nodes. With the normal sensor nodes, secure data packet transmission is attained in WSN. The algorithm of linear projective statistical regressive MAMBA deep learning is given below.

// **Algorithm 1: Linear Projective Statistical Regressive MAMBA deep Learning**
Input: Input: **Number of** sensor nodes '$SN_1, SN_2, SN_3, \ldots, SN_n$, Environmental data packets $DP_1, DP_2, DP_3, \ldots DP_n$ **Output:** Secure data transmission
Begin **Step 1: Collect** sensor nodes '$SN_1, SN_2, SN_3, \ldots, SN_n$ **Step 2: For each** sensor node SN_i **Step 3:** Perform linear projection using (6) **Step 4: End for** **Step 5: For each** sensor node SN_i **Step 6:** **Measure** residual energy using (3) **Step 7:** **Compute the** total trust using (7) **Step 8:** **Compute the** cooperative score using (10) **Step 9:** **End for** **Step 10:** **Project the higher** node with their characteristics in SSM **Step 11:** **Measure the** long-range relationship using regression function using (11) **Step 12:** **Project t**he SSM output using (13) **Step 13:** Output of first linear projection using (14**)** **Step 14:** Output of second linear projection using (15**)** **Step 15:** Obtain the multiplication output using (16**)** **Step 16:** Obtain final classification results with sigmoid activation function using (17) **Step 17:** $if\ (F = 1)$ **Step 18:** nodes authenticated as 'normal' **Step 19:** **else** **Step 20:** nodes authenticated as 'malicious' **Step 21:** **End if** **Step 22: Return** (normal **sensor nodes**) **Step 23: Perform secure** data packet transmission with normal sensor nodes

End

Algorithm 1 portrays step by step procedure of sensor node authentication using a linear projective statistical regressive MAMBA deep learning. The process begins by considering a set of sensor nodes into the MAMBA deep learning architecture. Following this, linear projection is employed with weights and bias. The projected results are transferred to a one dimensional convolution network. Within this convolution network, the characteristics of sensor nodes such as energy, trust and cooperative score are measured. Based on probability outcomes, SSM model measures the long range relationship of the sensor nodes characteristics based on regression analysis. Finally, combine the two linear projection outputs. Based on combined results, the sensor nodes are accurately classified with the help of sigmoid activation function. Finally, the proposed deep learning architecture distinguishes the normal or malicious sensor nodes within the network. Then the collected environmental data is transmitted to sink node via normal sensor nodes in a secured manner.

4. Simulation setup

In the section, simulation settings of the proposed LiPSR-MDL model existing methods, namely [1] and [2] are implemented in NS3 network simulator. In the simulation setup, a total of 500 sensor nodes are randomly deployed within a square area $1100\,m \times 1100\,m$. This network configuration is aimed to estimate energy efficient environmental data transmission mechanisms under controlled simulation conditions. In order to perform the simulation, Environmental Sensor Telemetry Dataset is used and collected from https://www.kaggle.com/datasets/garystafford/environmental-sensor-data-132k. The Random Waypoint model is implemented to represent node mobility in the simulation. In this scenario, the Dynamic Source Routing (DSR) protocol is employed to enable efficient data transmission within the WSN. The use of DSR helps in reducing routing overhead while enhancing overall network efficiency, particularly in large-scale WSN environments. The simulation is implemented for a total duration of 300 seconds. During this period, the movement rate of the sensor nodes varies between 0 m/s and 20 m/s. The detailed simulation settings are presented in Table 1.

Table 1 Simulation Parameters

Simulation parameter	Value
Simulator	NS3
Number of sensor nodes	50, 100, 150, 200, 250, 300, 350,400,500
Initial energy of node	0.5 Joule
Network area	1100m * 1100m
Simulation time	300s
Mobility model	Random Way Point
Routing protocol	DSR
Sensor nodes speed	0-20m/s
Environmental Data	10000,20000,30000,40000,50000,60000,70000,80000,90000,100000
Number of runs	10

4.1 Simulation implementation results

In this section, the various processes of the LiPSR-MDL model are described in detail with related screenshots. Initially, 50 sensor nodes are randomly deployed in a square region of $1100 * 1100\boldsymbol{m}$ to collect environmental data.

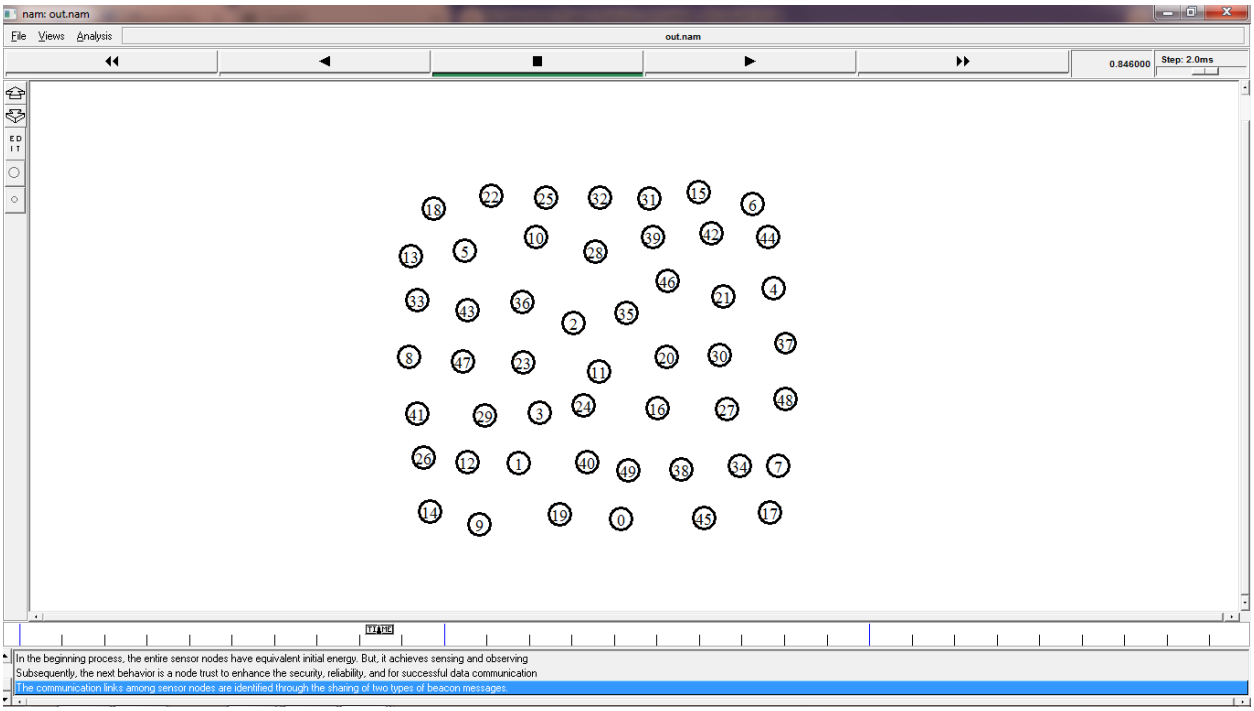

Figure 3 deployments of sensor nodes

Once the sensor nodes are distributed within the network model, each node is labeled with a unique identifier number ranging from 0 to 49. Two special nodes are highlighted with blue hexagons and labeled as Source and Sink as sown in figure 4.

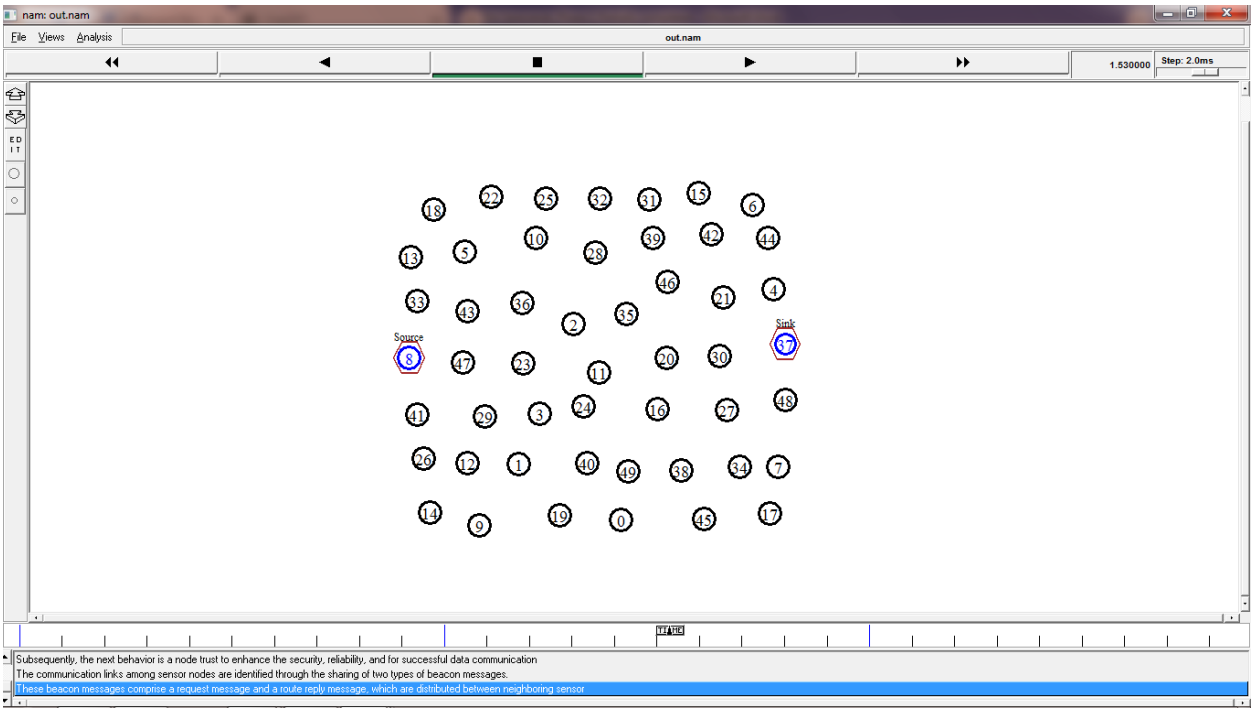

Figure 4 source and destination initialization

After initializing the sensor nodes, multiple security factors such as residual energy (RE), trust level, and cooperative score are calculated to identify normal and malicious nodes through a Mamba Deep Learning, as shown in Figure 5.

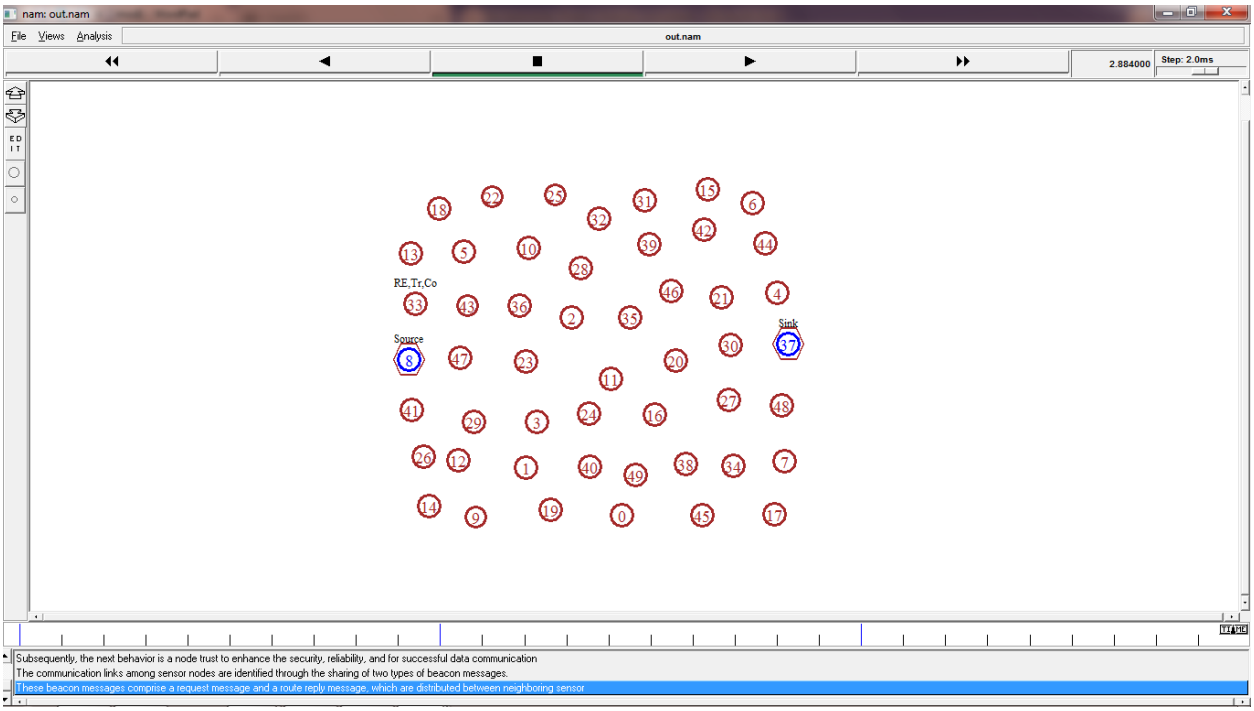

Figure 5 multiple security factors computation

After computing the security parameters of the sensor nodes, Mamba Deep Learning model is employed for classifying the normal and intruder sensor nodes within WSN based on statistical kitchen sink regression analysis.

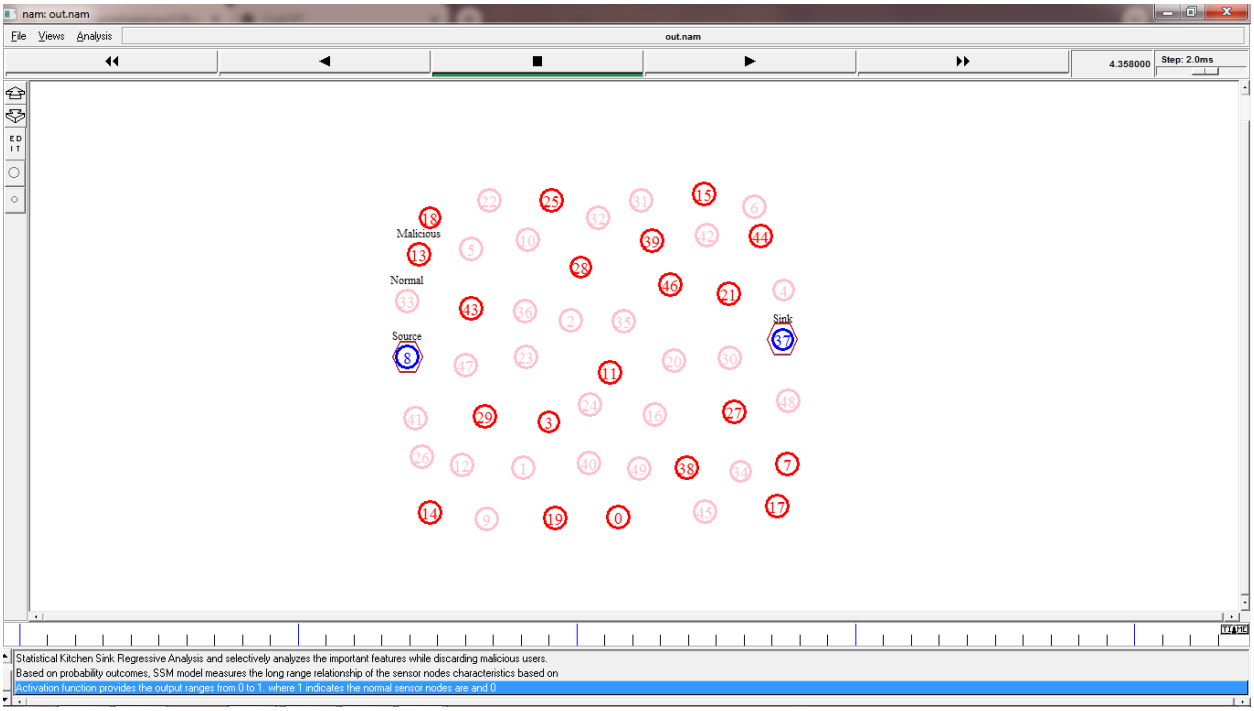

Figure 6 sensor node authentications

This simulation uses color coding to distinguish between malicious and normal nodes. Malicious nodes are shown in red, while normal nodes appear in light pink colored. Sigmoid activation function is applied to classify nodes as normal node and malicious one.

Finally, secure data transmission is performed from the source to sink node via normal sensor nodes as shown in figure 7.

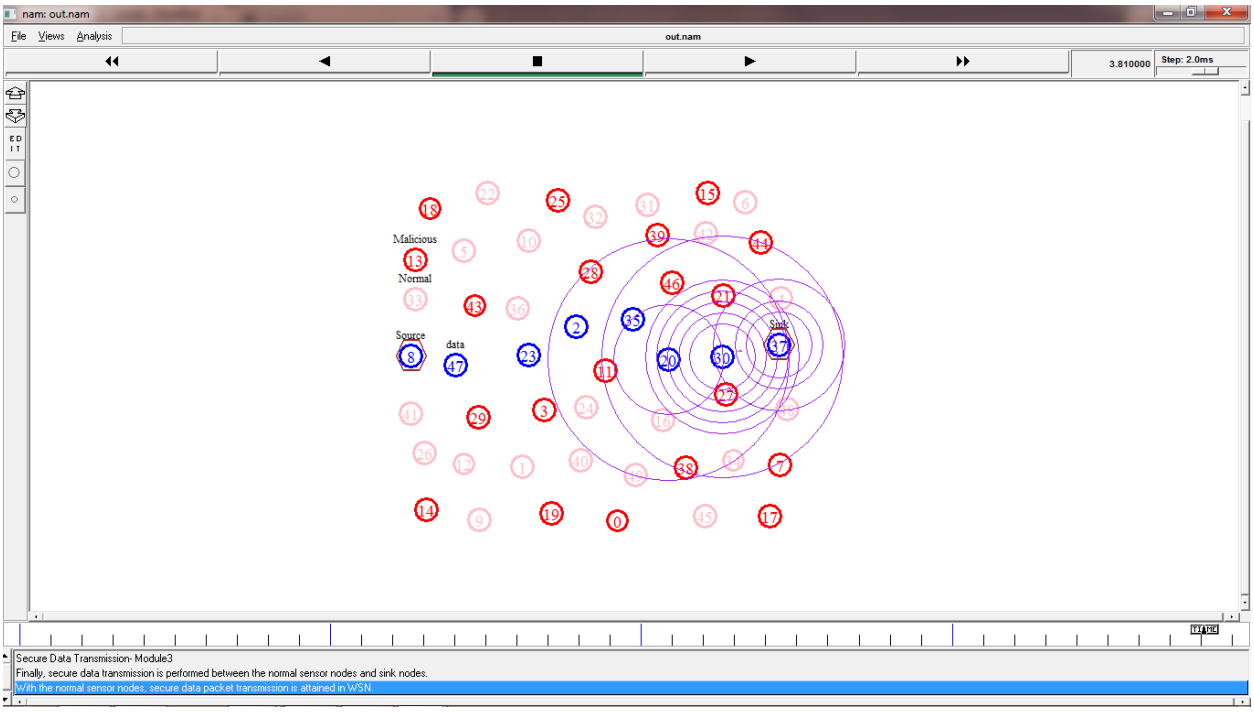

Figure 7 Secure data transmission

5. Performance results and discussions

The performance of the proposed LiPSR-MDL model is assessed through a comparative analysis with existing techniques, LCKAMAP [1] and MRHOF-RPL [2]. The LiPSR-MDL model performance is measured using multiple assessment metrics, including authentication accuracy, authentication time, energy efficiency, transmission success ratio, data drop rate and jitter. The experiments are conducted under different simulation settings by varying the number of sensor nodes as well as the environmental data packets.

5.1 Performance analysis of authentication accuracy

It is defined as the ratio of correctly classified the normal sensor nodes or malicious to the total number of sensor nodes distributed within the network environment. The formula for calculating authentication accuracy is expressed as follows,

$$AUA = \sum_{i=1}^{n} \left(\frac{CISN}{SN_i}\right) * 100 \qquad (19)$$

Where, 'AUA' denotes authentication accuracy, 'SN_i' indicates the number of sensor nodes as input for simulation, $CISN$ denotes a number of sensor nodes correctly identified as normal or malicious. The authentication accuracy is measured in terms of percentage (%).

Table 2 comparative analysis of authentication accuracy

Number of sensor nodes	Authentication accuracy (%)		
	Proposed LiPSR-MDL	Existing LCKAMAP [1]	Existing MRHOF-RPL [2]
50	98	94	92
100	97.36	93.63	92.32
150	97.22	93.25	92.11
200	97.48	93.41	92.45
250	97.27	93.21	91.89

300	97.63	93.05	91.63
350	97.22	94.02	92.34
400	97.41	93.44	91.32
450	97.88	93.12	91.47
500	97.32	93.03	91.22

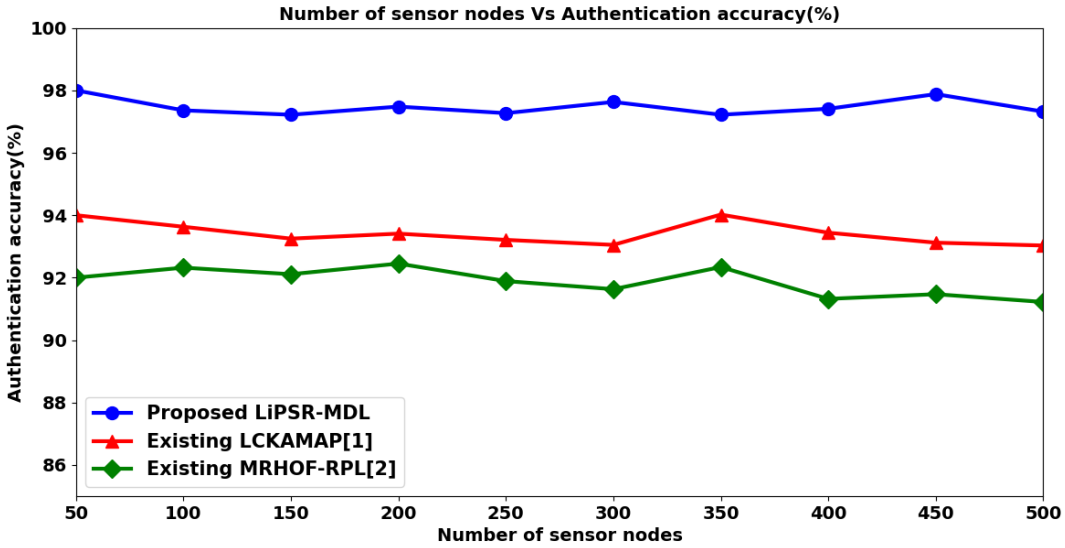

Figure 8 Graphical illustration of authentication accuracy

Figure 8 reveals a graphical evaluation of authentication accuracy using three approaches namely the proposed LiPSR-MDL model against existing approaches, including LiPSR-MDL model with existing techniques, LCKAMAP [1] and MRHOF-RPL [2]. In the figure 8, the horizontal direction represents the number of sensor nodes varied from 50 to 500, while the vertical axis describes the equivalent authentication accuracy. The results noticeably demonstrate that the LiPSR-MDL model consistently achieved better accuracy in sensor node authentication than the existing deep learning methods. For instance, when considering 50 sensor nodes, the LiPSR-MDL model achieves an accuracy of 98%, whereas the authentication accuracies of the existing methods [1] and [2] are 94% and 92%, respectively. This greater performance is attained due to the integration of a Mamba Deep Learning architecture, which increases the model's capability to accurately analyze the sensor node characteristics such as residual energy, trust and cooperativeness level by employing statistical kitchen sink regression analysis. During the analysis, the model utilizes a mamba deep learning model classified the sensor node into normal or malicious nodes with higher accuracy. The average value of ten observed results indicates that the LiPSR-MDL model exhibits an average improvement of 4% and 6% when compared to [1] and [2] respectively.

5.2 Performance analysis of authentication time

It refers to the amount of time consumed by the algorithm to authenticate sensor nodes as normal node or malicious nodes. Therefore, the authentication time is mathematically calculated as follows,

$$AUT = \sum_{i=1}^{n} SN_i * Time\ (SNA) \quad (20)$$

Where, 'AUT' represents the authentication time, 'n' denotes number of nodes, '$Time\ (SNA)$ ' denotes a time taken for sensor node authentication. The authentication time is measured in seconds.

Table 3 comparative analysis of authentication time

Number of sensor nodes	**Authentication time (seconds)**		
	Proposed LiPSR-MDL	**Existing LCKAMAP [1]**	**Existing MRHOF-RPL [2]**

50	22.5	26	30.5
100	24.6	28.5	34.6
150	30.5	35.8	39.4
200	35.4	38.9	42.4
250	38.7	42.5	50.8
300	45.6	50.9	55.9
350	52.8	58.7	63.4
400	55.9	62.6	70.5
450	67.4	74.5	82.4
500	75.6	80.5	88.6

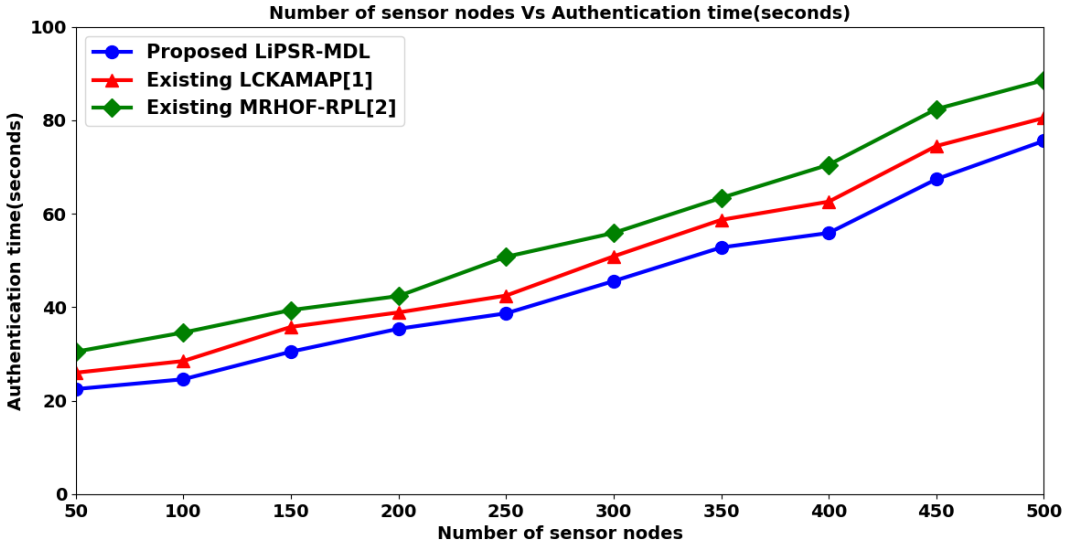

Figure 9 Graphical illustration of authentication time

Figure 9 demonstrates a graphical illustration of authentication time versus number of sensor nodes ranges from 50 to 500. The simulation results expose that authentication time of all three methods gets increased while increasing the number of sensor nodes. However, LiPSR-MDL model constantly reveals an important reduction in authentication time compared to the conventional deep learning approaches [1] and [2]. For example, in the first scenario with 50 sensor nodes, the proposed LiPSR-MDL model records an authentication time of 22.5 seconds, while the existing methods in [1] and [2] show authentication times of 26 seconds and 30.5 seconds, respectively. This improvement is mainly attributed to the integration of the Mamba Deep Learning architecture, which distinguishes the normal sensor nodes based on high residual energy, trust, and cooperativeness level. This process of Mamba Deep Learning system enables faster data aggregation with minimal time. Across increasing sensor node volumes, the LiPSR-MDL model achieves an average authentication time reduction of approximately 11% and 21% compared to the existing LCKAMAP [1] and MRHOF-RPL [2] respectively.

5.3 Performance analysis of energy efficiency

It referred as the ratio of the number of environmental data effectively transmitted to the amount of energy consumed. Therefore, the overall energy efficiency is calculated using the following formula:

$$EE = \frac{EDT\ (KB)}{EC\ (Joule)} \quad (21)$$

Where, EE indicates energy efficiency, $EDT\ (KB)$ indicates an environmental data transmitted, EC denotes an energy consumed by sensor node. It measured in terms of Kilo bytes per joule (KB/J).

Table 4 comparative analysis of energy efficiency

Number of sensor nodes	Energy efficiency (KB/J)		
	Proposed LiPSR-MDL	Existing LCKAMAP [1]	Existing MRHOF-RPL [2]
50	62.5	52.6	50
100	68.72	56.82	53.61
150	72.64	61.45	56.2
200	78.41	65.82	58.43
250	80.2	70.45	60.37
300	83.53	75.56	64.21
350	85.8	78.21	70.35
400	90.24	80.41	74.57
450	93.65	82.62	78.34
500	95.52	85.88	80.78

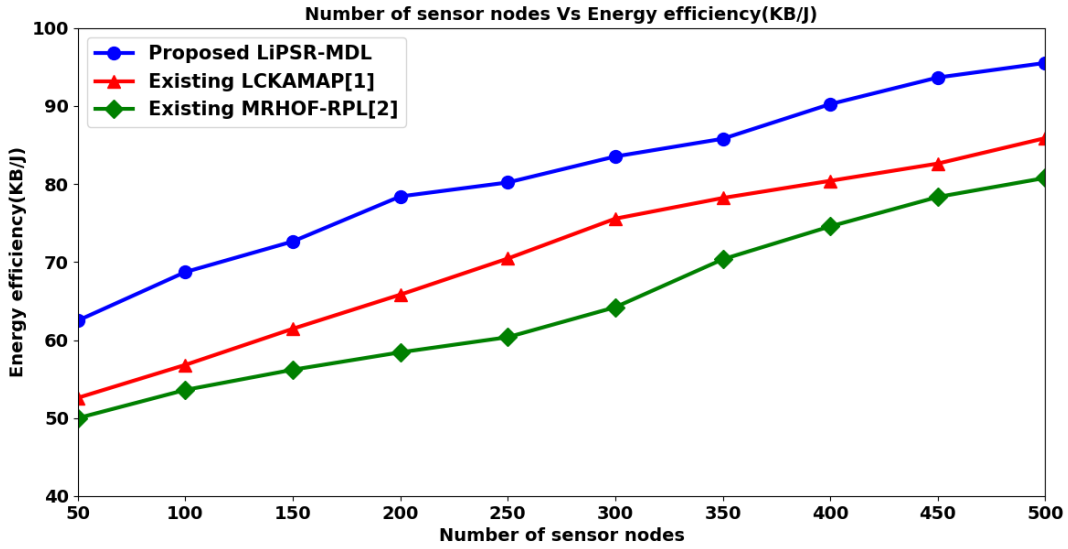

Figure 10 Graphical illustration of energy efficiency

Figure 10 illustrates simulation outcomes of energy efficiency versus the node density ranges from 50 to 500. As revealed in figure 10, horizontal axis represents the node density i.e. number of sensor nodes while the vertical axis indicates the simulation outcomes of energy efficiency. The energy efficiency is measured using thee different methods namely LiPSR-MDL model, existing LCKAMAP [1] and MRHOF-RPL [2] respectively. According to the obtained results, the energy efficiency of all three methods gets increased while increasing input count of the sensor nodes. This is due to sensor nodes consumes lesser energy during the environmental data transmission. Among three methods, the performance of proposed LiPSR-MDL model enhances the energy efficiency. Let us consider 50 sensor nodes to calculate the energy efficiency. By applying the LiPSR-MDL model, energy efficiency is 45.45 KB/J while the energy efficiency of **[1]** and [2] shows the 52.6 KB/J, and 50 KB/J respectively. Similarly, various counts of sensor nodes such as 100, 150 …500 are considered in simulation to compute the energy efficiency. For each method, ten different results were obtained. After observing the results, the performance of the LiPSR-MDL model is compared to that of existing methods. The observed results of LiPSR-MDL model, indicates that energy efficiency is increased by 15% and 26% compared to methods [1] and [2], respectively.

5.4 Performance analysis of transmission success ratio

It is measured as the ratio of environmental data that are effectively received at sink node to the total number of data sent by the sender node. The mathematical expression for this Transmission Success Ratio is given below.

$$TSR = \left(\sum_{j=1}^{m} \frac{SRDP}{DP_j}\right) * 100 \quad (22)$$

Where, TSR indicates a transmission success ratio is measured as a data sent by the source 'DP_j' and the data packets successfully received '$SRDP$'. It is measured in terms of percentage (%).

Table 5 Comparative analysis of transmission success ratio

Number of environmental data	Transmission Success Ratio (%)		
	Proposed LiPSR-MDL	Existing LCKAMAP [1]	Existing MRHOF-RPL [2]
10000	97.65	94.36	93.6
20000	97.22	94.27	93.21
30000	97.63	94.11	93.06
40000	97.89	94.65	93.04
50000	97.36	94.26	93.14
60000	97.12	94.34	93.26
70000	97.52	94.74	93.52
80000	97.55	94.22	93.45
90000	97.63	94.36	93.44
100000	97.59	94.74	93.03

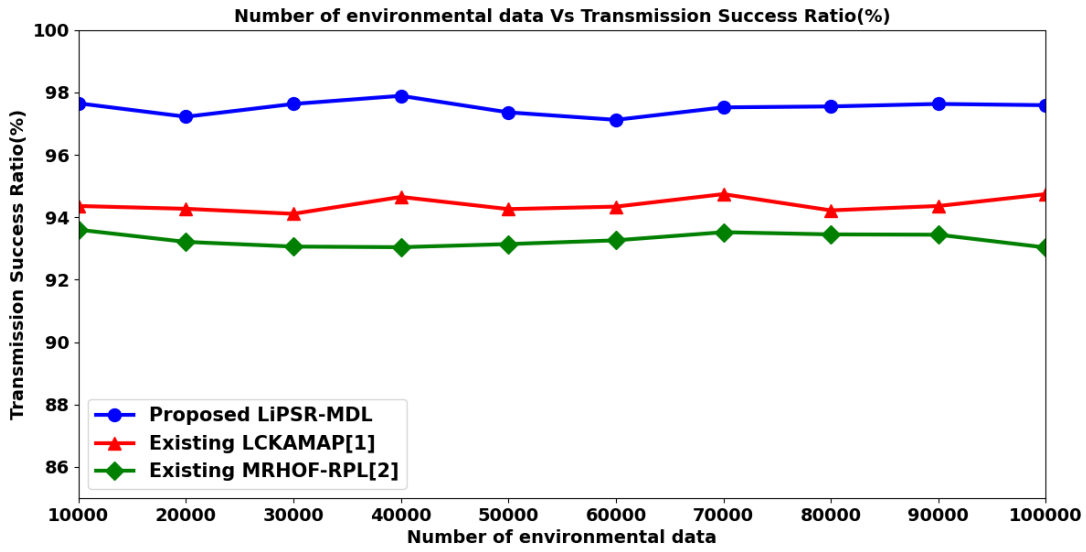

Figure 11 Graphical illustration of transmission success ratio

Figure 11 reports the graphical illustration of transmission success ratio versus number of environmental data samples taken in ranges from 10000 to 100000. The transmission success ratio is measured using three methods namely LiPSR-MDL model, existing LCKAMAP [1] and MRHOF-RPL [2] to evaluate transmission success ratio. The horizontal axis symbolizes the environmental data count, while the vertical axis designates transmission success ratio performance. The simulation findings expose that the LiPSR-MDL model consistently achieved superior

performance than the conventional approaches. For example, with 10000 environmental data from the dataset, the LiPSR-MDL model records a transmission success ratio of 97.65%, outperforming [1] and [2], which achieves transmission success ratio of 94.36% and 93.6%, respectively. This enhanced performance is achieved through the selection of normal sensor nodes based on high residual energy, higher trust level and better cooperative score which maximizes the data transmission at the receiver. Furthermore, the authentication process of the LiPSR-MDL model eliminates malicious nodes, thereby enhancing data delivery. The overall analysis indicates that the LiPSR-MDL model improved transmission success ratio by 3% over [1] and 5% over [2] respectively.

5.5 Performance analysis of data drop rate

This metric is an important indicator used to estimate the reliability of data transmission in a WSN. It measures the proportion of data packets that fail to reach the sink node from the total number of packets sent from the source node. The drop rate is measured as follows,

$$DDR = \sum_{j=1}^{m} \left[\frac{DP\ drop}{DP_j\ sent}\right] * 100 \quad (23)$$

Where, DDR represens a data drop rate, $DP\ drop$ indicates the number of dropped data packets at the sink node and $DP_j\ sent$ indicates a number of data packet sent. Data drop rate is measured in terms of percentage (%).

Table 6 Comparative analysis of data drop rate

Number of environmental data	Data drop rate (%)		
	Proposed LiPSR-MDL	Existing LCKAMAP [1]	Existing MRHOF-RPL [2]
10000	2.35	5.64	6.4
20000	2.78	5.73	6.79
30000	2.37	5.89	6.94
40000	2.11	5.35	6.96
50000	2.64	5.74	6.86
60000	2.88	5.66	6.74
70000	2.48	5.26	6.48
80000	2.45	5.78	6.55
90000	2.37	5.64	6.56
100000	2.41	5.26	6.97

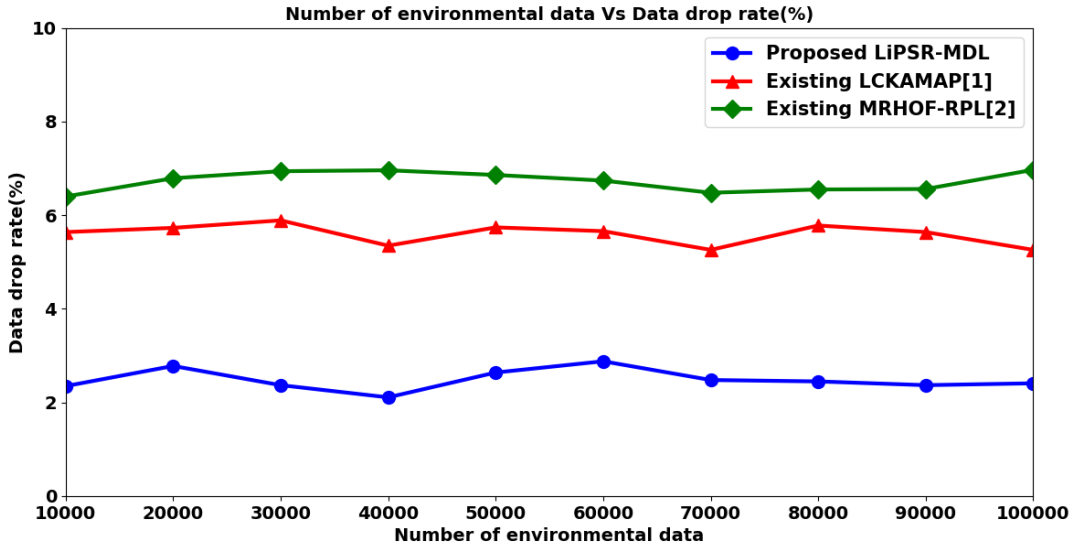

Figure 12 Graphical illustration of data drop rate

Figure 12 presents a graphical depiction of data drop rate using three methods LiPSR-MDL model, as well as two existing methods denoted as LCKAMAP [1] and MRHOF-RPL [2]. The chart portrays the data drop rate is measured based on the environmental data collected from the dataset. The horizontal axis represents the number of data packets, while the vertical axis represents the data drop rate performance. The simulation performs with 10000 environmental data and the results show a data drop rate of 2.35% using LiPSR-MDL model, 5.64% for method [1], and 6.4% for method [2] in data transmission from source to sink node. This reduction is achieved by selecting the normal sensor nodes and avoids the data drop caused by unauthorized nodes. The overall findings reveal that LiPSR-MDL model significantly reduces the drop rate in data transmission by 56% and 63% compared to methods [1] and [2], respectively.

5.6 Performance analysis of Jitter

It refers to the variation in the absolute difference between end-to-end delays of data packet transmission from source to destination. Lesser jitter indicates stable transmission and it lead to high data delivery. This is mathematically formulated as given below.

$$Jitter = \left|delay_j - delay_{j-1}\right| \quad (24)$$

Where, $delay_j$ denotes an end-to-end delay of the current packet 'j', End-to-end delay of the previous packet '$j-1$'. It is measured in terms of milliseconds (ms).

Table 7 Comparative analysis of Jitter

Number of environmental data	Jitter (ms)		
	Proposed LiPSR-MDL	Existing LCKAMAP [1]	Existing MRHOF-RPL [2]
10000	10.8	12.6	14.6
20000	12.5	13.8	15.3
30000	13.8	15.5	17.8
40000	14.7	16.2	18.2
50000	15.9	17.3	19.3
60000	16.4	18.6	20.4
70000	17.1	19.4	22.4

80000	18.3	20.2	23.7
90000	19.5	21.4	24.5
100000	20.2	22.7	25.4

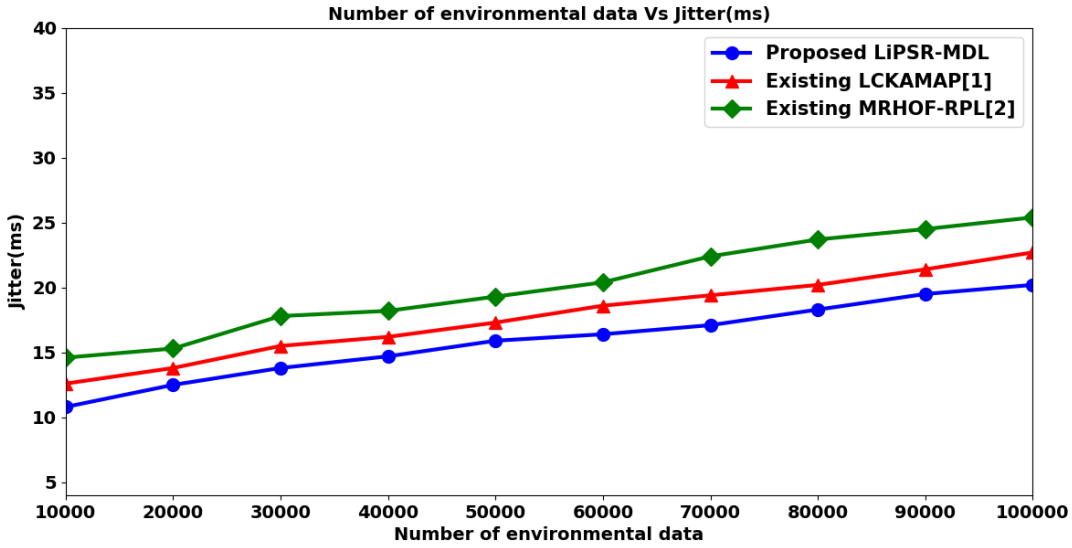

Figure 13 Graphical illustration of Jitter

Figure 13 shows the performance analysis of jitter by means of three methods namely LiPSR-MDL model, existing methods denoted as LCKAMAP [1] and MRHOF-RPL [2]. Simulation for each method is carried out across 10 various run, utilizing 100000 environmental data. The figure demonstrates that as the number of environmental data increases, the jitter for all the methods gets increased gradually for all three methods. However, the LiPSR-MDL model exhibits a considerably smaller performance of jitter compared to both [1] and [2]. For example, the simulation is done with 10000 environmental data, the LiPSR-MDL model observed only 10.8ms, 12.6ms by [1] and 14.6ms by method [2]. The observed improvement is achieved by selecting normal nodes and removes the malicious node for efficient data transmission from source to sink node. In addition, cooperativeness between the sensor nodes continuously transfers the data packets with minimal delay. These steps contribute to a notable reduction in the jitter. Overall, the comparison results highlights that the LiPSR-MDL model reduced the performance of jitter by approximately 11% and 21% when compared to the existing approaches.

6. Conclusion

This article designs an advanced deep learning model called LiPSR-MDL model for secure and energy-optimized data transmission within WSN. The suggested LiPSR-MDL model begins by deploying numerous sensor nodes throughout a sensor network for gathering the environment data. Mamba **D**eep **L**earning architecture is then employed in LiPSR-MDL model to categorize these nodes as either normal or intruders based on factors such as residual energy, trust level, and node cooperativeness. This advanced **d**eep **l**earning strategy enhances the overall authentication performance with high accuracy and minimal time consumption. Moreover, data transmission success ratio is enhanced particularly during communication between the normal sensor nodes and the sink. This ensures minimal data drop throughout the data transfer process.

A complete simulation analysis is conducted using several performance metrics, including authentication accuracy, authentication time, energy efficiency, data transmission success ratio, drop rate and jitter, under varying numbers of data packets and node densities. The results indicate that the LiPSR-MDL model considerably increases the authentication accuracy and data transfer rate while reducing jitter, and data drop rate compared with existing approaches.

References

1. Radha Raman Chandan, Hemalatha Thanganadar, Upendra Dwivedi, Surendra Kumar Shukla, Shreyas Pagare, Navruzbek Shavkatov, “Energy-efficient multi factor authentication protocols in sustainable security for wireless

networks using machine learning algorithm", Results in Engineering, Elsevier, Volume 28, 2025, Pages 1-8. https://doi.org/10.1016/j.rineng.2025.107196
2. Ajay Kumar, Ishan Budhiraja, Deepak Garg, Sahil Garg, Bong Jun Choi, Mubarak Alrashoud, "Advanced network security with an integrated trust-based intrusion detection system for routing protocol", Alexandria Engineering Journal, Elsevier, Volume 120, May 2025, Pages 378-390. https://doi.org/10.1016/j.aej.2025.01.087
3. Vikas, Charu Wahi, Bharat Bhushan Sagar and Manisha Manju, "Trusted Energy-Aware Hierarchical Routing (TEAHR) for Wireless Sensor Networks", Sensors, Volume 25, Issue 8, 2025, Pages 1-36. https://doi.org/10.3390/s25082519
4. Aswadhati. Sirisha & Kurra. Santhi Sri, "Cluster head based dual level node authentication model with node pattern analysis for intrusion detection in wireless sensor networks using machine learning", Discover Computing, Springer, Volume 29, 2026, Pages 1-35. https://doi.org/10.1007/s10791-026-09948-4
5. Prafull Goswami, Tayyab Khan, Vinay Pathak & Abdulatif Alabdultif, "Machine learning based dynamic trust estimation framework for Securing wireless sensor networks", Scientific Reports, volume 15, 2025, Pages 1-19. https://doi.org/10.1038/s41598-025-19768-z
6. Kaumudi Keerthana, A. Mahesh Babu, "A Novel Trust Management and Secure Communication Framework for Wireless Sensor Networks", Engineering Technology & Applied Science Research, volume 15, Issue 2, 2025, Pages 21728–21737. https://doi.org/10.48084/etasr.10009
7. Santosh Anand, Anantha Narayanan V, "Addressing Rogue Nodes and Trust Management: Leveraging Deep Learning-Enhanced Hybrid Trust to Optimize Wireless Sensor Networks Management", Robot Control (JRC), volume 6, Issue 2, 2025, Pages 846–861. https://doi.org/10.18196/jrc.v6i2.25600
8. Venkatesh Prasad B.S, Roopashree H.R, "Energy aware and secure routing for hierarchical cluster through trust evaluation", Measurement: Sensors, Elsevier, Volume 33, 2024, Pages 1-8. https://doi.org/10.1016/j.measen.2024.101132
9. G. Nagarajan , R.I. Minu, Meena Devi R, T. Samraj Lawrence, Sajith P J, M. Viju Prakash, "Eco-conscious multi-factor authentication protocols for energy-aware wireless networks", Results in Engineering, Elsevier, Volume 28, 2025, Pages 1-14. https://doi.org/10.1016/j.rineng.2025.107807
10. S. Kanthimathi, "Exploring Machine Learning Algorithms for Malicious Node Detection Using Cluster-Based Trust Entropy," IEEE Access ,Volume 12, 2024,Pages 137913 – 137925. DOI: 10.1109/ACCESS.2024.3465843
11. Bhanu Priyanka Valluri, Nitin Sharma, "Trusted head node for Node Behaviour Analysis for malicious node detection in wireless sensor networks", Measurement: Sensors, Elsevier, Volume 36, 2024, Pages 1-16. https://doi.org/10.1016/j.measen.2024.101159
12. Meshari D. Alanazi," A triple-layer authentication framework with elliptic curve cryptography for securing IoT-assisted wireless sensor networks", PLoS One, Volume 20, Issue 8, Pages 1-27. https://doi.org/10.1371/journal.pone.0329011
13. Makda Fekadie Tewelgne, Samuel Asferaw Demilew & Dagne Walle Girmaw, "Energy efficient inter-cluster multi-hop communication routing protocol for wireless sensor network based on centralized energy efficient clustering routing protocol, Discover Applied Sciences, Springer, Volume 7, 2025, Pages 1-22. https://doi.org/10.1007/s42452-025-07348-9
14. Shaha Al-Otaibi, Sarra Ayouni, Nadeem Sarwar, Asma Irshad & Faizan Ullah, "AI-driven intrusion detection and lightweight authentication framework for secure and efficient medical sensor networks", Scientific Reports, volume 16, 2026, pages 1-17. https://doi.org/10.1038/s41598-025-31981-4
15. Hao Feng and Bowen Cai, "A Provably Secure and Lightweight Two-Factor Authentication Protocol for Wireless Sensor Network", Electronics, Volume 13, Issue 21, 2024, Pages 1-19. https://doi.org/10.3390/electronics13214289
16. Jiaqing Mo,Zhihua Zhang and Yuhua Lin, "A Practically Secure Two-Factor and Mutual Authentication Protocol for Distributed Wireless Sensor Networks Using PUF", Electronics, Volume 14, Issue 1, 2025, Pages 1-21. https://doi.org/10.3390/electronics14010010
17. Pranav Gangwani, Alexander Perez-Pons and Himanshu Upadhyay, "Evaluating Trust Management Frameworks for Wireless Sensor Networks", Sensors, Volume 24, Issue 9, 2024, Pages 1-26. https://doi.org/10.3390/s24092852
18. K Hima Bindu and T Mounica Reddy," Protocol for Two-factor Authentication in Wireless Sensor Networks", Journal of Innovative Research in Engineering Technology and Management Science, Volume 01, Issue 03, 2025, Pages 18-19. https://creativecommons.org/licenses/by-nc-nd/4.0/
19. Jasmine Alponse, Yaashuwanth C, Prathibanandhi K, "A Novel Scalable Trust-Aware Deep Reinforcement Learning Algorithm for Energy-Efficient and Secure Routing in Software-Defined Wireless Sensor Networks for IoT", Measurement Science Review, Volume 25, Issue 6 ,2025, Pages 358-365. https://doi.org/10.2478/msr-2025-0039
20. Hongwei Zhang, Darshana Upadhyay, Marzia Zaman, Achin Jain, Srinivas Sampalli, "SC-MLIDS: Fusion-based Machine Learning Framework for Intrusion Detection in Wireless Sensor Networks", Ad Hoc Networks, Elsevier, Volume 175, 2025,Pages 1-18. https://doi.org/10.1016/j.adhoc.2025.103871
21. Marc Saideh, Jean-Paul Jamont and Laurent Vercouter, "Opportunistic Sensor-Based Authentication Factors in and for the Internet of Things", Sensors, Volume 24, Issue 14, 2024, Pages 1-12. https://doi.org/10.3390/s24144621
22. Ravi Kumar, Samayveer Singh, Deepti Singh, Mohit Kumar, Sukhpal Singh Gill, "A robust and secure user authentication scheme based on multifactor and multi-gateway in IoT enabled sensor networks", Security and privacy, Wiley, Volume 7, Issue 1, 2024, Pages 1-25. https://doi.org/10.1002/spy2.335
23. Pendukeni Phalaagae, Adamu Murtala Zungeru, Boyce Sigweni, Selvaraj Rajalakshmi, Herbet Batte, Odongo S. Eyobu, "An energy efficient authentication scheme for cluster-based wireless IoT sensor networks", Scientific African, Elsevier, Volume 25, 2024, Pages 1-16. https://doi.org/10.1016/j.sciaf.2024.e02287
24. Suman Sonia, Muzzammil Hussain, "Light Weight Authentication of Devices in Wireless Sensor Network", Procedia Computer Science, Elsevier, Volume 252, 2025, Pages 1005–1013. https://doi.org/10.1016/j.procs.2025.01.061

25. Vincent Omollo Nyangaresi, Ganesh Keshaorao Yenurkar, “Anonymity preserving lightweight authentication protocol for resource-limited wireless sensor networks”, High-Confidence Computing, Elsevier, Volume 4, Issue 2, June 2024, Pages 1-14. https://doi.org/10.1016/j.hcc.2023.100178
26. T. Sudhakar, R. Praveen & V. Natarajan, “An efficient ECC and fuzzy verifier based user authentication protocol for IoT enabled WSNs“, Scientific Reports, volume 15, 2025, Pages 1-16. https://doi.org/10.1038/s41598-025-94550-9
27. S. Ambareesh, Pundalik Chavan, S. Supreeth, Rajesh Nandalike, P. Dayananda & S. Rohith, “A secure and energy-efficient routing using coupled ensemble selection approach and optimal type-2 fuzzy logic in WSN”, Scientific Reports, volume 15, 2025, Pages 1-24. https://doi.org/10.1038/s41598-024-82635-w
28. Albandari Alsumayt, Majid Alshammari, Zeyad M Alfawaer, Fahd N Al-Wesabi, Nahla El-Haggar, Sumayh S Aljameel, Sarah Albassam, Shahad AlGhareeb, Nouf Mohammed Alghamdi, Nawir Aldossary, “Efficient security level in wireless sensor networks (WSNs) using four-factors authentication over the Internet of Things (IoT)”, PeerJ Comput Science, 2024, Pages 1-25. doi: 10.7717/peerj-cs.2091
29. S. Ramachandra, M. Baskar, “Real-time multi-level trust-based secure routing for improved QoS in WSN using blockchain”, Results in Engineering, Elsevier, Volume 26, June 2025, Pages 1-10. https://doi.org/10.1016/j.rineng.2025.104732
30. Nestor X. Arreaga, Rebeca Estrada, Sara Blanc, Andres Noboaa , Nelson Vera, “Security threat detection performance analysis of a distributed architecture WSN”, Procedia Computer Science, Elsevier, Volume 241, 2024, Pages 114-122. https://doi.org/10.1016/j.procs.2024.08.017