Iraqi Journal of Computers, Communications, Control and Systems Engineering

Volume 26 | Issue 1 Article 6

4-4-2026

Reliability Analysis for Deep Learning Secured Wireless Sensor Networks

Abeer Hussein Abdulrasool
Collage of Artificial Intelligence Engineering, University of Technology, Iraq,
cse.23.08@grad.uotechnology.edu.iq

Ekhlas Kadhum Hamza
Collage of Artificial Intelligence Engineering, University of Technology, Iraq,
ekhlas.k.hamza@uotechnology.edu.iq

Ahmed Mudheher Hasan
Collage of Artificial Intelligence Engineering, University of Technology, Iraq,
ahmed.m.hasan@uotechnology.edu.iq

IJCCCE 2026;26(1):69–82

RESEARCH ARTICLE

Reliability Analysis for Deep Learning Secured Wireless Sensor Networks

Abeer Hussein Abdulrasool *, Ekhlas Kadhum Hamza, Ahmed Mudheher Hasan

Collage of Artificial Intelligence Engineering, University of Technology, Iraq

ABSTRACT

With the advancement of software, wireless sensor networks (WSNs) face many problems and challenges, such as loss or limitation of node power resources, as well as intrusions and other cyberattacks. This study aims to improve the reliability of WSNs to mitigate the impact of cyber-attacks by applying effective detection and prevention techniques to ensure their continuous operation, as well as to maintain the security, privacy, and integrity of information. Several efficient approaches and smart techniques have been presented in literature to enhance the reliability and security of WSNs against various cyber-attacks. Recent studies focused on the deep learning (DL) algorithms as efficient and robust solutions in detecting and eliminating the threats up on WSNs.

In this study, a deep long short tern memory (LSTM) algorithm that utilizes both short-term and long-term memory and performs well with long-term dependencies was presented to handle intrusions in the sensor network. The model uses LSTM networks to manage these variances and provide security and reliability because mobile attacks might have unpredictable patterns. Every time the regulated parameters are iterated, each node communicates its position and degree of movement, along with other significant information. Important metrics included the ratio of active to dormant nodes, data received per node, communication time, energy consumption per iteration, and communication time between nodes. These measures help assess how stable the model is in different scenarios. Such measurements allow us to predict future node behaviors and the network's highly reliable operation in addition to focusing on stability and security. The proposed LSTM deep learning attack defense model has been applied to improve the reliability of the sensor network by 30%, extend the lifetime of active nodes by 22%, and reduce node energy consumption in the WSN by 55%.

Keywords: Wireless Sensors Networks (WSNs), Deep learning technique, Long Short Term Memory (LSTM) algorithm, Reliability analysis, Life time, Energy consumption

Received 27 October 2025; revised 3 December 2025; accepted 10 December 2025.
Available online 4 April 2026

* Corresponding author.
E-mail addresses: cse.23.08@grad.uotechnology.edu.iq (A. H. Abdulrasool), Ekhlas.K.Hamza@uotechnology.edu.iq (E. K. Hamza), ahmed.m.hasan@uotechnology.edu.iq (A. M. Hasan).

https://doi.org/xx.xxxxx/2617-3352.1518

Highlights

1. LSTM (Long Short-Term Memory) is a type of deep learning recurrent neural network (RNN) widely used in deep learning. It is characterized by its ability to capture long-term dependencies, making it ideal for sequence prediction tasks.
2. WSN, Wireless sensor networks consist of a set of spatially distributed sensors designed to monitor and record the physical conditions of the environment and send the collected data to a central location. Wireless sensor networks can measure environmental conditions such as temperature, sound, pollution levels, humidity, and wind.
3. AI, It is a technology that enables machines and computers to perform tasks that normally require human intelligence. These systems help in learning from data, recognizing patterns, and making decisions to solve complex problems.

1. Introduction

Numerous real-world applications, such as computer system management, industrial process control, environmental monitoring, crop monitoring, meteorology, healthcare, and other vital sectors of life, rely on Wireless Sensor Networks (WSNs). A group of sensor nodes dispersed across the network make up WSNs, which coordinate information transfer, keep an eye on transmitting and receiving, and regulate various parameters. They are controlled by a central node or base station and are linked to each other. The loss or restriction of energy sources for nodes, as well as other invasions and cyber-attacks, are some of the problems and challenges that WSNs face. These issues and challenges effect their operational continuity, as well as the security and privacy of information and dependability. A significant security risk that jeopardizes these networks' dependability, resulting in decreased stability and endangering the confidentiality and security of the data and information sent across them. To achieve the necessary level of security, prevent different cyber-attacks, neutralize risks and breaches, and guarantee the dependability of wireless networks, a variety of smart technologies are employed [1, 2]. In order to optimize node source energy investment, solve routing challenges, increase data transmission efficiency, and preserve network security and privacy, smart technologies and deep learning algorithms are used to resolve network concerns. The ability to precisely estimate sensor node positions and recognize movement patterns is necessary for these adaptive smart technologies to enhance information routing and transmission over such nodes. Fig. 1 shows schematic diagram of reliability based WSNs deep learning model [3–5].

Even while security has little to do with throughput and average residual energy, maintaining the accuracy of sink location forecasts depends on effective communication and minimizing power waste. This study's main driving force is the requirement to use precise and safe prediction models to increase the dependability and effectiveness of WSNs. By applying cutting-edge deep learning techniques, particularly Long Short-Term Memory (LSTM) networks, we intend to solve the dynamic nature of mobile sink motions and the related difficulties in trajectory prediction. The ability of LSTM networks to identify long-term relationships in data makes them perfect for sequence prediction tasks, including forecasting the locations of mobile sinks in WSNs [6–8]. In wireless sensor networks, we suggest the Deep LSTM Network, which has an advanced, dependable model for precisely forecasting the future paths of mobile sinks. Our model addresses the intrinsic unpredictability in mobile sink trajectories by using LSTM networks to capture both short-term variations and long-term trends in sink movement patterns. A thorough simulation setup covering parameter design, clustering, initialization of mobility parameters, and prediction model choices is part of our study. The performance of the suggested model

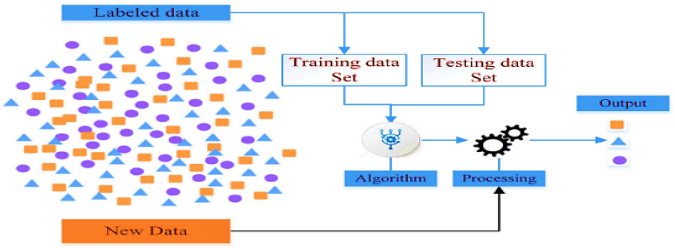


Fig. 1. Schematic chart of the reliable wsns deep learning structure [4].

may be evaluated in a reliable assessment environment thanks to this framework. The LSTM-Net model performs better than current techniques in terms of data transmission reliability, energy efficiency, and network longevity. According to our tests, the model can increase WSNs' operational lifetime, enhancing the overall performance and stability of the network.

1.1. Reliability analysis

Reliability is the probability that a wireless sensor network will perform its essential functions (such data collection and communication) for a predetermined period of time under specific conditions without encountering any issues. Network topology (such as mesh, star, or cluster-based networks), link failures (because to noise, interference, or physical obstacles), and node failures (due to hardware issues, power outages, or attacks) are the main factors affecting reliability. The reliability analysis schematic diagram in WSN contexts is shown in Fig. 2 [9, 10].

Fig. 2 illustrates how reliability data have been acquired over time using a typical wireless sensor network (WSN) for three distinct communication protocols: direct networks, floods, and the low-energy adaptive clustering hierarchy (LEACH). It's evident that the LEACH network protocol yields the best reading of reliability measures versus time, while the direct protocol yields a lower response. The flooding network protocol yields the poorest reliability response. Consequently, Table 1 compares the reliability analysis of three methods in WSNs [11, 12].

The likelihood that a sensor node will continue to work over time, or node reliability $R_n(t)$, is modeled using an exponential failure distribution, which is common for electrical equipment. The model node reliability $R_n(t)$ might be written as below [10–12]:

$$R_n(t) = e^{-\lambda_n t} \tag{1}$$

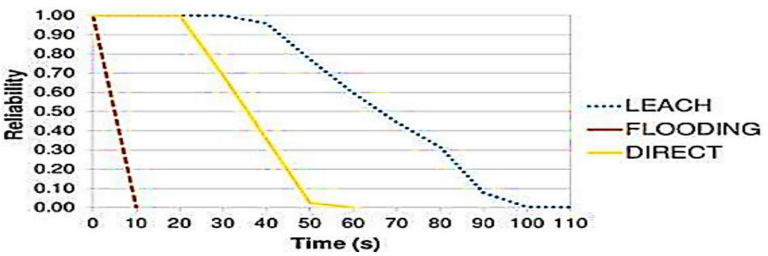


Fig. 2. Schematic diagram of reliability analysis in wsn environments [10].

Table 1. Comparison summary of the reliability analysis in wsns for three protocols.

Protocol Type	Reliability Trend	Failure Reason	Benefits/Drawbacks
LEACH	Slowest decay (0.50 → 0.20)	Balanced energy use via clustering	Energy-efficient but complex to implement.
DIRECT	Sharp drop (0.50 → 0.00)	Single-point energy depletion	Simple but inefficient for large WSNs.
FLOODING	Gradual decline (0.50 → 0.00)	Energy waste from redundant transmissions	Robust but energy-inefficient.

Whereas, λ_n indicates the node failure rate, L denotes the number of communication links, also t denotes the running period. It is also possible to define link reliability as the likelihood that a wireless sensor network (WSN) would remain stable. Using the formula below, this metric might be assessed based on the waveform strength (P_t), data transmission route loss (PL), and channel noise (N_0):

$$R_n(t) = e^{-\lambda_l t} \tag{2}$$

The following equation might be used to define, λ_l, which stands for the bit error rate (BER) in bits/sec:

$$BER = \frac{1}{2} erfc\left(\sqrt{\frac{E_b}{N_o}}\right) \tag{3}$$

Where, E_b denotes the bit energy, N_o indicates the Gaussian noise energy, and $erfc$ represents the error function. Also, The probability that the network will remain connected (i.e., at least one access between sensors and the sink) is represented by the Network Reliability (R_{net}). As a result, the Network Reliability (R_{net}) for parallel and series models might be written as follows [13–15]:

For series scheme (each nodes must activate):

$$R_{\text{net}} = \prod_{i=1}^{N} R_n^i(t) \tag{4}$$

Where, N denotes the total nodes number. For parallel scheme (arbitrary path):

$$R_{\text{net}} = 1 - \prod_{i=1}^{N} (1 - R_n^i(t)) \tag{5}$$

Where, R indicates the Network Reliability. Additionally, we were able to determine how battery depletion is explained by energy-based reliability. Thus, the Energy-based reliability computes the probability $R_{energy}(t)$ that any node energy E_t stays above threshold E_{th} as follows:

$$R_{energy}(t) = P(E(t) > E_{th}) \tag{6}$$

Where, E represent the energy index. Lastly, by calculating the average time before the network failure as shown below, we may calculate the mean time to failure (MTTF) [16, 18, 21]:

$$\text{MTTF} = \int_0^{\infty} R_{energy}(t)\, dt \tag{7}$$

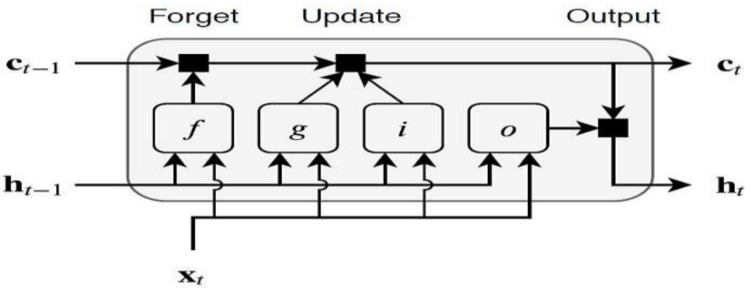


Fig. 3. Deep learning (LSTM) structure with inside data flow time steps *T* strategy [26].

Where, E_{th} indicates the threshold energy. Additional nodes and cables might be installed to increase WSN redundancy dependability. Reroutes and other self-healing techniques are examples of fault tolerance. Sleep scheduling and energy harvesting are also included in energy management. Additionally, the topology control places nodes as effectively as feasible. This is the structure of the remainder of the paper: An extensive overview of the literature is provided in Section 2, the methodology, including explanations of the process flow and algorithms, is described in Section 3, and the experimental studies that support the LSTM-Net approach are presented in Section 4. In Section 5, the integration of a trust model and future research possibilities are discussed.

1.2. Deep learning long short term memory (LSTM) algorithm

With vast amounts of data analysis, deep learning techniques are frequently utilized to mimic human brain activity in order to implement intelligent missions. The long short term memory (LSTM) structure's data flow diagram at time step t is shown in Fig. 3, with particular attention to the forgetting, updating, and departing cell gates and hidden states operations [26–30].

Therefore, the input weights W (InputWeights), the recurrent weights R (RecurrentWeights), and the bias b (Bias) are the learnable weights in the LSTM deep learning layer. The sequences of input weights, recurrent weights, and the bias value for each component are represented by the matrices W, R, and b, respectively. These matrices are defined by the following equations: [28–32]:

$$W = \begin{bmatrix} W_i \\ W_f \\ W_g \\ W_o \end{bmatrix}, \; R = \begin{bmatrix} R_i \\ R_f \\ R_g \\ R_o \end{bmatrix}, \; b = \begin{bmatrix} b_i \\ b_f \\ b_g \\ b_o \end{bmatrix} \tag{8}$$

The entry gate, forget gate, cell candidate, and resultant gate are therefore indicated by the letters i, f, g, and o, respectively. The following represents the cell state at time step t:

$$c_t = f_t \odot c_{t-1} + i_t \odot g_t \tag{9}$$

where the Hadamard product (vector-wise multiplication) is denoted by $\odot$. Additionally, the following represents the concealed state at time step t:

$$h_t = o_t \odot \sigma_c(c_t) \tag{10}$$

where σ_c is the state activation function and the LSTM layer function uses the hyperbolic tangent (tanh) function by default to evaluate the state activation function. Deep neural

networks are revolutionizing artificial intelligence because they can simulate complex data using multi-layered structures, and they are crucial for modern AI applications due to their versatility across domains—from language to vision—and their ability to learn hierarchical information [33–35].

1.3. Motivation & contribution

This study aims to analyse and improve the reliability of the deep learning LSTM algorithm for detecting and preventing cyber-attacks, thereby enhancing the safety and security of data transmission in WSNs. The appropriate theoretical background was reviewed in the introduction section to clarify the key theoretical concepts of this study, supported by mathematical equations and related diagrams. The focus was also on proposing an LSTM network model to handle cyber-attacks and studying the changes in the WSN system to close vulnerabilities, improve data security, and increase reliability. The iterations of the parameters organized for the proposed LSTM technique are calculated, updating the change amount of each node within its layers along with other important information. Additionally, connection times and energy consumption rates are evaluated in each iteration, while monitoring the data received by each node and the ratio of active to inactive nodes to enhance the network's reliability.

2. Literature review

Many studies and scientific articles have addressed the limitations and analysis of the topic of reliability in wireless networks supported by deep learning techniques to achieve optimal performance and maintain smooth data transfer while utilizing energy resources. In this section, the latest contributions from researchers in this field will be reviewed, and their proposals will be presented to achieve the best performance for network reliability, along with a demonstration of the limitations and gaps. A convolutional neural network (CNN), LSTM, Blockchain techniques are proposed for industrial IoT (IIoT) application. The suggested strategies provided improved intrusion detection using hybrid DL and blockchain for secure WSNs. The study has limitations of high computational overhead due to blockchain integration (Zhang et al. 2022) [20]. Also, Federated Learning (FL), AES techniques are suggested for Healthcare WSNs application. This study has advantages of providing privacy-preserving FL for anomaly detection with reduced data leakage risks. The proposed approaches requires high synchronization among nodes as study gaps (Khan et al., 2022) [21]. Next, Generative Adverse Networks (GANs), and Reinforcement Learning (RL) algorithm are presented for Smart Grids networks. The proposed strategy produced enhanced reliability against adversarial attacks using GAN-based defense. The suggested algorithm suffers from training complexity that increases with network size (Li et al., 2023) [22]. An Auto-encoders, SHA-3 Hashing approaches have introduced for Military Surveillance applications. The study contributes a Lightweight anomaly detection with low false positives. The proposed models have gaps of limited scalability for ultra-dense WSNs (Wang & Chen, 2023) [23]. Also, a Graph Neural Networks (GNNs) has recommended for Smart Cities. This strategy show improved trust management in WSNs using GNN-based reliability modeling. The study gaps represented with high memory consumption for large graphs (Al-Turjman et al., 2023) [24]. Next, Transformer Models, Homomorphic Encryption techniques are analyzed for Agricultural WSNs. This study show secure data aggregation with encrypted DL for real-time monitoring with high latency

due to encryption overhead limitations (Rana et al., 2024) [25]. The spiking neural networks (SNNs) has been proposed for environmental monitoring application. This study contributes with energy-efficient anomaly detection using bio-inspired SNNs. Also, the proposed technique show lower accuracy compared to traditional DNNs (Yadav & Singh, 2024) [26]. Table 2 summarized the most recent studies (2022–2025) related to the subject of "Reliability Analysis for Deep Learning Secured Wireless Sensor Networks (WSNs).

Table 2. Summary of related studies (2022–2025) concerning the topic of "reliability analysis for deep learning secured wireless sensor networks (WSNS)".

Author(s) & Year	Employed Technology	Application	Contributions	Limitations
Zhang et al. (2022)	CNN, LSTM, Blockchain	Industrial IoT (IIoT)	Improved intrusion detection using hybrid DL and blockchain for secure WSNs.	High computational overhead due to blockchain integration.
Khan et al. (2022)	Federated Learning (FL), AES	Healthcare WSNs	Privacy-preserving FL for anomaly detection with reduced data leakage risks.	Requires high synchronization among nodes.
Li et al. (2023)	GANs, Reinforcement Learning (RL)	Smart Grids	Enhanced reliability against adversarial attacks using GAN-based defense.	Training complexity increases with network size.
Wang & Chen (2023)	Autoencoders, SHA-3 Hashing	Military Surveillance	Lightweight anomaly detection with low false positives.	Limited scalability for ultra-dense WSNs.
Al-Turjman et al. (2023)	Graph Neural Networks (GNNs)	Smart Cities	Improved trust management in WSNs using GNN-based reliability modeling.	High memory consumption for large graphs.
Rana et al. (2024)	Transformer Models, Homomorphic Encryption	Agricultural WSNs	Secure data aggregation with encrypted DL for real-time monitoring.	High latency due to encryption overhead.
Yadav & Singh (2024)	Spiking Neural Networks (SNNs)	Environmental Monitoring	Energy-efficient anomaly detection using bio-inspired SNNs.	Lower accuracy compared to traditional DNNs.
Chen et al. (2024)	Edge AI, Differential Privacy (DP)	Industrial Automation	Edge-based DL with DP for reliable and private WSN data processing.	Trade-off between privacy and model accuracy.
Gupta et al. (2025)	Quantum ML, Post-Quantum Cryptography	Defense & Aerospace	Quantum-resistant security for mission-critical WSNs.	Early-stage technology, lacks real-world validation.
Liu et al. (2025)	Explainable AI (XAI), LSTM	Smart Healthcare	Interpretable DL models for reliable fault detection in medical WSNs.	Increased computational cost for explainability.

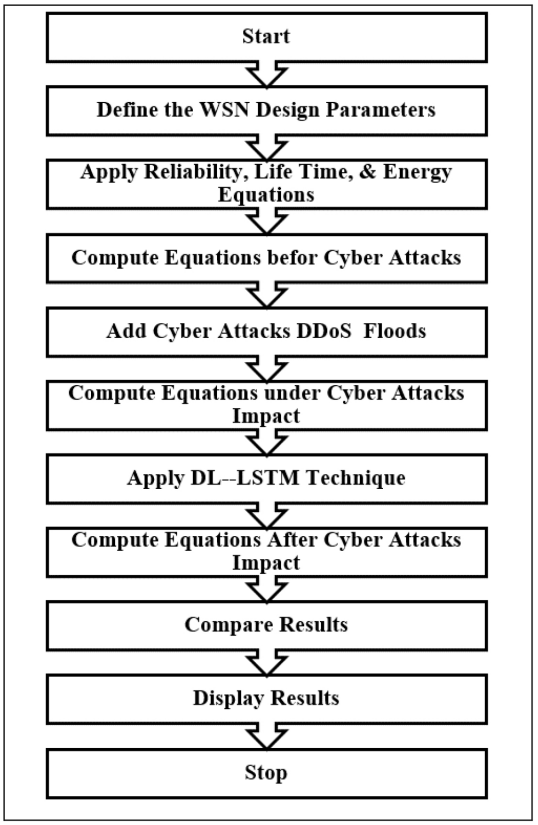


Fig. 4. Flow chart of the suggested wsns security model methodology.

3. Methodology

The process and methodology for creating and executing a reliability test model, lifetime, and energy consumption for every node in a wireless sensor network will be described in this section. In order to evaluate the effect of assaults, especially DDoS attacks, on the data transmission performance efficiency in the WSN, these metrics will be computed both before and after employing deep learning algorithms to identify and mitigate cyber-attacks. The transactions and design values for the wireless network model are set as the total number of nodes, the amount of energy for each node, the threshold energy value, in addition to the approximate distances between nodes and the mechanism for distributing nodes or the communication protocol. The flowchart proposed reliable WSN deep learning security model is shown in Fig. 4. Concerning Fig. 4, the rreliability equations, node lifespan, and energy consumption for the active nodes in the wireless sensor network are calculated under normal transmission conditions, in the event of a cyber- attack, and also in the case of countering and preventing attacks using deep learning technology LSTM. Also, Table 3 displays the design parameters and methodology settings of the proposed reliable WSN deep learning security model. Furthermore, the design details of the suggested LSTM DL algorithm could be presented in Fig. 5.

Fig. 6 shows the simulated diagram of the WSN structure employed to obtain the model environment. By looking Fig. 6, the simulated plan of the virtual WSN architecture has arbitrarily distributes network nodes (N = 50) to ensure fair data transfer between them to

Table 3. The design settings of the proposed model.

Parameter	Symbol	Value/Range	Description
WSN Type	–	Homogeneous	All nodes have similar capabilities
Number of Nodes	N	50	Total sensor nodes in the network
Threshold Energy	E_{th}	0.1 J	Minimum energy for active node operation
Network Protocol	–	LEACH	Cluster-based routing protocol
Initial Node Energy	$E_{initial}$	5–8 J (random)	Starting energy per node
Packet Rate	Λ	1 packet/node/round	Data generation frequency
Bit Error Rate (BER)	BER	10^{-4}	Probability of bit transmission error
Round Duration	T_{round}	60 sec	Time per simulation round
Connection Distance	D	100 m	Max distance between node and BS/cluster head
Electrical Energy (Tx)	E_{Tx}	50 nJ/bit	Transmitter/receiver circuit energy
Electrical Energy (Amp)	$E_{electrical}$	10 pJ/bit/m^2	Amplifier energy for free-space transmission

```
layers =

  6×1 Layer array with layers:

     1   ''   Sequence Input      Sequence input with 500 dimensions
     2   ''   LSTM                LSTM with 200 hidden units
     3   ''   Fully Connected     50 fully connected layer
     4   ''   Dropout             50% dropout
     5   ''   Fully Connected     500 fully connected layer
     6   ''   Regression Output   mean-squared-error
```

Fig. 5. Design details of the suggested lstm deep learning algorithm.

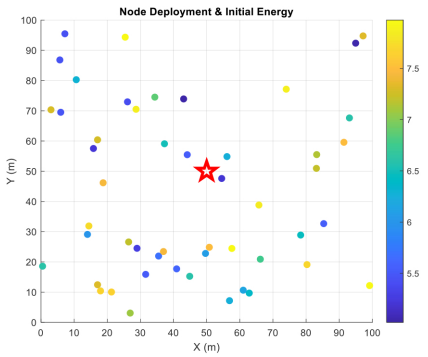


Fig. 6. The simulated diagram of the wsn structure employed to obtain the model environment.

achieve a working environment, where information data is sent and received between the distributed nodes, which represent wireless communication stations. Next, Fig. 7 displays the distribution of the same WSN nodes under DDoS attacks and with deep learning LSTM model. Concerning the results in Fig. 7, we could notice the difference between the WSN nodes distributions, such that, under DDoS attack floods, the WSN inactive nodes are increased due to the intrusion effect as presented in the upper Figure half. On the other hand, the inactive nodes are decreased to minimal sum when applying anti-attack deep learning LSTM algorithm as displayed in the lower Figure half. Next, applying reliability, life time, and energy consumption equations on the proposed WSN anti-attack model for three case studies. Normal WSN structure, WSN under cyber-attacks impact, and WSN after employing anti-attack LSTM deep learning model. Thus, Fig. 8 demonstrates the energy consumption results without and with anti-attack deep learning LSTM model.

The methodology of the proposed model will be designed and implemented using MATLAB code script.

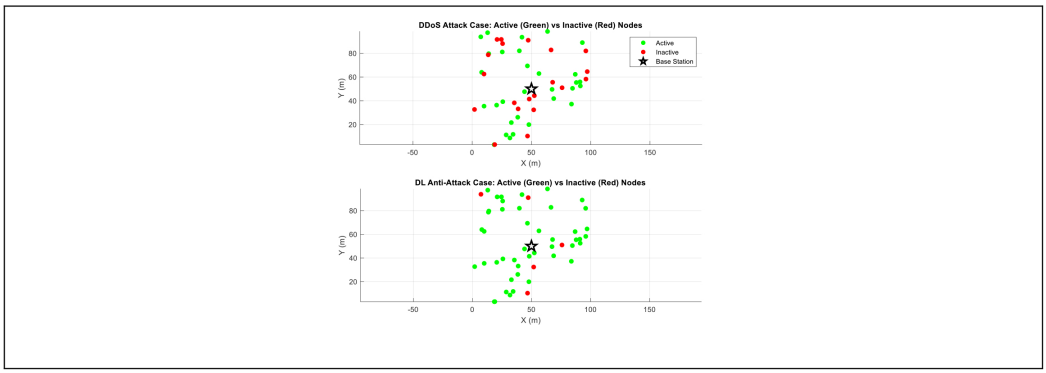
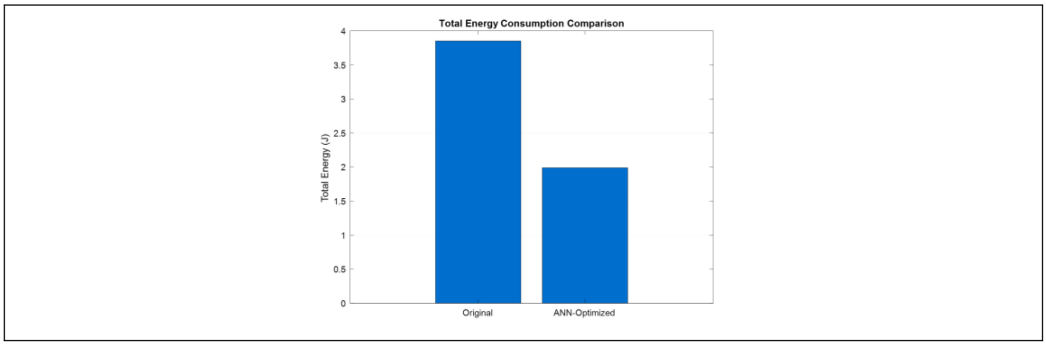
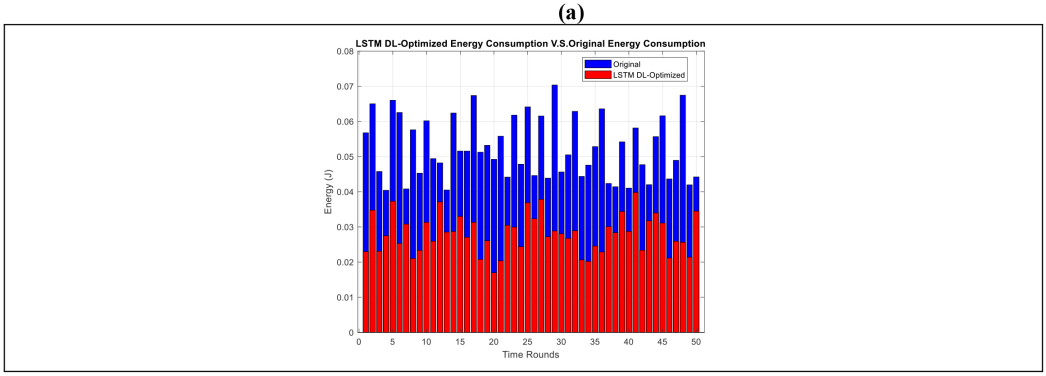


Fig. 7. The distribution of the same wsn nodes under ddos attacks and with deep learning LSTM model.



(a)



(b)

Fig. 8. Results of the energy consumption metric without and with anti-attack deep learning lstm model, (a) total nodes rounds, (b) energy per each round.

4. Results & discussions

In this paper, the reliable WSN deep learning security model has been successfully simulated and employed using MATLAB code scripts according to the proposed model structure and design settings.

Referring to the results presented in Fig. 8, it is clear that the energy consumption metric of the total WSN nodes has enhanced from 3.7 Joules to 2 Joules through employing LSTM deep learning anti-attack model which ensures the successful of the proposed model

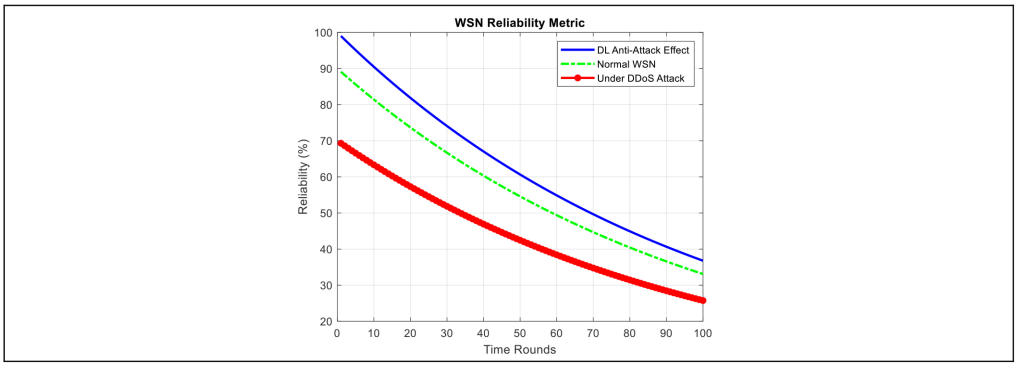


Fig. 9. The computed reliability metric, (a) normal wsn model, (b) wsn under cyber-attack effect, and (c) wsn under the proposed lstm dl model.

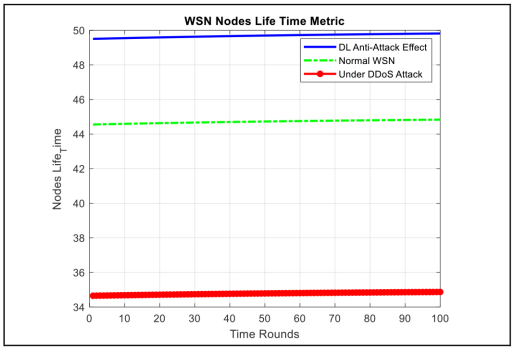


Fig. 10. The obtained life time metric, (a) normal wsn model, (b) wsn under cyber-attack effect, and (c) wsn under the proposed lstm dl model.

in saving total network nodes energy. Also, the reliability metric has been computed for the three cases of normal WSN model, WSN under cyber-attack effect, and WSN after employing the proposed anti-attack LSTM DL model as shown in Fig. 9. As outlined in Fig. 9, it might be noticed that, the computed reliability metric for our WSN secure model has display the lowest readings (from 70 to 26)% against time rounds when the WSN environment was under DDoS cyber-attack flood impact. Next, this reliability metric show improved records (from 90 to 34) % against round time when the WSN operates normally without cyber-attacks impact. At last, the best reliability measure has been achieved (from 100 to 36) % against round time has been obtained when applying the proposed anti-attack LSTM DL model.

Moreover, the life time metric has been evaluated for the same three cases of normal WSN model, WSN under cyber-attack effect, and WSN after employing the suggested anti-attack LSTM DL model as displayed in Fig. 10. Similarly, as might be observed from Fig. 10, the attained life time measure for our WSN secure model shows the lowest values (between 34 and 35) of active nodes against time rounds during the flood impact of a DDoS cyber-attack on the WSN environment. This dependability indicator then displays enhanced records (from 43 to 44) of active nodes versus round time when the WSN functions normally and is not impacted by cyber-attacks. Finally, using the suggested anti-attack LSTM DL model, the best reliability measure (from 49 to 50) active nodes against round time was found.

Table 4. Results comparison summary achieved for the simulated results.

Metric	Reliability	Life Time	Total Energy Consumption	WSN Life Nodes
Case Study	%	Active Nodes	Joules	Nodes
Normal WSN	90 to 34	43–44	3.6	45–50
Under DDoS Attack	70 to 26	34–35	Unknown	5–10
Proposed Anti-Attack LSTM DL Model	100 to 36	49–50	2	48–50
Overall Enhancement	30%	22%	55%	6%

Finally, results comparison summary might be achieved for the simulated results as outlined in Table 4.

5. Conclusions

To handle intrusions in the sensor network, a deep LSTM algorithm that leverages both short-term and long-term memory and works well with long-term dependencies was introduced in this study. Because mobile assaults might have erratic patterns, the model makes use of LSTM networks to handle these variations and offer security and dependability. Every time the regulated parameters are iterated, each node communicates its position and degree of movement, along with other significant information. Communication time, energy consumption each iteration, data received per node, the ratio of active to dormant nodes, and communication time between nodes were all significant metrics. These metrics aid in evaluating the model's stability under various conditions. In addition to concentrating on stability and security, these metrics enable us to forecast future node behaviours and the network's very dependable functioning. The performance metrics of wireless sensor networks were improved using the proposed attack prevention model based on LSTM deep learning technology by reducing node power consumption in the wireless sensor network by 55%, enhancing the lifetime of active nodes by 22%, and increasing the reliability of the sensor network by 30%. The network constraints were developed by training the layers of the proposed deep learning algorithm and continuously updating them to adapt to real-time changes.

Acknowledgments

The authors would like to thank the University of Technology, Iraq, for providing the necessary resources and support to complete this research.

Conflict of interest statement

The authors declare no conflict of interest.

Data availability

The datasets generated during and/or analyzed during the current study are available from the corresponding author on reasonable request.

References

[1.] D. Sethi, "Anapproachtooptimize homogeneousandheterogeneous routing protocols in WSN using sink mobility," *MAPAN*, vol. 35, no. 2, pp. 241–250, 2020, doi: 10.1007/s12647-020-00366-5.

[2.] S. Baskar, R. Selvaraj, V. M. Kuthadi, and P. M. Shakeel, "Attribute-based data fusion for designing a rational trust model for improving the service reliability of internet of things assisted applications in smart cities," *Soft Comput.*, vol. 25, no. 18, pp. 12275–12289, 2021, doi: 10.1007/s00500-021-05910-2.

[3.] O. Banimelhem, E. Taqieddin, and I. Shatnawi, "An efficient path generation algorithm using principle component analysis for mobile sinks in wireless sensor networks," *J. Sens. Actuator Netw.*, vol. 10, no. 4, 2021, Art. no. 69, doi: 10.3390/jsan10040069.

[4.] P. P. Jadhav and S. D. Joshi, "Atom search sunflower optimization for trust-based routing in internet of things," *Int. J. Numer. Model.*, vol. 34, no. 3, 2021, Art. no. e2845, doi: 10.1002/jnm.2845.

[5.] S. A. Hashim, E. K. Hamza, and N. N. Kamal, "Analyzing dynamic source routing protocol behavior in MANETs," *Ingenierie des Systemes d'Information*, vol. 29, no. 6, pp. 2357–2365, 2024.

[6.] S. Boyineni, K. Kavitha, and M. Sreenivasulu, "Mobile sink-based data collection in event-driven wireless sensor networks using a modified ant colony optimization," *Phys. Commun.*, vol. 52, 2022, Art. no. 101600, doi: 10.1016/j.phycom.2022.101600.

[7.] I. Slama, H. Jouini, A. Mami, and N. Boulajfen, "Wireless sensor network energy optimization in smart home using LEACH protocol: Comparative study with CTP routing protocol," *Int. J. Eng. Technol.*, vol. 7, pp. 147–154, 2018.

[8.] E. K. Hamza, E. K. Ibraheem, and S. J. Abou-loukh, "Improvement and analysis of polar codes based on new radio-deep learning," *International Journal of Intelligent Engineering and Systems*, vol. 18, no. 3, pp. 322–337, 2025.

[9.] D. P. Kumar, A. Tarachand, A. Chandra, and S. Rao, "ACO-based mobile sink path determination for wireless sensor networks under non-uniform data constraints," *Appl. Soft Comput.*, vol. 69, no. 3, pp. 528–540, 2018, doi: 10.1016/j.asoc..05.008.

[10.] L. A. Mohammed and A. M. Hasan, "Dynamic parameter adjustment in ant colony optimization for energy efficiency in wireless sensor network," *Journal of Engineering Science and Technology*, vol. 19, no. 6, pp. 2225–2249, 2024.

[11.] T. Elie, Z. Aline, and E. Tonye, "A reliable and efficient path discovery method for mobile sink based wireless sensor networks," *Int. J. Comput. Appl.*, vol. 176, no. 25, pp. 17–22, 2020.

[12.] V. Narawade and U. D. Kolekar, "ACSRO: Adaptive cuckoo search based rate adjustment for optimized congestion avoidance and control in wireless sensor networks," *Alex. Engi. J.*, vol. 57, no. 1, pp. 131–145, 2018, doi: 10.1016/j.aej.10.005.

[13.] Z. Mustafa and E. K. Hamza, "Enhancing indoor positioning accuracy using a hybrid Li-Fi/Wi-Fi system with deep learning support," *Engineering, Technology and Applied Science Research*, vol. 15, no. 2, pp. 21575–21585, 2025.

[14.] S. Yadav *et al.*, "Traffic and energy aware optimization for congestion control in next generation wireless sensor networks," *J. Sens.*, vol. 2021, 2021, Art. no. 5575802, doi: 10.1155/2021/5575802.

[15.] R. B. Pedditi and K. Debasis, "Energy efficient routing protocol for an IoT-based WSN system to detect forest fires," *Appl. Sci.*, vol. 13, no. 5, 2023, Art. no. 3026, doi: 10.3390/app13053026.

[16.] R. Ibrahem and E. Hamza, "The comparative analysis between distance deec and IOT DEEC based on network lifetime and energy consumption," *International Journal of Intelligent Engineering and Systems*, vol. 17, no. 5, pp. 142–157, 2024.

[17.] H. A. Tarish, "SS-FD: Internet of medical things-based patient health monitoring system," *Periodicals of Engineering and Natural Sciences*, ISSN: 23034521, vol. 9, no. 3, pp. 641 –651, 2021, Article, *Open Access,*, EID: 2-s2.0-85117194877, Tarish H.A., DOI: 10.21533/pen.v9i3.2220.

[18.] H. Almuslehi, A. A, F. M. Salbi, and A. J. Qasim, "Wireless sensor networks: Optimal routing strategy by bluetooth mesh low power nodes using ACO algorithm," *Journal of Theoretical and Applied Information Technology, 15th October*, vol. 99, no. 19, 2021, ©2021 Little Lion Scientific, https/www.jatit.org/volumes/Vol99No19/14Vol99No19.pdf.

[21.] A. Q. Raheema and H. A. Tarish, "Secure data transfer aware grouping technique for cloud-assisted Internet of things applications," *International Journal of Communication Systems*, ISSN: 10745351, vol. 36, no. 1, 2023, Article, EID: 2-s2.0-85070746264, DOI: 10.1002/dac.4129.

[20.] Z. Zhang, Y., X. Li, and H. Wang, "Hybrid deep learning and blockchain for secure wireless sensor networks in IIoT," *IEEE Internet of Things Journal*, vol. 9, no. 4, pp. 5678–5692, 2022, https://doi.org/10.1109/JIOT.2022.3156789.

[21.] S. Khan, A. N. Alvi, and A. Rehman, "Federated learning for privacy-aware anomaly detection in healthcare WSNs," *IEEE Sensors Journal*, vol. 22, no. 10, pp. 9210–9225, 2022, https://doi.org/10.1109/JSEN.2022.3171234.

[22.] W. Li, M. Zhao, and L. Sun, "GAN-based adversarial defense for reliable smart grid WSNs," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 3, pp. 2105–2118, 2023, https://doi.org/10.1109/TII.2023.3267890.

[23.] J. Wang and Y. Chen, "Lightweight autoencoder-based anomaly detection for military WSNs," *IEEE Communications Letters*, vol. 27, no. 6, pp. 1459–1463, 2023, https://doi.org/10.1109/LCOMM.2023.3287654.

[24.] F. Al-Turjman, H. Zahmatkesh, and L. Mostarda, "GNN-based trust management in smart city WSNs," *Future Generation Computer Systems*, vol. 141, pp. 512–525, 2023, https://doi.org/10.1016/j.future.2023.01.020.

[25.] K. Rana, N. Kumar, and A. Singh, "Secure transformer-based data aggregation in agricultural WSNs," *Computer Networks*, vol. 234, p. 109876, 2024, https://doi.org/10.1016/j.comnet.2024.109876.

[26.] R. Yadav and P. Singh, "Energy-efficient spiking neural networks for WSN anomaly detection," *IEEE Sensors Journal*, vol. 24, no. 5, pp. 6789–6801, 2024, https://doi.org/10.1109/JSEN.2024.3356721.

[27.] X. Chen, T. Wu, and R. Zhang, "Edge AI with differential privacy for industrial WSNs," *IEEE Internet of Things Journal*, vol. 11, no. 2, pp. 1892–1905, 2024, https://doi.org/10.1109/JIOT.2024.3356789.

[28.] S. Gupta, P. Sharma, and H. Kim, "Quantum machine learning for secure defense WSNs," *IEEE Transactions on Quantum Engineering*, vol. 6, no. 1, pp. 1–15, 2025, https://doi.org/10.1109/TQE.2025.3367123.

[29.] M. Liu, Y. Zhou, and Q. Zhang, "Explainable LSTM models for healthcare WSN reliability," *Artificial Intelligence in Medicine*, vol. 155, p. 102789, 2025, https://doi.org/10.1016/j.artmed.2025.102789.

[30.] Z. Mustafa and E. K. Hamza, "Nhancing indoor positioning accuracy using a hybrid li-fi/wi-fi system with deep learning support," *Engineering Technology and Applied Science ResearchOpen source preview*, vol. 15, no. 2, pp. 21575–21585, 2025.

[31.] S. A. Hashim, E. K. Hamza, and N. N. Kamal, "Analyzing dynamic source routing protocol behavior in MANETs," *Ingenierie Des Systemes D InformationOpen source preview*, vol. 29, no. 6, pp. 2357–2365, 2024.

[32.] R. Ibrahem and E. Hamza, "The comparative analysis between distance DEEC and IOT DEEC based on network lifetime and energy consumption," *International Journal of Intelligent Engineering and SystemsOpen source preview*, vol. 17, no. 5, pp. 142–157, 2024.

[33.] E. K. Hamza, L. A. Mohammed, and A. M. Hasan, "Dynamic parameter adjustment in ant colony optimization for energy efficiency in wireless sensor network," *Journal of Engineering Science and TechnologyOpen source preview*, vol. 19, no. 6, pp. 2225–2249, 2024.

[34.] E. K. Hamza, S. S. Husain, H. M. Jasim, . . . A. J. Humaidi, and H. M. Ahmed, "Synergetic control design to controlled PWM buck power converter," *Icetas 2024 9th IEEE International Conference on Engineering Technologies and Applied SciencesOpen source preview*, 2024.

[35.] E. K. Hamza and S. N. Jaafar, "Nanostructured electrode materials in bioelectrocommunication systems," *Advanced Nanomaterials and Nanocomposites for Bioelectrochemical SystemsOpen source preview*, pp. 187–204, 2023.