International Journal of Industrial Engineering
2026;10(1):1-10.
ISSN: 2456-8449

AI-Driven Self-Learning Network Management for Industrial IoT Wireless Sensor Networks Using Autoencoder and Reinforcement Learning

Suresh Babu Changalasetty[1*], Rahaf Alhwaij[1], Meznah Shaail Albogami[2]

[1]*Department of Computer Science, College of Computer Science, King Khalid University, Abha, Saudi Arabia.*
[2]*Department of Informatics and Computer Systems, College of Computer Science, King Khalid University, Abha, Saudi Arabia.*

[*]*Corresponding author: sbabu@kku.edu.sa*

Abstract. Industrial Wireless Sensor Networks (IWSNs) are essential to Industrial Internet of Things (IIoT) systems because they allow automation, data-driven decision-making, and monitoring in smart industrial settings. However, these networks encounter several challenges such as energy limitations, abnormal node behavior, packet loss, and unpredictable communication links. To discover these problems, this paper introduces an Artificial Intelligence (AI)-driven self-learning network management system that combines Autoencoder-based anomaly detection and Reinforcement Learning (RL)-based routing optimization. The Autoencoder algorithm learns normal network behavior patterns and identifies anomalous sensor nodes based on reconstruction error, allowing early detection of anomalous activities or faults. Using network characteristics like residual energy, link quality, and congestion level, reinforcement learning is used to dynamically choose the best routing path. This hybrid AI approach assists adaptive decision-making and nonstop learning in dynamic industrial environments. Simulation results illustrate that the proposed system enhances anomaly detection accuracy and increases network throughput compared with traditional approaches. This intelligent approach offers a scalable solution for dynamic network management in IIoT environments.

Keywords: Autoencoder, Reinforcement Learning, Industrial Wireless Sensor Networks, AI-driven self-learning, Adaptive decision

INTRODUCTION

The fast growth of IIoT technologies has supported smart factories to adopt large numbers of sensors and linked devices for supervising industrial processes [1]. These devices transmit through IWSNs to gather and forward data from industrial apparatus, sensors, and control systems. Despite their benefits, IWSNs have several drawbacks, including low battery life, communication interference, node failures abnormal behavior initiated by hardware faults or attacks. These issues can defeat network performance and minimize the system consistency. Traditional routing approach's function established on pre-set network conditions and static decision process. While these approaches are operational in simple network scenarios, they effort to adjust to quickly changing network situation in industrial environments [2]. IWSN may issue from packet loss, higher delay, energy consumption, and decreased throughput. As a result, there is a growing need for intelligent network management techniques that can comprehend network dynamics and dynamically modify routing decisions.

Recently, machine learning (ML) [3] and AI approaches [4] have become effective algorithms for tackling these issues in Wireless Sensor Network (WSN). AI-based techniques can automatically optimize routing choices, identify anomalous activities, and evaluate network trends. Specifically, the development of adaptive and self-learning network management systems is made possible by deep learning and reinforcement learning approaches. In this work, an AI-driven self-learning network framework is proposed for IIoT WSNs. To improve network speed and security, the proposed solution combines RL-based adaptive routing optimization with autoencoder-based anomaly detection. To recognize anomalous behaviors like hostile nodes, connection failures, or unusual packet delivery, the autoencoder model learns typical network traffic patterns. Once an anomaly is identified, the system exhibits the anomaly nodes or links and prevents them from contributing to the routing process. An RL agent is used to dynamically identify the best routing pathways depending on current network circumstances to further increase network efficiency. Through constant interaction with the network environment, the RL agent

Received: 09-10-2025 Revised: 15.12.2025 Accepted: 29.12.2025

determines the optimal routing strategy by evaluating a variety of network factors, including residual energy, link quality, and congestion levels. This self-learning approach enables the network to adjust to changing situation and conserve reliable communication even in the presence of anomaly nodes or network failures. The simulation results shows that the proposed system improving throughput, energy efficiency, and anomaly detection accuracy.

RELATED WORKS

This literature survey discusses Machine Learning based routing efficiency and detect anomalies in IWSNs. These are described below. Several studies have applied RL techniques to optimize routing decisions in WSNs. RL algorithms tolerate sensor nodes to discover optimal routing rules established on environmental feedback. A routing mechanism applying Q-learning to choose optimal routes among sender and receiver [5]. The RL learns from network situation, for example, energy and link quality, aiding nodes to energetically choose the best forwarding path. In addition, deep reinforcement learning dynamically adapts routing decisions utilizing network state information. Hence, enhances the routing efficiency [6]. A Support Vector Machine (SVM)-based energy-efficient routing strategy [7]. By improving energy efficiency, SVM has also been utilized to increase routing efficiency. Sensor nodes are categorized by the system using SVM according to criteria including residual energy, communication distance, and node density. After that, the chosen cluster heads carry out data forwarding and aggregation, cutting down on unnecessary transmissions and extending network lifespan. SVM-based routing dramatically lowers energy usage and enhances overall network performance, according to experimental data.

According to recent research, deep learning methods analyze intricate network factors including energy distribution, node mobility, and traffic patterns. These methods dynamically adjust to changes and forecast the best routing options. In IoT-enabled WSN contexts, deep learning-based techniques provide better throughput, reduced latency, and greater packet delivery ratios than traditional routing approaches [8]. Deep RL can energetically optimize routing paths. It analyses network parameters and chooses the best routes thus raises the throughput [9]. However, deep learning methods need more processing energy and training overhead that might be trying for sensor nodes with restricted resources. To improve routing efficiency, hybrid ML algorithm combines several algorithms, involving neural networks and RL. Research demonstrates that this system enhances performance by applying residual energy, node density, connection reliability, and communication delay. Adaptive routing techniques that efficiently change industrial contexts, minimize duplicate transmissions, maximize data flow, and raise network lifespan [10].

Conventional ML algorithms discover the essential features via definite feature extraction methods that raise the computation complexity. The proposed method utilizes a deep learning technique for attack details and their subcategories [11]. The detection model combines ResNet based on inception with a SVM to notice WSN intrusions. However, the deep learning algorithm needs large training datasets and developed computational resources. An enhanced Long Short-Term Memory (LSTM)-based anomaly detection system for detecting unusual network traffic patterns [12]. To enhance hyperparameter tuning and detection accuracy, the proposed system used optimization methods including Salp Swarm Algorithm and Particle Swarm Optimization. A hybrid deep learning algorithm that combines convolutional neural networks (CNN) and LSTM for identifying abnormalities in WSN [13]. CNN algorithm is used to extract spatial characteristics, and LSTM is used to extract temporal relationships. This approach detects the denial-of-service attacks efficiently. However, it increases computational complexity and needs large training datasets.

A federated learning framework in conjunction with LSTM networks to recognize anomalies in IoT-based WSNs [15]. This approach enhances privacy and scalability by enabling many IoT devices to cooperatively train a global LSTM model without exchanging raw data. The federated LSTM model increases the detection accuracy. An optimized Random Forest (RF) algorithm incorporated with the metaheuristic algorithm for anomaly detection in WSN. The proposed system automatically tunes RF hyperparameters to enhance classification accuracy and stability. It demonstrated how feature significance analysis enhances anomaly detection models' interpretability. A Tabu Search optimized RF algorithm to detect anomalies efficiently [16]. It improves the RF performance by improving features parameters and selection of features. Although it mainly focuses on attack detection rather than adjusting routing optimization. Aan ML based intrusion detection system which incorporates feature scaling and data considering techniques to enhance the detection performance [17]. However, it essentially concentrates on security detection rather than routing optimization, for further enhancement in network management.

A selection of Variables Ensemble machine learning algorithms as a foundation for detecting DoS attacks in

security risks. The system detects flooding, scheduling, blackhole, and grayhole threats using ensemble machine learning methods [18]. A self-supervised anomaly node detection model using autoencoders. To increase the accuracy of anomaly identification, this method uses graph neural networks to integrate temporal information, spatial node interactions, and network structure [19]. The research showed that anomaly detection ability is much enhanced when spatial-temporal information is combined. A survey of ML algorithms for anomaly detection in the network [20]. The autoencoders with recurrent neural network algorithms offer better capability for recognizing complex anomalies. But this approach also pointed out that many methods aren't flexible enough to function in dynamic network contexts.

A hybrid architecture that enhances anomaly detection by combining ensemble learning with deep reinforcement learning [21]. The system dynamically optimized communication tactics by using contextual data like signal strength and ambient factors. It demonstrated that reinforcement learning can significantly improve network reliability, signal quality, and adaptive decision-making in large-scale IoT environments. These results demonstrate how RL is appropriate for adaptive network management. Deep RL-based variational autoencoders for multivariate time-series anomaly identification [22]. To enhance anomaly categorization and adapt to shifting system circumstances, the suggested approach makes use of an RL agent. The advantages of hybrid AI models for intricate industrial monitoring systems are highlighted by this method. Several research gaps are found in the evaluated literature [23]. A lot of current anomaly detection models do not include route optimization; instead, they exclusively concentrate on fault detection. When choosing network pathways, traditional routing protocols do not take anomaly information into account. While mixed AI models are seldom used in IIoT network management, most searches use single AI methodologies. Adaptive self-learning frameworks are necessary due to resource limitations and changing network settings.

PROPOSED METHOD

The Industrial IoT environment signifies the smart factory system where several machines, equipment, and functioning monitoring devices. Here, several wireless sensor nodes are distributed throughout the industrial region and observe physical industrial parameters such as machine status, temperature, pressure, and vibration. The factory system utilizing four types of sensors such as temperature sensor for observing the heat levels in manufacturing equipment, vibration sensor for noticing abnormal machine vibrations for sustaining prediction, pressure sensor for evaluating pressure in pipelines and machine sensor for observing machine status and functional performance. Every sensor node also observes network parameters including residual energy, communication ratio, communication delay, and link quality. The base station (BS) exploits as the central transmission hub of the IWSN. The collected sensor data and network parameters are communicated to an edge computing unit. Data aggregation minimizes the redundancy, clean noisy sensor readings and makes the data for further analysis. Edge computing assists minimizes the network delay by processing data nearer to the sensor nodes rather than forwarding everything to the cloud. Autoencoders are unsupervised deep learning models that measure reconstruction errors to identify anomalies and learn patterns of typical network activity. Finding anomalous node activity, such as anomaly sensors, faulty sensors, packet dropping attacks, and energy reduction, is its primary goal.

Abnormal nodes may seriously impair network performance in Industrial WSN. The Autoencoder module aids in the detection of malicious or compromised nodes, malfunctioning or malfunctioning sensor nodes, packet dropping behavior, abnormal energy consumption patterns, and the prevention of anomalous nodes from taking part in routing. The technology increases network longevity, security, and reliability by identifying abnormalities early. The Encoder, Latent Space, and Decoder are the three primary parts of the Autoencoder. The proposed system combines Autoencoder-based anomaly detection and RL based routing optimization to enhance network reliability, energy efficiency, and fault tolerance. Figure 1 demonstrates an AI-driven self-learning network management system considered for Industrial IoT WSNs. The architecture is collected of many connected modules that work together to observe network behavior and optimize transmission dynamically. The proposed system contains four types of modules such as industrial environment, edge unit, Autoencoder based anomaly detection and RL based Route optimization.

Encoder: high-dimensional network data is compressed into a smaller representation by the encoder. Nodes' residual energy, communication ratio, packet delay, link quality indicator are examples of input parameters. In terms of math:

$$l = f(y) = f(Wy + c) \quad (1)$$

Where, y denotes input feature vector, f indicates an activation function, W refers weight matrix, c represents

bias and l indicates latent representation. The encoder obtains significant features which denote normal network behavior.

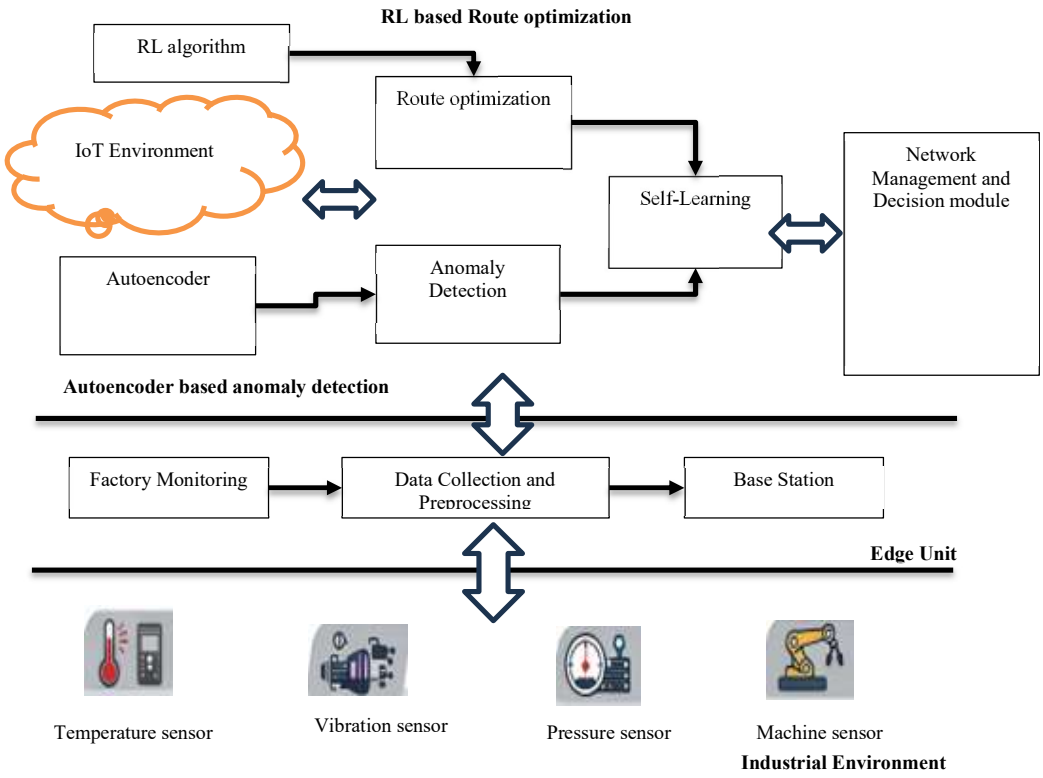

FIGURE 1. Architecture of the proposed system

Latent Space: The input data is represented in a compressed form in the latent space. It captures the key elements of typical network patterns, such as traffic patterns, energy use patterns, and link stability behavior. Anomalies cannot be adequately expressed in this tight area since they are uncommon.

Decoder: Using the compressed latent representation, the decoder reconstructs the original input.

$$\hat{x} = g(l) \tag{2}$$

Where, l denotes the latent representation, $\hat{y}$ refers reconstructed output, The decoder tries to replicate the original parameters.

Anomaly Detection: The anomaly detection process is based on reconstruction error, and it is specified below.

$$ER = || y - \hat{y} ||^2 \tag{3}$$

Where, x indicates original input data, $\hat{x}$= reconstructed output, ER indicates the reconstruction error. The decision rule for detecting anomaly nodes is specified below.

- If $ER <$ threshold that denotes the Normal node behavior
- If $ER >$ threshold that denotes an Anomaly node behavior

A high ER represents that the system cannot correctly rebuild the input that means the data pattern is abnormal. The algorithm of the training and testing phase is specified below.

Training steps

1. Gather factory data from several sensor nodes.
2. Preprocess the data
3. Train the Autoencoder to reform normal patterns.
4. Decrease reconstruct error via a loss function.
5. Loss function:
6. $L = \frac{1}{k}\sum(y_i - \hat{y}_i)^2$ (4)
   After training, the autoencoder learns normal network behavior patterns.

Testing steps

1. New sensor data is maintained into the Autoencoder.
2. The autoencoder reconstructs the input data.
3. ER is determined.
4. If the ER exceeds the threshold, the sensor is indicated anomaly.
5. Detected anomaly nodes are then disqualified from routing decisions.

The output of the anomaly detection phase is utilized by the RL routing optimizer. RL routing agent evades these nodes, and optimal routes are chosen via normal sensor nodes. RL is a ML method that uses interactions with the environment and incentives or penalties to teach an agent the best course of action. To find trends and forecast network conditions, machine learning algorithms examine network data. The IWSN serves as the environment and the network management controller as the RL agent in the proposed system. The RL agent observes the status of the network, chooses a course of action (such as routing), and is rewarded according to how well the network performs. By choosing the best course of action, the RL search to optimize the network performance. The components of RL algorithm are specified below.

Agent: It represents the system of network management that learns and produces decisions.

Environment: The IWSN contains several sensor nodes, links, and channels interaction.

State (S): The present network situation performed by the agent. Example state parameters are sensor node residual energy, delay, link quality, and congestion level.

Action (A): The RL agent takes an action. Feasible actions include choosing the best routing path, adapting transmission power, evading low-energy nodes and reconfiguring communication parameters

Reward (R): The response obtained by the agent after executing an action. Example reward design: high reward for link quality, Penalty for packet loss, penalty for high energy utilization and reward for low delay transmission. This reward function is specified below:

$$RW = \lambda(link\ quality) - \tau(Delay) - \gamma(Energy\ utilization) \quad (5)$$

Where, λ, τ, γ are weighting factors.

RL Algorithm: A RL algorithm for network optimization is Q-learning. The Q-value indicates the estimated reward for acting $a$in state s.

$$QV(s,a) = QV(s,a) + \eta[RW + \rho \max\ Q(s',a') - QV(s,a)] \quad (6)$$

where, $QV(s,a)$ represents the QV for state-action pair, indicates the learning rate, RW represents the reward, ρ denotes the discount factor, s'denotes the next state. The agent informs the QV-table till it discovers the optimal rule. The algorithm of the RL-based route optimization is specified below.

1. Sensor nodes forward factory information to the controller.

2. RL agent monitors the present state.
3. Agent chooses an action (decision of routing or configuration).
4. Network performs the action.
5. System estimates performance of network.
6. Reward is computed and fed back to the agent.
7. Agents inform their rules to adjust future decisions.

This procedure repeats incessantly, accepting the system to learn optimal network management strategies.

RESULTS AND DISCUSSION

The Network Simulator 2 (NS-2) environment was used to run simulations to assess the performance of the proposed AI-Driven Self-Learning Network Management system. Because NS-2 offers thorough modeling of network protocols, node behavior, and wireless communication, it is often used for evaluating the operation of IWSN. Simulation results demonstrate that the proposed Autoencoder with RL (AE-RL) system significantly improves network performance compared with RF, LSTM and SVM based approaches. significantly improves the performance of industrial wireless sensor networks. The RL based self-learning algorithm dynamically adjusts routing decisions to evade faulty nodes and optimize routing paths efficiently. The Autoencoder model effectively detects anomalous nodes by discovering deviations from normal network behavior. The parameters of the proposed system are specified in Table 1.

TABLE I. Simulation parameters of RL with autoencoder system

Parameter	Value
Simulation Region	600 x 700 m^2
Anomalous nodes	5-20 nodes
Sensor nodes	200 nodes
Propagation model	Two ray ground
Size of packet	512 bytes
Type of traffic	Constant Bit Rate
Communication Range	150 metres
Sensor node energy	2 joules

Sensor nodes were deployed in an industrial monitoring environment to carry out simulation tests. The simulation contained both normal and anomalous nodes to assess the flexibility of the proposed method. Throughput, anomaly detection accuracy, network latency, and energy consumption are some of the key measures used to assess the simulation's performance. An essential performance indicator for assessing how well a system detects anomalous activity in IWSNs is anomalous detection accuracy. Anomalies in industrial settings may be caused by hardware failures, unexpected traffic patterns, malicious nodes, or link failures. Maintaining network security, dependability, and effective communication depends on the accurate identification of these abnormalities. Figure 2 shows the anomaly detection accuracy of SVM, RF, LSTM and AE-RL based approaches.

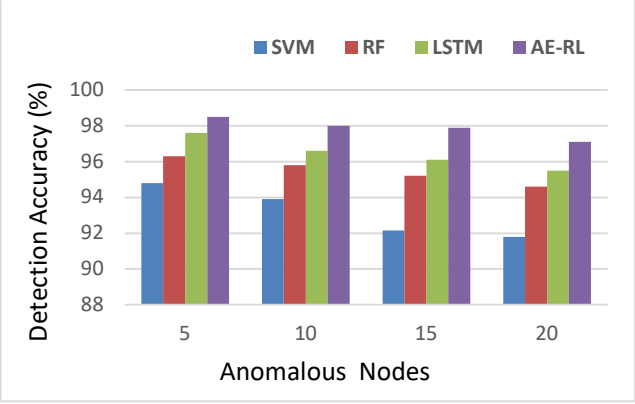

FIGURE 2. Anomaly detection accuracy of SVM, RF, LSTM and AE-RL based approaches

By creating a hyperplane that divides typical and anomalous network traffic patterns, the SVM-based method detects anomalies. SVM performs poorly when dealing with complicated nonlinear network dynamics in large-scale industrial WSN. By using an RF method, SVM outperforms in detection performance. To categorize anomalous occurrences, RF may examine a variety of network characteristics. Nevertheless, deep temporal correlations in network data cannot be learned by RF since it depends on predetermined feature patterns. LSTM outperforms SVM and RF in anomaly detection accuracy because of its capacity to identify temporal trends. However, longer training times and more processing power are often needed for LSTM models. Out of all the approaches examined, the proposed AE-RL solution, which combines an Autoencoder for anomaly detection with RL for adaptive network management, gets the greatest detection accuracy. By calculating the reconstruction error between the original input data and the output reconstruction, the autoencoder learns the typical patterns of network traffic behavior and identifies abnormalities efficiently. Throughput signifies the rate at which data packets are effectively distributed over the network. It is typically measured in kbps (kilobits per second). Figure 3 illustrates the throughput analysis of SVM, RF, LSTM and AE-RL based approaches.

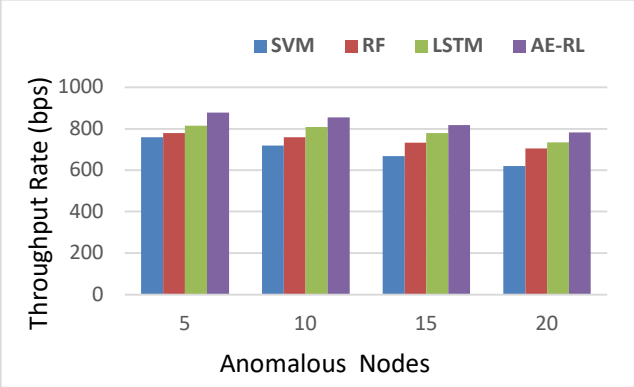

FIGURE 3. Throughput analysis of SVM, RF, LSTM and AE-RL based approaches

The simulation results demonstrate that the proposed AE-RL model reaches the highest throughput compared to other algorithm-based approaches. The combination of anomaly detection and adaptive routing enables the AI-RL system to evade faulty nodes and chooses reliable data transmission paths. This minimizes packet loss and enhances data transmission. LSTM executes well in analyzing temporal traffic patterns; however, it requires dynamic routing adaptation, resulting in marginally lesser throughput compared to the proposed AE-RL- approach. RF offers good categorization capability but does not nonstop learn network conditions that restrict routing efficiency. The SVM based approach reveals the lowest throughput because it fights with nonlinear and dynamic network conditions in Industrial IoT environments. Energy consumption is a critical performance indicator in wireless networks as excessive energy usage reduces network lifetime and jeopardizes overall communication reliability. Figure 4 explains energy consumption of SVM, RF, LSTM and AE-RL based approaches-based approaches.

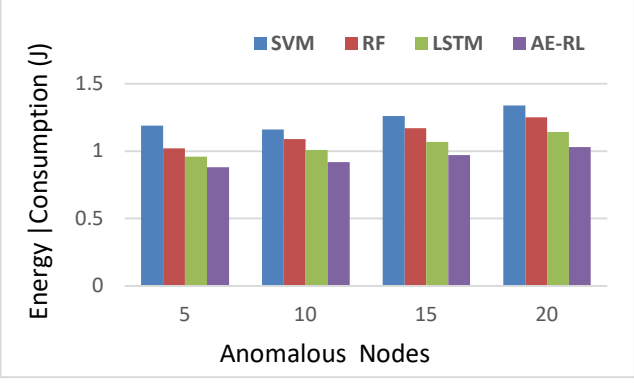

FIGURE 4. Energy consumption of SVM, RF, LSTM and AE-RL based approaches

Due to raising packet loss and routing errors, SVM, RF, LSTM and AE-RL algorithms consume more energy as the number of anomalous nodes increases. Retransmissions and needless communication are greatly decreased by the model's early detection of anomalous nodes and avoidance of routing via them. Because it can assess temporal traffic patterns, LSTM outperforms RF and SVM; nevertheless, it does not have adjust routing optimization. Although RF offers high categorization, its inability to constantly modify routing choices results in low energy usage. Due to its difficulties with dynamic anomalous activity and nonlinear network dynamics, SVM has the greatest energy usage. According to the simulation findings, the suggested AE-RL framework uses the least amount of energy in all anomalous node situations. However, by swiftly identifying anomalous nodes, dynamically choosing dependable routing methods, and reducing packet retransmissions, the suggested AI-driven self-learning framework retains greater energy efficiency.

The overall amount of time needed for a data packet to get from the sender sensor to the receiver sensor is known as the end-to-end delay. Retransmissions, network congestion, malicious packet dropping, and ineffective pathways may all cause delays in IWSN. Figure 5 shows the delay of SVM, RF, LSTM and AE-RL-based approaches.

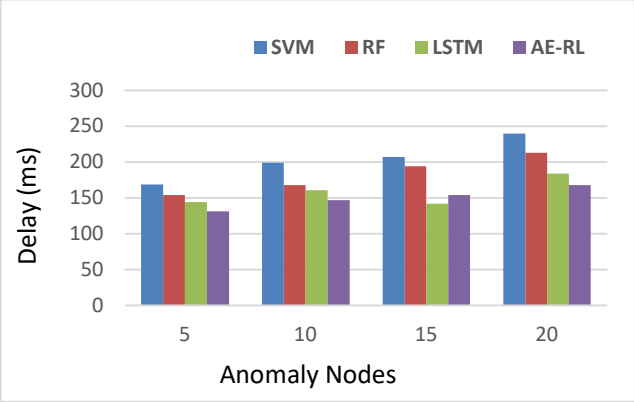

FIGURE 5. Delay of SVM, RF, LSTM and AE-RL based approaches

The network encounters more congestion and packet retransmissions as the number of malicious nodes rises, which causes SVM, RF, LSTM, and AE-RL algorithms to take longer. Retransmissions and packet forwarding delays are greatly decreased by the system's rapid detection of rogue nodes and avoidance of them during routing. Because it can assess traffic patterns, LSTM outperforms RF and SVM, but it is unable to dynamically improve routing pathways. Although RF has a reasonable latency, it does not continuously adjust to network conditions. Due to its inability to manage changing risky activity in large-scale networks, SVM exhibits the largest latency. However, because of early anomalous node identification, adaptive routing optimization, and enhanced network stability, the proposed AI-driven self-learning network management framework maintains noticeably reduced delay. This shows that, in comparison to conventional machine learning techniques, the suggested solution offers quicker and more dependable communication in IWSNs.

CONCLUSION

An AI-Driven Self-Learning Network Management framework for IWSNs was proposed in this study. It uses RL-based adaptive routing optimization and autoencoder-based anomaly detection. Malicious node activity, link failures, congestion, energy constraints, and unpredictable network circumstances are some of the issues that WSNs often face. These issues lower communication dependability and increase energy consumption. The proposed system combines deep learning and RL to provide an intelligent and flexible network solution to overcome these problems. The autoencoder algorithm effectively detects anomalous nodes and network abnormalities by learning the typical traffic behavior of the network and recognizing abnormal patterns by evaluating reconstruction errors. Then the RL agent dynamically chooses the best routing pathways depending on network factors like node energy, link quality, and congestion level when anomalies are identified. The simulation results demonstrated improvements in several critical performance parameters, such as end-to-end delay, network throughput, energy consumption and anomaly detection accuracy. Even though the proposed AI-driven

framework demonstrates notable advancements in anomalous detection and network management, there are still several areas that need more investigation. The proposed system may be expanded to accommodate real-time edge computing settings, where gateway nodes or edge devices handle routing and anomaly detection. This would enhance the system's scalability for extensive industrial installations and decrease processing latency. To further assess the proposed system usefulness in industrial monitoring systems, hardware-based sensor networks and real-world Industrial IoT datasets may be used for implementation and validation.

REFERENCES

[1]. O. Peter, A. Pradhan, and C. Mbohwa, 2023, "Industrial internet of things (IIoT): opportunities, challenges, and requirements in manufacturing businesses in emerging economies," *Procedia Computer Science*, 217, pp. 856-865.

[2]. J. Liu, Y. Du, K. Yang, J. Wu, Y. Wang, X. Hu, and V.C. Leung, 2026, "Edge-cloud collaborative computing on distributed intelligence and model optimization: A survey," *IEEE Communications Surveys & Tutorials.* pp. 1-43.

[3]. A. Zila, A. Ouchatti, and Y. Mouzouna, 2025, "Exploring node failure and packet loss in wireless sensor networks: a comprehensive simulation analysis," *International Journal of Communication Systems*, 38(13), pp. 1-15.

[4]. Y.Y. Ghadi, T. Mazhar, T. Al Shloul, T. Shahzad, U.A. Salaria, A. Ahmed, and H. Hamam, 2024, "Machine learning solutions for the security of wireless sensor networks: A review," *IEEE Access*, 12, pp. 12699-12719.

[5]. A. Neelu, J.P. Pramod, and A. Lahari, 2025, "Optimizing Networks Using AI and Machine Learning: The Role of Agentic AI in Transforming Network Management," *In the Power of Agentic AI: Redefining Human Life and Decision-Making: In Industry* 6.0, *Cham: Springer Nature Switzerland*, pp. 229-254.

[6]. M. Akram, S.U. Bazai, M.I. Ghafoor, S. Akram, Q.M. Ilyas, A. Mehmood, and M.A. Rafique, 2025, "EEMLCR: Energy-efficient machine learning-based clustering and routing for wireless sensor networks," *IEEE Access,* 13, pp. 70849 - 70871.

[7]. D. Godfrey, B. Suh, B.H. Lim, K.C. Lee, and K.I. Kim, 2023, "An energy-efficient routing protocol with reinforcement learning in software-defined wireless sensor networks," *Sensors*, 23(20), Article. 8435.

[8]. M. Al-Naeem, M.M. Hafizur Rahman, A. Banerjee, and A. Sufian, 2023, "Support vector machine-based energy efficient management of UAV locations for aerial monitoring of crops over large agriculture lands," *Sustainability*, 15(8), Article. 6421.

[9]. B.F. Azevedo, A.M.A Rocha, and A.I. Pereira, 2024, "Hybrid approaches to optimization and machine learning methods: a systematic literature review," *Machine Learning*, 113(7), pp. 4055-4097.

[10]. S. Thakur, N.I. Sarkar, and S. Yongchareon, 2025, "AI-Driven Energy-Efficient Routing in IoT-Based Wireless Sensor Networks: A Comprehensive Review," *Sensors*, 25(24), Article. 7408.

[11]. M. Sakthimohan, J. Deny, and G.E. Rani, 2024, "Secure deep learning-based energy efficient routing with intrusion detection system for wireless sensor networks," *Journal of Intelligent & Fuzzy Systems*, 46(4), pp. 8587-8603.

[12]. V. Gowdhaman, and R. Dhanapal, 2024, "Hybrid deep learning-based intrusion detection system for wireless sensor network," *International Journal of Vehicle Information and Communication Systems*, 9(3), pp. 239-255.

[13]. N. Dash, S. Chakravarty, A.K. Rath, N.C. Giri, K.M. AboRas, and N. Gowtham, 2025, "An optimized LSTM-based deep learning model for anomaly network intrusion detection," *Scientific Reports*, 15(1), Article. 1554.

[14]. C.W. Chang, C.Y. Chang, and Y.Y. Lin, 2022, "A hybrid CNN and LSTM-based deep learning model for abnormal behavior detection," *Multimedia Tools and Applications*, 81(9), pp. 11825-11843.

[15]. R.W. Anwar, M. Abrar, A. Salam, and F. Ullah, 2025, "Federated learning with LSTM for intrusion detection in IoT-based wireless sensor networks: a multi-dataset analysis," *PeerJ Computer Science*, 11, Article. e2751.

[16]. I. Gad, 2025, "TOCA-IoT: threshold optimization and causal analysis for IoT network anomaly detection based on explainable random forest," *Algorithms*, 18(2), Article.117.

[17]. V.K. Pandey, S. Prakash, T.K. Gupta, P. Sinha, T. Yang, R.S. Rathore, and S.T. Bakhsh, 2025, "Enhancing intrusion detection in wireless sensor networks using a Tabu search-based optimised random forest," *Scientific Reports*, 15(1), Article. 18634.

[18]. M.A. Talukder, S. Sharmin, M.A. Uddin, M.M. Islam, and S. Aryal, 2024, "MLSTL-WSN: machine

learning-based intrusion detection using SMOTETomek in WSNs," *International Journal of Information Security*, 23(3), pp. 2139-2158.

[19]. A. John, I.F.B. Isnin, S.H.H. Madni, and M. Faheem, 2024, "Cluster-based wireless sensor network framework for denial-of-service attack detection based on variable selection ensemble machine learning algorithms," *Intelligent Systems with Applications*, 22, Article. 200381.

[20]. M. Ye, Q. Zhang, X. Xue, Y. Wang, Q. Jiang, and H. Qiu, 2024, "A novel self-supervised learning-based anomalous node detection method based on an autoencoder for wireless sensor networks," *IEEE Systems Journal*, 18(1), pp. 256-267.

[21]. S. Zehra, U. Faseeha, H.J. Syed, F. Samad, A.O. Ibrahim, A. W. Abulfaraj, and W. Nagmeldin, 2023, "Machine learning-based anomaly detection in NFV: A comprehensive survey," *Sensors*, vol. 23, no. 11, Article. 5340.

[22]. M. Al-Saadi, M. Al-Greer, and M. Short, 2023, "Reinforcement learning-based intelligent control strategies for optimal power management in advanced power distribution systems: A survey," *Energies*, vol. 16, no. 4, Article. 1608

[23]. K. Arshad, R.F. Ali, A. Muneer, I.A. Aziz, S. Naseer, N.S. Khan, and S.M. Taib, 2022, "Deep reinforcement learning for anomaly detection: A systematic review," *IEEE Access*, 10, pp. 124017-124035.

[24]. J. Liu, Y. Du, K. Yang, J. Wu, Y. Wang, X. Hu, and V.C. Leung, 2026, "Edge-cloud collaborative computing on distributed intelligence and model optimization: A survey," *IEEE Communications Surveys & Tutorials*. 28, pp. 5049-5080.