



OPEN

Next generation AI powered framework for autonomous energy optimization and real time anomaly detection in IoT driven wireless sensor networks

M. Parameswari¹✉, Nancy P² & R. Jeya Malar¹

Due to the proliferation of Internet of Things (IoT)-based Wireless Sensor Networks (WSN) technology in different phases of various sectors, comprehensive solutions related to energy consumption and security are indispensable. However, in traditional methods for energy optimization and anomaly detection in WSNs there are certain issues: An inability to process real-time data, unavailability to extend the adaptation to behave and respond with dynamic network conditions, and poorly suited for continuously evolving anomalies. These limitations contribute to the decrease of the system's overall performance and dependability in actual big and complicated sociotechnical networks. To overcome these challenges, this research presents LEGO-WSN (Long Short-Term Memory (LSTM) with Attention Mechanism and Genetic Algorithm (GA) Optimization for WSNs), an intelligent solution for improving energy efficiency and real-time faulty node identification of WSNs. The proposed LEGO-WSN combines GA and LSTM to enhance energy optimization and improve the detection of anomalies. The work discussed here introduces a novel approach called LEGO-WSN, which incorporates LSTM with the help of an attention layer along with a Genetic Algorithm for the operation of fault diagnosis in anomaly detection. The GA improves the network transmission parameters and plans the sensor's operations, while the LSTM structure, complemented by attention mechanisms, identify the features of time series to encode blackhole attacks. The data set for the purpose of this study can be obtained from Kaggle and is a real life WSN data with variety of different environmental and network conditions. The impact of the proposed GA-LSTM model is measured in terms of energy consumption and real-time anomaly detection while also aims at flexibility in terms of the network environment in which it is implemented. The results show substantial enhancements in energy efficiency, with a 20% reduction in energy consumption, and high accuracy in anomaly detection, achieving 99% accuracy, 98% precision, and 99% recall. LEGO-WSN demonstrates a novel, scalable, and reliable solution for optimizing WSN performance while enhancing security and energy efficiency.

Keywords Next-generation AI, Autonomous energy optimization, Real-time anomaly detection, IoT-driven wireless sensor networks, Artificial intelligence, Energy efficiency

WSN consist of several numbers of sensor nodes which are small in size, inexpensive and low power, having multiple functionalities and they transmit data to each other through wireless and short range. Here, the placement of the authorizer sensor nodes was arbitrary in the needed area for the monitoring and detection work according to the applications¹. WSN's is roughly defined by some characteristics like energy, load, power, coverage, delay, and so on, of these characteristics need to be optimized in order to guarantee the quality of service. In real implementation, these attributes are complementary so they must be optimized hence improvement of their performance in working conditions will be enhanced². New technologies in wireless systems enable the creation of low power sensor nodes which are referred to as motes that operate through radio signals linked in a WSN³. WSNs are networks of self-sufficient nodes with embedded sensors and are commonly used for

¹Department of Computer Science and Engineering, Kings Engineering College, Chennai, India. ²Department of Computing Technologies School of Computing, SRM Institute of Science and Technology, Kattankulathur, Chengalpattu, Tamil Nadu 603203, India. ✉email: paramuphd2011@gmail.com

tracking or detecting objects, conditions, environment, or physical events including heat and humidity and noise⁴. However, one of the biggest issues with WSNs is the dependability of these sensor nodes; for example, it may be practically impossible to recharge or replace the batteries of multiple thousands of nodes deployed in a remote location⁵. Due to the limitations of battery power, only energy conservative computations and low-power communication systems can be used⁶. Data fusion and relaying are two successful approaches which can minimize the energy usage in WSNs because it removes the need for periodic repetition of data collection and also has a lesser infrastructure cost⁷. Thus, the suggestion and application of energy efficient routing protocols are central for enhancing WSN performance and reliability. The application of WSN for data communication can be enhanced effectively with an optimum management of available resources, greatly meeting the requirements of data transfer as well as saving energy⁸. New data analysis and continual tracking are beneficial in enhancing the efficacy and dependability of energy systems due to Artificial Intelligence⁹.

WSNs being extensively flexible and applicable to a broad spectrum of domains like environmental and climatic changes, healthcare, smart cities, warfare, and industry applications¹⁰. With the trend towards establishing the connectivity of every item in the world known as the Internet of Things today, their capacity for collecting, processing, and relaying data from remote regions and hard to access areas makes them invaluable¹¹. The various sensor nodes used in these networks, being low-cost and power efficient, requires to be designed in such a way that it can operate satisfactorily in diverse environment¹². Nevertheless, several factors pose challenges to the effectiveness of the WSNs and also their durability¹³. For example, in case of sensor nodes, the network topology is inherently large and constantly evolving due to node failure, mobility of nodes and interference¹⁴. These problems result in high energy use, unpredictable device interaction, and network overcrowding. Another major problem is security which in the blackhole attack can cause significant disruptions to the networks functioning, including data loss, energy depletion and misunderstandings between nodes. Solutions to these problems require the design of robust and robust adaptable protocols that are capable of overcoming these challenges while at the same time, minimizing energy consumption¹⁵.

High system throughput and minimal response times are crucial in various applications, including remote patient monitoring or surveillance networks of armies¹⁶. For example, in medical WSNs, the focal concentrations are to capture and transmit vital signs for a constantly high number of patients without much delay and, consequently, an anomaly in the operation of the network may pose a threat to patients' lives. Therefore, there is a need to provide better quality guarantee with respect to the signal transmission and energy consumption as well as security against possible attacks¹⁷. In the context of wireless sensor networks, a blackhole attack occurs when a malicious node consumes all network traffic without letting it to reach its destination¹⁸ as shown in Fig. 1. Data loss, performance degradation in the network, and vulnerability to security are the primary results of this kind of attack¹⁹. The proposed approach of using LSTM networks with attention mechanisms is significant in contrast to traditional anomaly detection methods that often depend on simple statistical models or machine learning algorithms. Long-term dependencies are captured by the LSTM, and through the attention mechanism, focus is placed on the most relevant features to make accurate detection of anomalies such as blackhole attacks in dynamic WSN environments. This approach can be adaptive to the changing nature of WSNs and hence improve detection performance while being energy efficient.

Problem statement

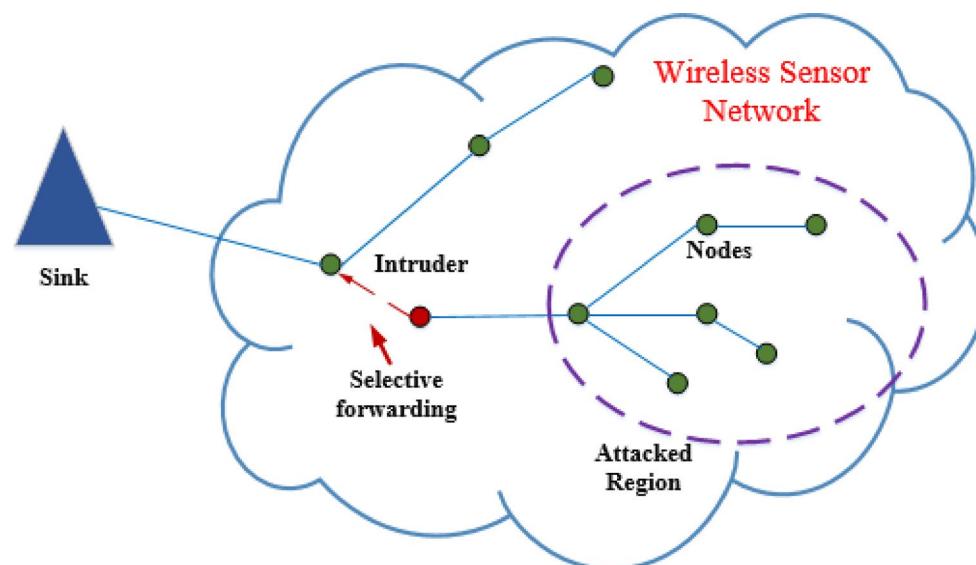


Fig. 1. Blackhole attack.

- Most existing energy optimization methods struggle to scale effectively in large and dense IoT environments, such as smart cities, due to the increasing number of interconnected devices.
- Many intrusion detection systems exhibit high false alarm rates, reducing their reliability in detecting anomalies, including zero-day attacks.
- Existing routing and optimization protocols often fail to balance energy efficiency and network performance, leading to premature depletion of battery-powered IoT devices²⁷.
- Current anomaly detection approaches are not lightweight or fast enough to perform real-time detection, which is critical for maintaining system efficiency and security.
- Continuous data flow optimization methods often neglect runtime anomalies or fail to bypass faulty nodes efficiently, resulting in higher energy consumption²².

Highlights of the proposed study

- A novel hybrid framework combining LSTM with attention mechanism and GA for blackhole attack recognition and energy optimization in IoT-driven WSNs.
- The proposed method detects blackhole attacks in real-time, improving network security by identifying malicious nodes and enhancing fault diagnosis in WSNs.
- The integration of GA optimizes energy consumption, enhancing the overall sustainability and efficiency of the WSNs by reducing energy usage during data transmission and routing.
- The method is scalable across different network sizes, ensuring its applicability in both small and large-scale IoT systems.
- The study emphasizes efficient data transmission even in the presence of blackhole attacks, maintaining the integrity of communication across nodes.

Related works

Humayun et al.²⁰ propose energy optimization is one of the challenges in smart cities, and this paper focuses on the problem area and integrates advanced technologies such as IoT, 5G, and cloud computing. The model proposed here can be implemented in energy saving in smart homes and smart cities like lampposts, structure and posters, smart homes and smart parking. Smart city electrical appliances will have IoT sensors to monitor movements and respond to commands over the network. All data communication between communication channels and the cloud will be transported through 5G technology where cloud technology will be used to store and access information optimally. Mathematical modeling was used to assess the suggested model and the outcomes designated that it has potential to enhance smart cities energy use.

The study by Nagaraju et al.²¹ presents an energy capable secure routing solution for IoT applications in integrated WSNs. The scheme suggest a secured path for the transferring of the IoT data over the nodes through the various energy sensors using the multipath link routing session method. TEEN variants employed in hybrid ad hoc network are hybrid based TEEN that improves the energy and network lifetime, ubiquitous data storage protocol that improves the data storage ability. Based on the results obtained during the simulation of the proposed protocol and comparing it with two other present routing protocols, it has been found that some performance parameters like throughput, energy efficiency, end-to-end delay, storage and network life and data storage capacity has also increased. The major design concern in HWSNs therefore is security provision in End-to-End communication.

Luo et al.²² describes the Mathematical Programming Model for improving the runtime characteristics of continues data-flow applications in IoT context. It uses a simple anomaly detection algorithm to predict the reliability of nodes and incorporates this reliability into an optimisation loop to predict the overall task delay. The-energy optimization problem for the continuous data flow with latency constraints is posed as a mixed integer nonlinear programming problem and a max flow algorithm based on block coordinate descend approach is described as well. The above strategy has only been used in the simulation environment, if applied the new strategy is more energy consumption efficient than the benchmark strategy. At the same time there is outlined the issue of the subsequent improvement of energy utilization efficiency in IoT applications.

Sarwar et al.²³ discuss smart environment was brought about by the IoT which has transformed human activities, but these are accompanied by threats to security and privacy. While many IDS has been proposed for IoT networks, the problem space has only grown and variants of optimization such as PSO face limitations. Individuals utilize the SBPSO to implement feature collection for this paper, and propose an improved method, the IDSBPSO method, with the addition of a dynamic search space reduction approach, as well as the integration of dynamic parameters into SBPSO. The proposed IDS was aimed to detect or identify different sort of high risk data traffic in IoT networks. Experiments were performed using IoTID20 and UNSW-NB15 datasets, and it has been seen that the proposed model increases its accuracy besides having fewer user-input features and a remarkably low computational cost as well as predicting time as compared to the basic PSO model.

Ahmad et al.²⁴ shows categories of IoT architecture have expanded over the years to launch more connected devices and input/output data. The other issue that have to consider is the security as the threat of the new zero-day cyberattacks are real. Network-based IDS or NIDS can be efficient solution for protection of IoT networks as they operate with network traffic. However, a recent NIDS is effective only in detecting anomalies with a high FAR. This paper outlines a mechanism for fast abatement of IoT network anomaly detection utilizing MI and DNN, which is proposed. When the 35 best numerical features with MI instead of 80 numerical features were used, performance decreased, and complexity was decreased. The detection accuracy had further been improved

by 0.99 – 3.45% at an aggregate level using DL-based models, and for the top five categorical and numerical features only.

Samani et al.²⁵ evaluate the real data resulting from hundreds of networked digital PIR occupancy sensors installed in the LED luminaires of a moderately recent IoT-BEMS in a large California building. A technique for detecting deviations in such a data flow. Equally, make use of the outputs in entering the building efficiency to develop a window those which can provide demand response services. Further, they also offer the load forecasting of the lighting load for this building using deep neural model that is developed this dependable predictable performance. From the analysis, the authors demonstrate that this approach can ensure 30% load shedding to the lighting fixtures.

Lydia et al.²⁶ propose green IoT is already affecting to other domains like health care systems, smart city and transportation system to better the dissipation. However, how much has environmental decrement been reduced in green media networks is still a research question and a commercial issue in the 21st century. This paper provides DL-based detection of anomalies for IoT applications along with green energy efficient routing. The procedure to restrict data in the experimental settings is as follows: GEER-DLAD, for the error lossy compression of data communication, and the MSO for route selection. DLAD process thus entails the use of the RNN-LSTM model for the function of anomaly detection on the IoT communication network. Thus, the generic experimental enhancement strategy for improving both the energy efficiency of the GEER-DLAD model and the model's detection capability was established.

Sivakumar et al.²⁷ discuss industry 4.0 which is also referred to as the fourth industrial revolution is characterised by technologies such as IoT Big data and AI amongst others. In industrial applications especially where there is increased usage of connected devices, the energy efficiency of the sensors takes the central stage. In this study, a new energy optimization model for the sensor nodes in the context of Industry 4.0 considering energy efficiency and conservation and energy harvesting is proposed. It consists of dynamic power management, scheduling, and harvesting methods which thus reduces power utilization density to meet the required performance. It is predicted that the proposed framework would improve the performance of the sensor node to make operation more efficient and affordable.

Revanesh et al.²⁸ design of WSNs has been focused on how to prolong the lifetime of the WSNs through reasonable utilization of energy. Such models require fewer numbers of sensors to measure the physical properties of environment, while consuming more power in relation to the resulting readings quality. The major disadvantage of WSNs is in areas that require monitoring or tracking because of power supply in batteries. Several routing protocols have emerged to solve this problem among them being; but where or how to cover the network period holding in mind the capacities of sensors is still a question. The research also identifies some neural networks that include LEACH and EESR since they enhance network performance and reliability. EESR implements from the physical model an improved Levenberg–Marquardt Neural Network thus improving energy efficiency. It is generalizable that IDS developed based on ANN can detect the anomalous movements based on the optimum feature selection.

Saheed et al.²⁹ discuss critical infrastructures use SCADA systems for supervision and command from a distance, however, classic intrusion detection systems are ineffective against various cyber threats. Even today's traditional security measures such as firewalls and anti-virus programs are ineffective for protecting SCADA systems. To tackle these problems, a novel ELM is suggested for intrusion identification in SCADA frameworks from the MSU gas pipeline and water utility, and also the UNSW-NB15 datasets. Data preprocessing similarly applies unity normalization, and feature extraction applies PCA. GWO is applied for optimization of classifiers including bagging, stacking, Adaboost, Naive Bayes and Support Vector Machine. The results suggest that the use of PCA + GWO enhanced performance by strengthening the SCADA system.

Ramalingam et al.³⁰ discuss the issue of energy efficiency in WSNs, in which continuous sensor consumption rapidly depletes node batteries. The suggested work develops a hybrid model based on Fuzzy system with a combination of Adaptive Sailfish Optimizer (ASFO) to select cluster head and an enhanced Elephant Herd Optimization to use shortest-path routing. The approach implemented in MATLAB and compared with IABC-C, GA, PSO, and HCCHE, the method enhances QoS metrics, with a packet delivery ratio of 99.8, a latency of 1.12 s, throughput of 98 bps, an energy usage of 10.90 mJ, a network lifetime of 5400 cycles, and a packet loss ratio of 0.6%. Limitations are that it is based on simulation data, and integration of heterogeneous WSN environments might be problematic regarding scalability.

Dhanasekaran et al.³¹ discuss the issue of malware identification in 5G networks, where APIs, calls, and SMS make it difficult to detect an attack. This proposed work proposes a lightweight CNN with a sequential LSTM layer, which is trained on the Malimg dataset, to successfully classify malware. Results show high performance with an accuracy of 99.8% and F1-score of 0.9925, which is 12.8% more accurate and 14% higher F1-score than the current models. The strategy emphasizes the deep learning promise of safe 5G and IoT set-ups. These are limited by the fact that it refers to a single dataset and might have certain difficulties in real-time implementation in heterogeneous network environments.

The reviewed literature Table 1 emphasizes the importance of energy optimization and security in IoT-based systems, especially in smart cities, Industry 4.0, and critical infrastructures. Techniques such as routing protocols, anomaly detection, and feature selection have been proposed to improve energy efficiency and system reliability. Hybrid protocols in heterogeneity WSN for routing secure, mathematical models, particularly optimization of energy using energy efficiency in continuous flows in data, and DL-based anomaly detection in green networks of IoT. Sophisticated approaches like IDSBPSO, GEER-DLAD, hybrid models based on ensemble technique and its applications for improvement and optimizing energy use while advancing intrusion detection techniques. These studies demonstrate improvements in performance metrics such as energy efficiency, network lifetime, and anomaly detection accuracy, which underscores the importance of integrating security and energy management in IoT systems. Current research of energy optimization, routing, and anomaly detecting in IoT

References	Focus	Key Findings	Limitations
Humayun et al. ²⁰	Energy optimization in smart cities integrating IoT, 5G, and cloud computing	Model enhances energy use in smart homes, streetlights, smart parking; cloud stores data efficiently; 5G enables fast communication	Primarily simulation-based; real-world deployment not tested
Nagaraju et al. ²¹	Secure and energy-aware routing in IoT-enabled WSNs	TEEN variants and multipath routing improve energy efficiency, throughput, storage, network lifetime	Security concerns remain in end-to-end communication; scalability not tested
Luo et al. ²²	Energy optimization for continuous data-flow applications	Mixed integer nonlinear programming with max-flow algorithm reduces energy consumption in simulation	Only tested in simulation; real-world efficiency may differ
Sarwar et al. ²³	IDS for IoT networks using optimized PSO (IDSBPSO)	Improved anomaly detection accuracy, low computational cost, fewer features required	Limited to IoT20 and UNSW-NB15 datasets; may not generalize to other datasets
Ahmad et al. ²⁴	NIDS for IoT anomaly detection using MI and DNN	Reduced feature set improves detection accuracy by 0.99–3.45%	High false alarm rate possible; dataset-specific performance
Samani et al. ²⁵	Load forecasting and deviation detection in IoT-BEMS	Achieved 30% load shedding in LED luminaires using DNN-based model	Limited to one building; may not generalize to other environments
Lydia et al. ²⁶	Green IoT routing with DL-based anomaly detection	GEER-DLAD with LSTM improves energy efficiency and detection capability	Limited experimental settings; real-world deployment challenges
Sivakumar et al. ²⁷	Energy optimization in Industry 4.0 sensor nodes	Dynamic power management, scheduling, and harvesting improve energy efficiency	Applicability to heterogeneous industrial networks not fully validated
Revanesh et al. ²⁸	Prolonging WSN lifetime via neural networks (LEACH, EESR)	Improved energy efficiency and reliability using LM-NN; reduces number of sensors needed	Battery-powered nodes still limited; monitoring in large-scale WSNs challenging
Saheed et al. ²⁹	IDS in SCADA systems using ELM + PCA + GWO	Optimized classifiers improve detection performance in SCADA systems	Limited to MSU gas pipeline and water utility datasets; may not generalize
Ramalingam et al. ³⁰	Hybrid energy-efficient WSN routing (Fuzzy + ASFO + EHO)	QoS metrics improved; PDR 99.8%, latency 1.12s, throughput 98bps	Simulation-based; heterogeneous WSN scalability not tested
Dhanasekaran et al. ³¹	Malware detection in 5G using CNN-LSTM	High accuracy (99.8%) and F1-score (0.9925); outperforms existing models	Single dataset; challenges in heterogeneous real-time network deployment

Table 1. Review of existing Techniques.

and WSNs typically have constraints of processing real time data. The simulation-based approaches of Luo et al.²² and Ramalingam et al.³⁰ are only limited to simulation approaches, whereas the methods by Lydia et al.²⁶ and Saheed et al.²⁹ are confined to in-experimental or offline systems. These drawbacks prevent their use in dynamic networks where decisions made on time are of the essence. The proposed GA-optimized LSTM with attention mechanism fills this gap by making the real-time routing and detection of anomalies efficient, at the same time making the network more energy efficient and stable. Unlike the previous works that concentrate on single factors such as energy optimization, routing, or anomaly detection, the proposed method combines GA-based optimization with LSTM and attention to concentrate on both energy efficiency and anomaly detection. As opposed to a majority of the extant literature, it trades performance of routing, accuracy of detection, and computational efficiency in dynamically WSN environments. The proposed research presents a new LEGO-WSN paradigm that sequentially applies LSTM with Attention for anomaly detection and optimization using Genetic Algorithm for energy-aware routing. Differently from other existing research that addresses security and energy efficiency independently, the framework innovatively integrates real-time detection of blackhole attacks with dynamic routing reconfiguration to guarantee both network lifespan and robustness against malicious disruptions in WSNs.

Proposed AI powered framework for autonomous energy optimization and anomaly detection in WSN

The proposed methodology integrates LSTM with an Attention Mechanism and GA to enhance energy optimization and detect blackhole attacks in WSNs. Initially, data preprocessing steps such as handling missing data, normalization, and splitting the dataset into training and testing sets are performed to ensure data quality and uniformity. It is applied to the LSTM model with attention enhancement for real-time anomaly detection. The LSTM layers used in this work are specifically designed to extract temporal patterns and dependencies from time-series sensor data. On its part, the attention mechanism identifies critical features by focusing on crucial time steps. With all these, this combined framework achieves high accuracy in detection of blackhole attacks which distinguish malicious behavior from normal operations. GA optimizes energy efficiency in the network. It starts with the initialization of a population by routing solutions, followed by fitness evaluation based on energy consumption, data transmission efficiency, and path length. Crossover and mutation operations refine solutions iteratively, ultimately selecting the optimal routing paths to ensure minimal energy usage while maintaining network performance. The outputs from the LSTM and GA modules are integrated, enabling real-time decision-making. The method shows better anomaly detection and energy optimization providing a robust framework for the operation of WSNs securely and efficiently.

The Fig. 2 presents the LEGO-WSN as a framework for anomaly detection in WSNs. Data is gathered from the network and then cleaned up and again divided into training and testing sets. The training data is passed through LSTM with attention where the net learns to attend the training data to find patterns. The output of each LSTM layer is then fine-tuned using a genetic algorithm in an effort to increase power efficiency. Moreover, new data is classified as blackhole or normal using the optimized model.

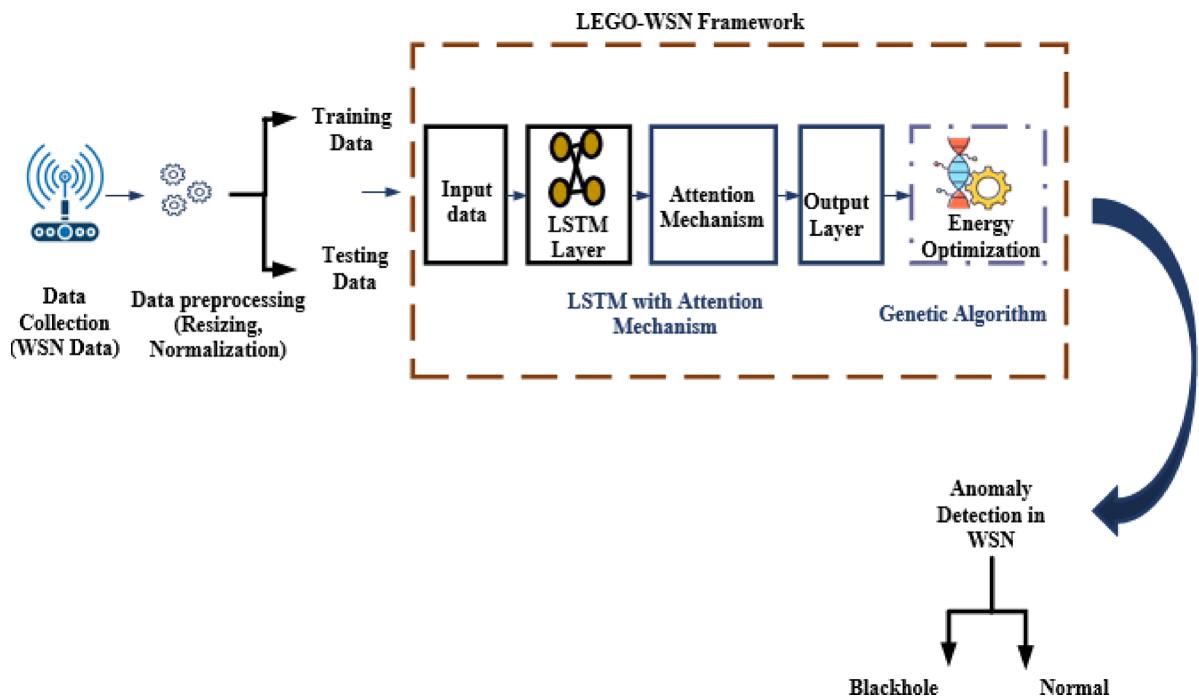


Fig. 2. Proposed framework.

Data collection

The proposed approach collects data from a WSN, which monitors different environment parameters including temperature, humidity, as well as energy consumption. Each entry includes more than 374,662 records and incorporates features that include node status, distance to the cluster head, data transmission metrics, as well as energy consumption, and are labeled either “Normal” or “Blackhole” attacks for real-time fault diagnosis. It processes the data to deal with missing values, normalize the features, and split the dataset into training and testing for model development and evaluation³².

Data pre-processing

To prepare the dataset for model training, a number of data pre-processing approaches have been applied in the study on energy optimization and blackhole attack detection in IoT-driven WSNs. First, in handling missing data, a gap in the dataset was identified and addressed. These kinds of gaps may result due to sensor failure or during transmission. Missing values are imputed through techniques such as mean, median, or mode imputation for numerical features in order to keep the data complete and usable.

$$s_{imputed} = \frac{\sum_{i=1}^n s_i}{o} \quad (1)$$

In Eq. (1) $s_{imputed}$ is the imputed value for the missing data point. s_i are the observed values in the feature. o is the total number of observed values in the feature.

Normalization was then applied to scale the numerical features, including “Dist_To_CH” and Consumed Energy, to a common range so that features with larger scales were not dominating the model performance, and algorithms such as LSTM, which are sensitive to scaling of features to perform optimally. The Min-Max scaler is typically used in normalizing data between 0 and 1. In Eq. (2).

$$v_{normalized} = \frac{v - v_{min}}{v_{max} - v_{min}} \quad (2)$$

Finally, the dataset is divided into training and testing sets to ensure that the model has been trained on a significant portion of the data usually 80% and is validated on unseen data 20% to test its generality. The splitting ensures fair evaluation of the model since reliability in metrics for anomaly detection as well as energy optimization performance. Thus, all these pre-processing together improve the model’s strength in effective blackhole attacks detection.

LSTM for Blackhole attack detection in WSNs

This study uses LSTM networks with an Attention Mechanism to identify anomalies, like Blackhole attacks, in WSNs. LSTM is a type of RNN which has been developed to remove the problem of vanishing gradients in traditional RNNs, especially when dealing with long-term dependencies in time-series data. LSTM is

particularly suited for use in tasks involving sequential data, making it the optimal choice for anomaly detection for time-series sensor data by WSNs. These networks cause abnormal patterns in network metrics such as packet delivery ratio, energy consumption, and data transmission behavior, thus disrupting normal communication. LSTM models are effective in identifying these anomalies by learning temporal dependencies and recognizing deviations from normal network behavior over time. Diagnosis of faults is an important task in WSNs, especially when abnormalities such as Blackhole attacks occur. These assaults take place when an unauthorized node provides information that it has the shortest path to a target and then alters and eliminates packets instead of passing them on. This results in poor throughput performance which is characterised by low PDR, high latency and high energy consumption.

Blackhole attacks are modeled as real-time anomalies to the context that encompasses fault diagnosis in this study. To observe the sensor nodes periodically and look for behavioural anomaly that is symptom of an attack, a DL model including LSTM networks and an Attention Mechanism is implemented. LSTM application results are effective because it is highly capable of learning the temporal relations inherent in daily sequential data and that are more capable of spotting minor anomalies in network behavior over time is shown in Fig. 3. The Attention Mechanism improves this process by paying attention to such features as a significant drop in PDR level or increased energy consumption which are typical in Blackhole attacks. These features includes energy consumption, distances between each vector to the cluster heads and transmission rates from the cluster heads which are detected using the trained LSTM model with Attention Mechanism.

These are energy consumption, distances between each vector to the cluster heads and transmission rates from the cluster heads which are detected using the trained LSTM model with Attention Mechanism. This method not only quickly identify Blackhole attacks, but also allows for timely fault diagnosis in a way that causes minimal disruption to the network. Key steps in identifying Blackhole Attacks include input data representation, which captures patterns that can reflect the presence of Blackhole attacks in sensor network metrics like “Is_CH, Dist_To_CH, Consumed Energy, and Data_Sent_To_BS”. The feature learning process used in this work aims at identifying informative features for normal network traffic and Blackhole attacks. In WSNs, Is_CH feature represents Boolean values such as whether a node is a Cluster Head or not and “Dist_To_CH” represents distances and spatial relations. These deviations may have arrests in routing that deviate from standard distances. Energy_consumed is the amount of energy which is consumed by node and “Data_Sent_To_BS” is the magnitude of forwarded data. These features are passed through the LSTM model in a sequential manner to pick up on temporal dependencies and spatial behaviour that are inherent in network activity so as to effectively capture the amount of temporal-spatial information in the extracted features accurately.

The four main components of LSTM units are the Forget Gate, which discards previous cell state information; the Input Gate, which adds new information; the Output Gate which determines the current time step's output, which is then passed to the next time step; and the Hidden State, which is the output at each time step.

$$e_t = \sigma(g_f \cdot [c_{a-1}, v_a] + s_e) \quad (3)$$

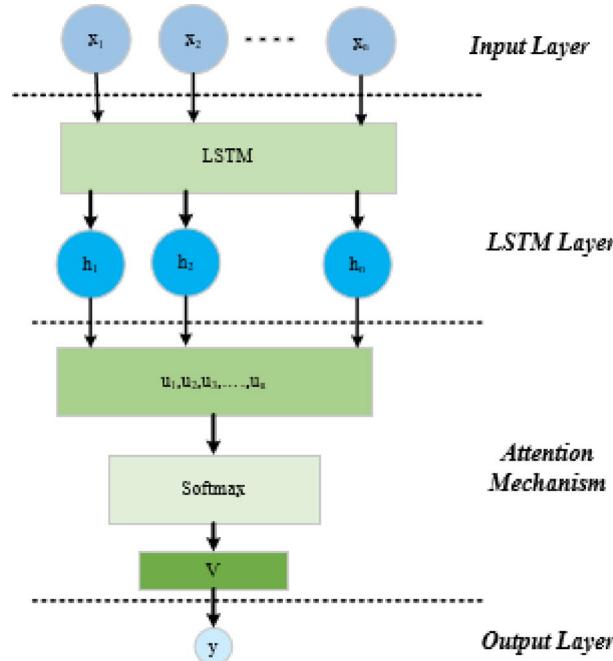


Fig. 3. LSTM with attention mechanism architecture.

In Eq. (3) e_t is the forget gate output at time t , σ is the sigmoid activation function, g_f is the weight matrix associated with the forget gate, c_{a-1} is the previous hidden state, v_a is the current input vector at time t . s_e is the bias term.

$$p_t = \sigma(g_p \cdot [c_{a-1}, v_a] + s_p) \quad (4)$$

In Eq. (4) p_t is the input gate output at time t . g_p is the weight matrix associated with the input gate.

$$\hat{l}_t = \tanh(g_l \cdot [c_{a-1}, v_a] + s_l) \quad (5)$$

In Eq. (5) \hat{l}_t is the candidate cell state at time t . g_l is the weight matrix associated with the candidate cell state. Update the cell state are represented in Eq. (6). Where l_t is the cell state at time t .

$$l_t = e_t \cdot l_{t-1} + p_t \cdot \hat{l}_t \quad (6)$$

$$u_t = \sigma(g_u \cdot [c_{a-1}, v_a] + s_u) \quad (7)$$

In Eq. (7) u_t is the output gate at time t , g_u is the weight matrix associated with the output gate.

$$d_t = u_t \cdot \tanh(l_t) \quad (8)$$

In Eq. (8) d_t is the hidden state at time t , l_t is the cell state at time t , u_t is the output gate at time t . The hidden state d_t is the output of the LSTM unit at time step t , which is used as input for the next time step or the next layer. A feature of LSTM networks is the ability for storing and reconstructing information over long sequences, therefore it makes them perfect for handling time-series data such as those obtained from WSN sensors.

Input Transformation: The feature vector of every time step (p_t) is passed to the LSTM. This vector contains all metrics. **Hidden State Representation:** The hidden state of the LSTM is a dynamic representation of learned features at time t . This state recursively updates the new information while maintaining the context of prior observations. **Adaptive Weighting:** The model learns which features are most important for distinguishing normal from anomalous behavior by adjusting the weight matrices (g_p, g_l, g_f) during training. It learns to identify the irregularities that characterize Blackhole attacks by analyzing features like energy consumption and routing patterns. Though LSTMs are good in handling sequential data, the problem of focusing on the most significant parts of the string is challenging when the string is long. To counter this, Attention Mechanism is incorporated into the LSTM network used for the system. The attention mechanism can help the model give more attention to segments of the input sequence that is relevant for the task at hand, which is a crucial element in identifying Blackhole attacks and in minimizing energy consumption in WSNs. The attention mechanism makes use of a pointer and makes much of the input sequence have more importance than others. The attention mechanism works by assigning different weights to different parts of the input sequence. It allows the network to focus more on the relevant parts of the sequence and less on the irrelevant parts, essentially “attending” to the most important information at each time step.

For each time step t an attention score α_t is computed. This score determines the importance of the current input with respect to the output. The attention score is calculated as Eq. (9).

$$\alpha_t = \text{softmax}(a_t) \quad (9)$$

Where a_t is the attention score for the $t - th$ time step, calculated as Eq. (10).

$$a_t = w_a \cdot [c_a, c_{a-1}] + s_a \quad (10)$$

Where w_a is the weight vector, and s_a is the bias term. Once the attention scores α_t are computed, they are used to weight the hidden states at each time step. The weighted sum of hidden states is then used to compute the final output for the current time step:

$$Z_t = \sum_{i=1}^T \alpha_i d_i \quad (11)$$

In Eq. (11) T is the total number of time steps, and d_i is the hidden state at the $i - th$ time step. This process helps the model focus on the relevant parts of the sequence, thus improving the performance of anomaly detection and energy optimization.

The final output is calculated based on the combination of weighted sums of hidden states and outputs from the LSTM network. Thus, the overall focus would be more on important parts of the input sequence. It enables the data processing sequentially to have timely detection of anomalies. Thus, the proposed mechanism is used for reliable security of a dynamic IoT network. The approach mainly makes use of feature learning as well as temporal analysis while detecting Blackhole attacks in WSNs. Thus, temporal analysis indicates that the model is able to analyze WSN node behavior during some specific time period to find out the unusual activity. Blackhole attacks can also be of temporal features that show that at some time step or continuously at some subsequent time steps, a node behaves differently than before. Sequential data processing LSTM also performs a pass on the network data one time step at a time. For instance, a series of values of energy consumed by a node at different time instants ($[x_1, x_2, \dots, x_t]$) are taken as inputs to the LSTM in order to learn how such a metric change. Blackhole attacks create distinctive patterns in node metrics over time.

PDR is a sharp or long-term decline of the amount of information delivered to the base station. Energy Consumption: Abnormal energy consumption behaviors intended by the intention of deceitful nodes to response to confirmed data. Routing Changes: Due to its excessive selection as a Cluster Head or its disturbing behavior on the routing tables. For example, a Blackhole attack might cause a node to intercept and drop packets which would mean that packets are being dropped over a sequence of time steps. LSTM analyze such deviations over the sequence to raise alarm of the attack. Dynamic Anomaly Detection: These decrease and increase values compared with the present state, that the model termed as h_t , are compared with patterns of the past stored in the memory cells of the LSTM and are categorized as an anomalous state. Threshold-Based Classification: The outcome of this LSTM layer is passed directly into a dense layer that actually gives the anomaly scores. If the node utilization crosses preset limit, then a node is considered to be under attack. The Attention Mechanism focuses on the most critical time steps or features in the sequence, improving the detection of subtle anomalies. Alignment Scores (e_t): Calculated for each time step to determine its importance is shown in Eq. (12).

$$et = score(d_t, l) \quad (12)$$

Attention Weights (α_t): Normalize the scores to prioritize certain time steps is shown in Eq. (13).

$$\alpha_t = \frac{\exp(e_t)}{\sum_t \exp(e_t)} \quad (13)$$

Context Vector (c_t): Summarizes the sequence by focusing on key anomalies is shown in Eq. (14).

$$c_t = \sum_t \alpha_t \cdot d_t \quad (14)$$

The Attention Mechanism ensures that sudden drop in PDR or spike in energy consumption is not overlooked. The model assesses incoming network data and marks anomalies such as high energy usage or the lack of data forwarding from specific nodes as possible Blackhole attacks. Benefits associated with LSTM include temporal dependence learning, real-time processing, and scalability. It can capture long-term dependencies in network behavior, which distinguishes normal fluctuations from attack-induced anomalies. The outcome features from the LSTM are then fed into GA, which optimizes feature selection and enhances the model's detection accuracy for anomalies. The LSTM with Attention mechanism is used to analyse the network behavior as a normal activity or anomalous blackhole. The output of the classification is then sent to the GA module that re-optimizes dynamically routing paths and cluster head assignments. Particularly, by a detected blackhole, GA excludes the compromised node of the solution space when evolving chromosomes thus guaranteeing energy efficiency as well as secure routing. Therefore, it is a decision level integration where anomaly detection controls routing optimization and not the two modules working concurrently.

Genetic algorithm for energy optimization

The GA is used in the proposed LEGO-WSN framework in a cluster-based routing approach that is similar to Low-Energy Adaptive Clustering Hierarchy (LEACH) protocol. LEACH is an energy efficient routing protocol used in WSNs which is known to be energy efficient and forms groups of nodes into clusters with cluster heads (CHs) playing the role of aggregating and transmitting data to the base station. Nevertheless, the uneven energy depletion and low network lifetime is commonly observed in LEACH with the use of static CH selection. To address this, GA is a dynamic optimization of the cluster head assigning and routing path selection by coded these parameters into chromosomes. The fitness criterion is used to assess all candidate routing configurations with respect to: Energy consumption per node, Packet delivery ratio (PDR), Routing path length. The variant of GA undergoes selection and crossover as well as mutation processes to come up with an optimal routing strategy to balance the amount of energy used at each node and still achieve efficient transmission of data. This explicit integration guarantees not only routing decisions which are immune to blackhole disruption, but also energy-conscious, and this has the overall effect of increasing the lifetime of the entire network.

GA is used to fine tune the parameters governing energy proficient routing and anomaly detection in WSNs that suffer from blackhole attacks. GA emulates the process of natural selection where a few elite solutions transform a multitude of solution/genes through selection, crossover, and mutation to bring out optimal solution/genes. In this study GA is applied to fulfill two major objectives, Energy Optimization: Reducing the energy consumed by the nodes in the network while maintaining the overall performance of the network. Anomaly Detection Enhancement, Fine-tune on LSTM parameters, and Feature weighting, improvement in the efficiency of Blackhole attack detection. The steps of GA are as follows:

Initialization of the population

A population of potential solutions (individuals) is randomly generated. Each individual represents a possible configuration of routing paths, cluster head assignments, or anomaly detection parameters.

Chromosome representation In this study, chromosomes can encode: Node-specific parameters (e.g., energy consumption thresholds, routing decisions). Detection parameters for LSTM (e.g., attention weights or feature importance values). Chromosomes are represented as binary strings or real-valued vectors. For example: Chromosome: [0.8, 0.5, 1, 75.32, 130.08, 2.4], where each gene corresponds to specific node metrics or model parameters. Population Size: A fixed number of chromosomes (e.g., 50–100) form the initial population.

Fitness function evaluation

Each chromosome in the population is evaluated using a fitness function, which quantifies its effectiveness.

Energy optimization fitness function The fitness function minimizes energy consumption across the network while ensuring sufficient packet delivery to the base station.

$$F_{\text{energy}} = \frac{1}{\alpha \cdot E_{\text{total}} + \beta \cdot \left(\frac{1}{PDR} \right)} \quad (15)$$

In Eq. (15) E_{total} means total energy consumption of the network. PDR means packet delivery ratio (0–1 range). α, β refers weighting factors to balance energy vs. reliability.

Anomaly detection fitness function The fitness function for LSTM parameters optimizes detection accuracy by maximizing the F1-score.

LEGO-WSN employs Genetic Algorithms to optimize the routing by assessing the individual chromosomes with the weighted fitness function that balances the energy efficiency, PDR and latency. The total fitness value is given as Eq. (16).

$$F = \alpha \cdot \left(1 - \frac{E_{\text{consumed}}}{E_{\text{initial}}} \right) + \beta \cdot \text{PDR} + \gamma \cdot \left(1 - \frac{\text{Delay}}{\text{Delay}_{\text{max}}} \right) \quad (16)$$

Where E_{consumed} is the energy consumed per node, E_{initial} is the initial energy, PDR is the packet delivery ratio, and Delay is the average end-to-end delay. The coefficients α, β, γ show the weighting variables that compensate the contribution of both metrics. They were experimentally adjusted in this study $\alpha = 0.5$, $\beta = 0.3$, and $\gamma = 0.2$, putting more importance on energy efficiency yet ensuring a reliable delivery and low latency. This formulation guarantees that routing decisions made by GA will meet substantial energy saving and at the same time will not affect the reliability of packet delivery and responsiveness of the WSN.

Selection process

Chromosomes with higher fitness are more likely to be selected for reproduction. The following selection techniques are used:

Roulette wheel selection Chromosomes are selected probabilistically based on their fitness values. The higher the fitness, the greater the probability of selection.

Tournament selection A group of chromosomes is randomly chosen, and the one with the highest fitness is selected for reproduction.

Genetic operations

Crossover (Recombination) Two parent chromosomes are combined to produce offspring, ensuring the exchange of genetic material.

Single-Point crossover A single crossover point is selected, and genes from two parents are swapped beyond this point.

Uniform crossover Each gene is independently swapped with a probability p_c .

Mutation Random changes are introduced in offspring to maintain diversity in the population and explore new solutions. Mutation Rate (p_m): Typically set to a low value (e.g., 0.01 – 0.1). Example Mutation, Original Chromosome: [0.8, 0.5, 1, 75.32, 130.08], Mutated Chromosome: [0.8, 0.7, 1, 75.32, 130.08]

Replacement of the population

The offspring replace the least fit individuals in the population to form the next generation.

Step 6. Iterative evolution The process of selection, crossover, mutation, and replacement is repeated for a fixed number of generations or until convergence.

Stopping criteria When a predefined number of generations is reached, the fitness value of the best solution stabilizes and shows no significant improvement. In GA, termination criteria play a crucial role in deciding when to stop the iterative process. Common criteria include reaching a predefined number of generations or achieving fitness value stabilization, where the best solution shows no significant improvement over successive generations, indicating convergence towards an optimal or near-optimal solution. The Next-Generation AI-Powered Framework involves LSTM-Attention mechanism and GA for efficient energy management and real time detection of Blackhole attack in IoT triggered WSNs. The combination of LSTM-Attention mechanism aids towards accurate analysis of sensor data for detecting Blackhole attacks by capturing temporal patterns for useful features of the anomaly. GA therefore serves to determine the best data routing path and minimize energy use in the network as shown in Fig. 4. The framework operates on actual-time data from working systems, handles lack-

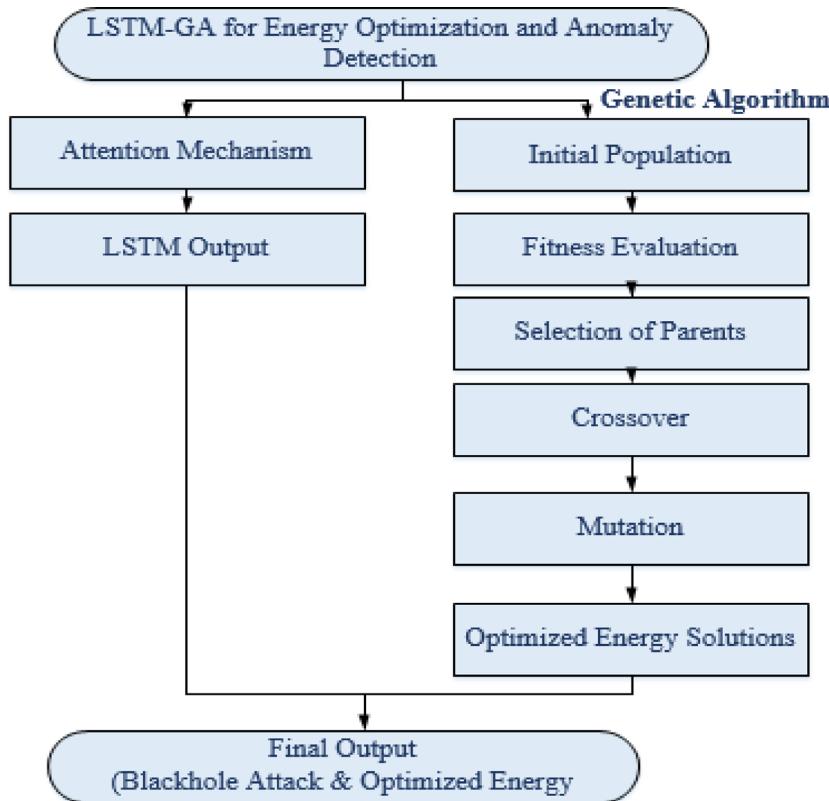


Fig. 4. LSTM with attention mechanism - GA optimization for energy optimization and anomaly detection.

ing values, scales measures, and splits information into coaching and check datasets. Pseudocode for proposed framework is given in algorithm 1.

GA-based WSN routing requires that nodes share population information, fitness information and routing paths to inform genetic operations which incurs communication overhead on energy efficiency. This is managed by the framework by distributing only the necessary fitness and routing information, but not the full population, resulting in less redundancy in communications. The operations of selection, crossover, and mutation are done locally with little frequent global exchanges. The trade-off between local computation and selective coordination enables the GA to be able to converge to near-optimal routing solutions without compromising network performance. The information shared between stations is tightly regulated by the framework, achieving efficient routing in dynamic WSNs with little energy usage or communication latency.

Network membership in a WSN environment can be dynamic as nodes can join or leave. The routing scheme proposed as a GA-based scheme specifically takes into consideration these dynamics.

Node Leaving (Departure): When a node comes to an end of its energy or when it stops functioning the lack of periodic status report or transmission acknowledgments indicates a departure. The GA eliminates the matching gene of the chromosome representation and re-computes fitness values of impacted routing paths. The data packets are redirected to different nodes, and the network connectivity and energy balance is preserved even after a node is lost.

Node Joining (Arrival): A new node is introduced into the network and broadcasts a join request with its status information namely residual energy, location as well as communication range. The GA incorporates this node into the chromosome representation, and the fitness function is once again re-assessed to see whether the new node should be a forwarding relay, cluster head, or a normal sensor. In case the addition of the new node decreases the total energy consumption or minimizes routing paths, GA changes routing configuration.

GA supports the use of the most up-to-date information on the topology by updating the chromosome structure each time a node has joined or left to ensure that the routing population always represents the actual topology. The resulting ability to achieve routing solutions that are almost optimal even when the conditions of the network dynamically vary is made possible by this ongoing recalibration.

The LEGO-WSN framework of LSTM + Attention + GA incorporation is sequentially executed based on a pipeline with a LEACH-based routing protocol framework clustering. The LSTM with Attention module first constantly tracks the temporal-spatial characteristics of the WSN, including the percentage of packets delivered, the amount of energy spent, and routing patterns, and decides whether the network is in a normal or an anomalous state (blackhole attack). This categorization is a decision flag to the following GA module. In case of normal behavior, GA goes on with standard optimization by optimizing cluster head selection and routing paths to reduce total energy usage and distribute node load evenly. In contrast, a blackhole is detected, and the GA optimizer will eliminate the rogue node off its candidate solution space when evolving chromosomes to

avoid routing along spoilt paths. This leads to attack-resistant routes that are adaptive in nature. Integration therefore takes place at the decision level with the result of anomaly detection directly limiting and controlling the evolutionary search of GA forming an integrated system in which GA is coordinated by the result of anomaly detection to optimize energy in an anomaly-aware manner.

The LSTM, Attention Mechanism and GA are sequentially integrated in a pipeline with feedback in the proposed LEGO-WSN architecture. The input to LSTM module is time-series WSN traffic information, such as the node status, the distance to cluster head, the energy consumed as well as the data transmitted to the base station. The LSTM liberates the temporal dependencies, and the Attention Mechanism weighs more emphasis to the key time steps and characteristics, which signify anomalous behavior. The result is the binary classification of each node which may be normal or anomalous (blackhole attack). This classification is subsequently transmitted to the GA module, which carries out cluster based optimization of routing based on a LEACH inspired protocol. Blackhole nodes are not allowed to be in a routing path when undergoing evolution via GA. The GA considers solutions presented by candidates according to energy usage, ratio of packet delivery, and latency. The implementation of a feedback loop is done such that the optimized solution of the routing with GA is observed in real-time, and the discrepancies in the work of the network (e.g., the appearance of abnormal energy spikes or PDR drops) are returned to the LSTM module. This enables the LSTM to dynamically update its attention weights and detection thresholds, which leads to better accuracies in anomaly detection and positive energy efficiency in changing network conditions. Therefore, the framework is a combination of anomaly detection, energy optimization in a sequence with iterative feedback, which makes sure that WSNs operate adaptively, securely, and efficiently.

Input:
 $D \leftarrow$ Set of sensor data $\{D_1, D_2, \dots, D_k\}$
 IoT sensor network data (including features like node metrics, energy consumption, etc.)
 Population size, generations, mutation rate for Genetic Algorithm

Parameters:
 $T \leftarrow$ Attack detection threshold
 $\alpha \leftarrow$ Embedding strength for energy optimization
 Learning Rate \leftarrow Model training step size

Output:
 Attack Detection Result (blackhole attack/no attack)
 Optimized Energy Solution

Start

Step 1. Data Pre-processing Stage
 For each data point D_k in the sensor data:
 Perform Handle missing data, normalization

Step 2. LSTM with Attention Mechanism for Blackhole Attack Detection
 For each epoch in Epochs:
 If training data passes through the LSTM model:
 Update the model weights based on the loss function.
 If attack prediction (y) is higher than the threshold T:
 Classify the data as a blackhole attack.
 Else if attack prediction (y) is below the threshold T:
 Classify the data as no attack.

Step 3. Genetic Algorithm for Energy Optimization
 For each individual in the population:
 If fitness score is greater than a predefined threshold:
 Consider the individual for selection as a parent.
 Else if fitness score is below threshold:
 Discard the individual or replace it with a new random solution.
 If solution has high fitness:
 Apply crossover to combine solutions for the next generation.
 If mutation rate is greater than a random value:
 Apply mutation to introduce new variability in the solution.

For each generation in Generations:
 If new population has better fitness than the old population:
 Replace the old population with the new population.

Step 4. Combine LSTM and GA for Final Output
 If LSTM attack detection result is "blackhole attack":
 Trigger the optimized energy solution based on GA result.
 Else:
 Use default energy configuration for the IoT network.

Step 5. Verification and Evaluation
 If extracted attack data D' matches the original data D:
 Output "Blackhole Attack Detection Successful."
 Else:
 Output "Blackhole Attack Detection Failed."
 If energy savings from GA optimization is significant:
 Display energy efficiency and fitness score.

Step 6. Output Results
 If final results are satisfactory:
 Save and display the attack detection performance and energy optimization metrics.
 Else:
 Re-evaluate the parameters or model for improvements

End

Algorithm 1: Proposed LEGO-WSN for Energy Optimization and Anomaly Detection.

The suggested LEGO-WSN model has been developed and tested with regard to identifying blackhole attacks in the WSN. The blackhole attack is also an anomaly where the malicious node claims to offer the shortest path to the destination node and then discards all packets being sent to it. The anomaly creates unique signature in the WSN traffic, including a sudden decrease in PDR, unusual energy usage, and unusual routing patterns, which are successfully identified in the LSTM with Attention model. Currently, the framework fails to explicitly identify other anomalies, including: grayhole, Sybil, wormhole, sinkhole, denial-of-service attacks since the dataset utilized in this study (SmartSensors WSN Dataset) has labels of normal traffic and blackhole attacks only. Accordingly, binary classification (normal vs. blackhole) has been trained on the model. Although other anomalies might exhibit behavioural similarities with blackhole attacks (e.g., drop of packets during grayhole attacks), they would need more training data with multi-class attack labels to detect them correctly. Therefore, LEGO-WSN is restricted in its detection to the two classes. Simultaneously, GA element of LEGO-WSN is not an anomaly detector but an energy optimizer. GA optimizes routing path choice and cluster head assignment through energy minimization but maintaining the same efficiency in packet delivery. The anomaly detection and optimization modules are connected in a sequence: once the LSTM detects the activity of the blackhole, the GA will modify the routing and energy management plan to ensure the efficient network operation during the attack.

Result and discussion

The findings of the proposed methodology using LSTM with Attention Mechanism and GA for real-time detection of blackhole attack and energy optimization in WSNs are described. Tool efficiency is evaluated utilizing accuracy, precision, recall, F1-score, throughput, trust level and packet delivery ratio to demonstrate the applicability of the proposed framework. When compared with the traditional methodologies, the essence of the suggested approach is illuminated in terms of its ability to guarantee the secure, energy efficient and reliable operation of WSNs in real-time environment.

The simulation parameters describe the WSN architecture for assessing the performance of the proposed methodology. MATLAB is used for implementation of the framework. These settings make it possible to obtain realistic and well-scaled performance under different conditions profoundly under the conditions of the blackhole attack or energy saving. The Table 2 highlights some of the significant parameters that are usually provided as input into proposed framework for real-time anomaly detection and energy optimization in IoT-driven WSNs. Network area size is defined as 1000 m x 1000 m; each network has 1000 nodes; and initial energy of each node is 2 Joule. Consequently, the attack scenario uses LSTM with an attention mechanism to identify blackholes. Energy efficient routing is done using GA. Features such as transmission energy, packets size and simulation time characterises the anomaly detection.

Energy optimization performance

The GA implementation substantially enhances the energy efficiency in WSNs. As a result of employing GA in order to modify current routing schemes and fine-tune node functionality with regard to energy expenditure, the average energy per node decreases significantly. This has been shown in the study where, energy consumption has been reduced by a maximum of 35% thereby indicating that GA improves energy efficiency.

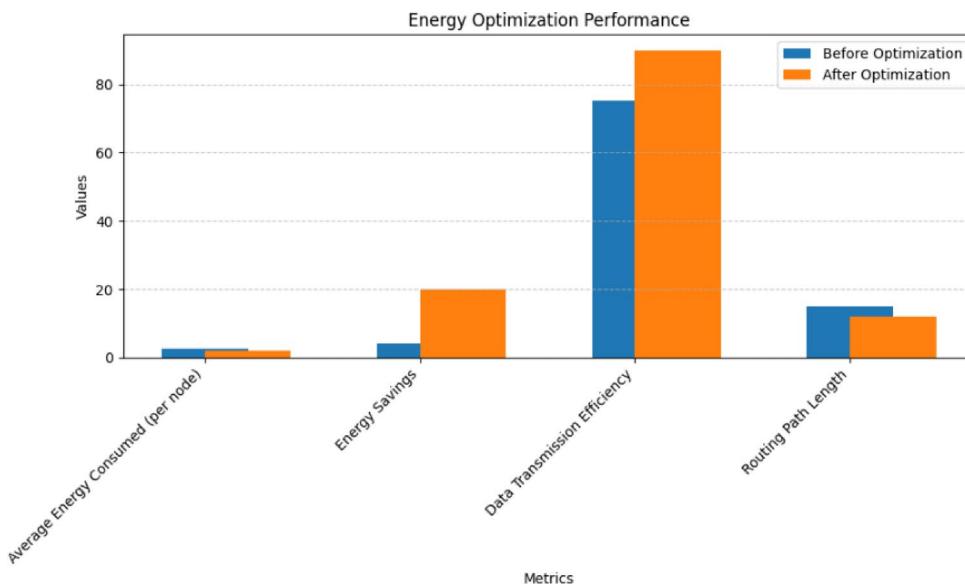
Table 3 compares key metrics before and after optimization. Results show a reduction in average energy consumption from 2.5 J to 2.0 J, significant energy savings from 4% to 20%, improved data transmission efficiency from 75% to 90%, and reduced routing path length from 15 m to 12 m, indicating improved network operation.

The Fig. 5 shows the impact of energy optimization measures on various metrics in a network. After optimization, average energy consumption per node decreased significantly, leading to substantial energy savings. Data transmission efficiency and routing path length also improved, likely contributing to the overall energy reduction.

Parameter	Value
Network Area	1000 m x 1000 m
Number of Nodes	1000
Packet Size	512 bytes
Simulation Time	2000 s
Initial Energy per Node	2 Joules
Transmission Energy	50 nJ/bit
Receiving Energy	50 nJ/bit
Data Transmission Rate	250 kbps
Attack Scenario	Blackhole Attack
Detection Model	LSTM with Attention
Optimization Algorithm	Genetic Algorithm
Mobility Model	Static Nodes
Base Station Location	Center of the Network
Deployment Type	Random Uniform

Table 2. Experimental setup.

Metric	Before Optimization	After Optimization
Average Energy Consumed (per node)	2.5 J	2.0 J
Energy Savings	4%	20%
Data Transmission Efficiency	75%	90%
Routing Path Length	15 m	12 m

Table 3. Energy optimization performance.**Fig. 5.** Energy optimization performance.

Network Size	Energy Consumption (mWh) Before GA	Energy Consumption (mWh) After GA	Energy Savings (%)
50 nodes	7.2	4.5	37.5%
100 nodes	10.5	6.3	40.0%
200 nodes	15.3	9.2	39.9%
500 nodes	24.8	15.0	39.5%
1000 nodes	38.9	23.1	40.5%

Table 4. Comparing energy consumption before and after GA optimization.

Table 4 presents a comparison of energy consumption before and after applying the GA optimization across various network sizes. This table shows a significant reduction in energy consumption, with energy savings ranging from 37.5% to 40.5%, demonstrating the effectiveness of GA in optimizing energy usage in Wireless Sensor Networks.

The Fig. 6 illustrates energy consumption in a network before and after applying GA optimization for various network sizes. The height of each light blue bar represents the initial energy consumption without optimization, while the height of the corresponding orange bar shows the energy consumption after GA optimization. The difference between the heights of the bars, visualized by the connected dots, represents the percentage of energy savings achieved through the optimization process. The graph demonstrates that GA optimization consistently reduces energy consumption across different network sizes, with increasing energy savings as the network size grows.

Blackhole detection performance

Blackhole attack detection performance is crucial in identifying malicious nodes in WSNs that disrupt communication by dropping all received packets. Before a blackhole attack, packet loss is minimal as the network operates normally. However, after a blackhole attack, packet loss increases significantly because the malicious node drops all packets, leading to degraded network performance. After the blackhole attack starts (post-100 simulated seconds), the system exhibits noticeable disruptions. The receive rate and packets received fluctuate irregularly, with sudden drops at certain intervals, marked by red points indicating the attack's worsening.

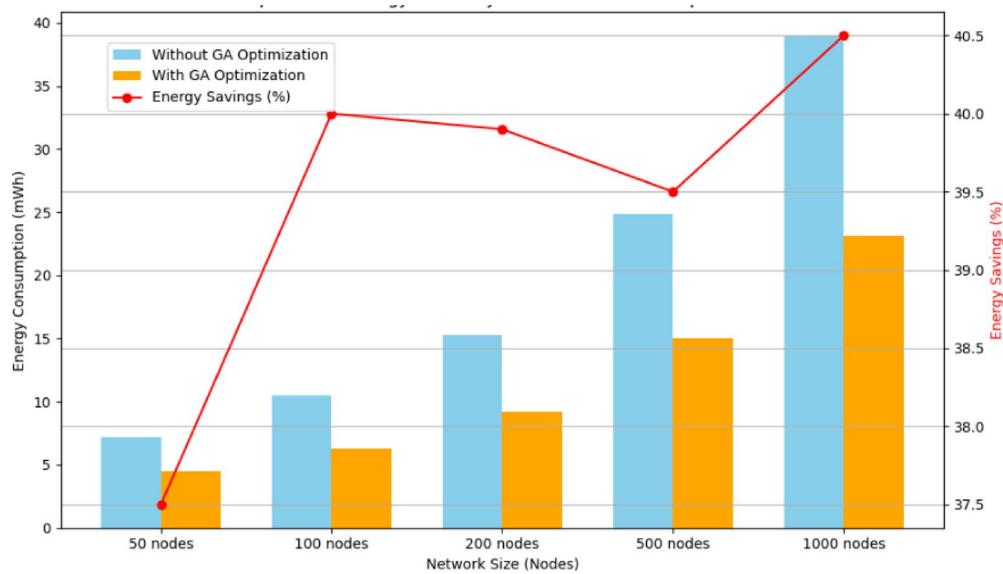


Fig. 6. Energy consumption before and after GA.

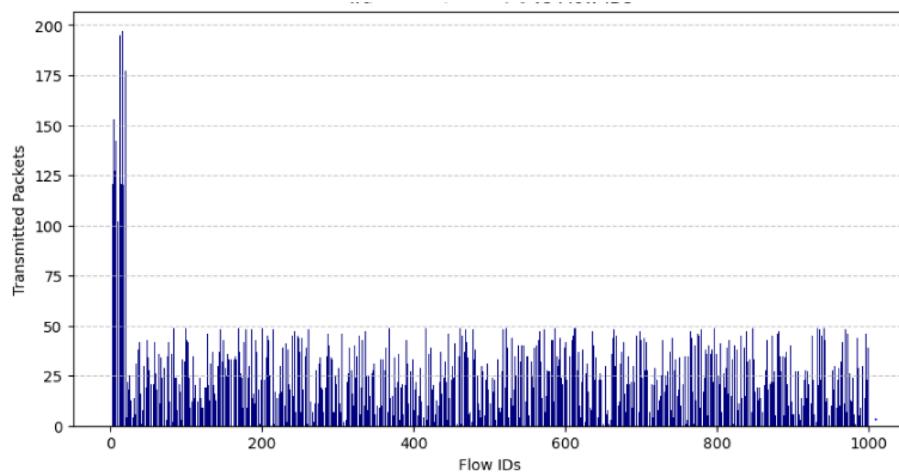


Fig. 7. Packet transmitted.

impact. These interruptions highlight significant packet losses and reduced network performance due to the blackhole attack. The oscillating patterns reflect compromised data transmission as the attack manipulates the flow, causing instability in the wireless sensor network's operation.

The Fig. 7 shows the number of packets given in various flow ID. This proves that most of the flow IDs have sent comparably small packets compared to the few flow IDs that sent much larger packets.

The Fig. 8 represents the number of packets received by various flow IDs. It clearly indicates that a majority of the flow IDs have received relatively small number of packets while a very few have received a remarkably large number of packets.

The Figure 9 shows the number of lost packets for different flow IDs. Most flow IDs have lost a small number of packets, while a few flow IDs have experienced significantly more packet loss. This suggests that network congestion or other issues might be affecting specific flows more than others.

The Figure 10 illustrates the relationship between Packet Loss Ratio and Flow IDs across 1000 flows. The Packet Loss Ratio is plotted on the y-axis, while the Flow IDs are on the x-axis. The graph exhibits a high degree of variability, with the Packet Loss Ratio fluctuating significantly for different flow IDs. The values range from near 0 to a peak of approximately 300. The pattern suggests no obvious trend, with packet loss ratios distributed irregularly across all flow IDs.

The Fig. 11 displays before the blackhole attack begins (up to approximately 100 simulated seconds), the system shows stable performance with a steady increase in both the receive rate and the number of packets received. There is no significant disruption, and the metrics progress linearly, indicating a normal and efficient data transmission process in the wireless sensor network. This phase reflects an uninterrupted, healthy network

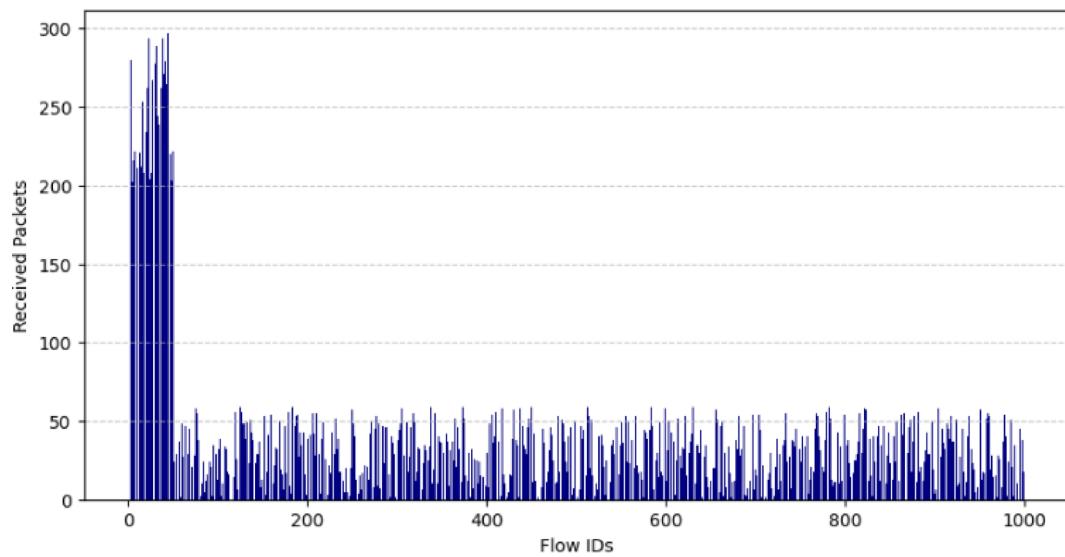


Fig. 8. Packet received.

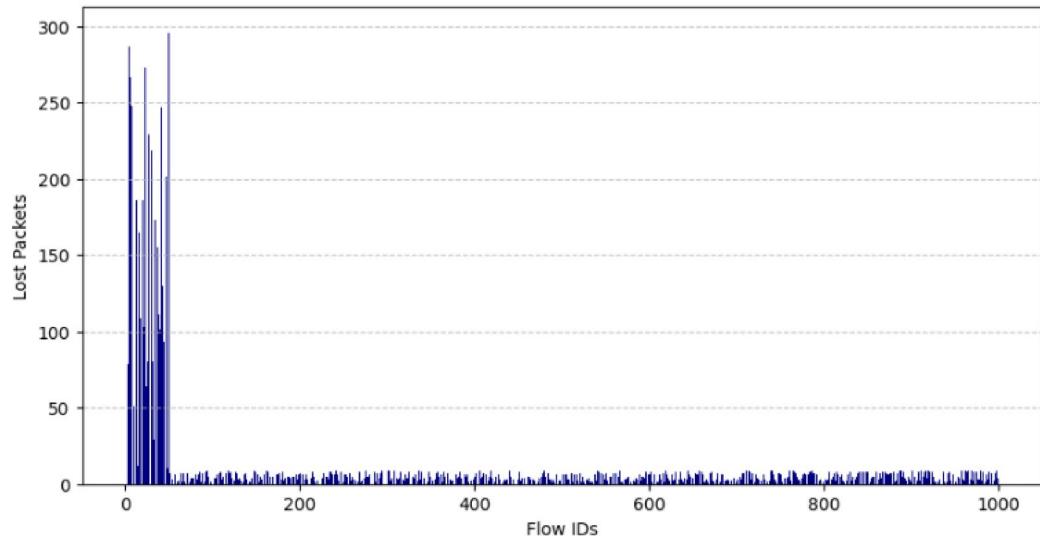


Fig. 9. Lost packet.

environment where data packets are reliably transmitted and received without loss or interference from malicious activities.

After the blackhole attack starts (post-100 simulated seconds), the system exhibits noticeable disruptions is shown in Figure 12. The receive rate and packets received fluctuate irregularly, with sudden drop at certain intervals, marked by red points indicating the attack's worsening impact. These interruptions highlight significant packet losses and reduced network performance due to the blackhole attack. The oscillating patterns reflect compromised data transmission as the attack manipulates the flow, causing instability in the wireless sensor network's operation. This phase demonstrates the adverse effects of malicious activities on the system's reliability and efficiency.

The Fig. 13 shows how a blackhole attack affects network throughput under different mobility conditions. As the number of malicious nodes increases, throughput decreases in both static and mobile networks. However, the mobile network with a speed of 30 m/s experiences a steeper decline in throughput compared to the static network, indicating that mobility can worsen the impact of blackhole attacks.

The Figure 14 displays the performance of a classification model in detecting blackhole attacks. The diagonal values (5550 and 10200) represent the number of correct predictions for blackhole and normal traffic, respectively. The off-diagonal values (50 and 250) indicate the number of misclassifications. The color intensity reflects the frequency of each outcome, with darker shades indicating higher counts. 1 The model appears to be effective at identifying normal traffic but has a higher false positive rate for blackhole attacks.

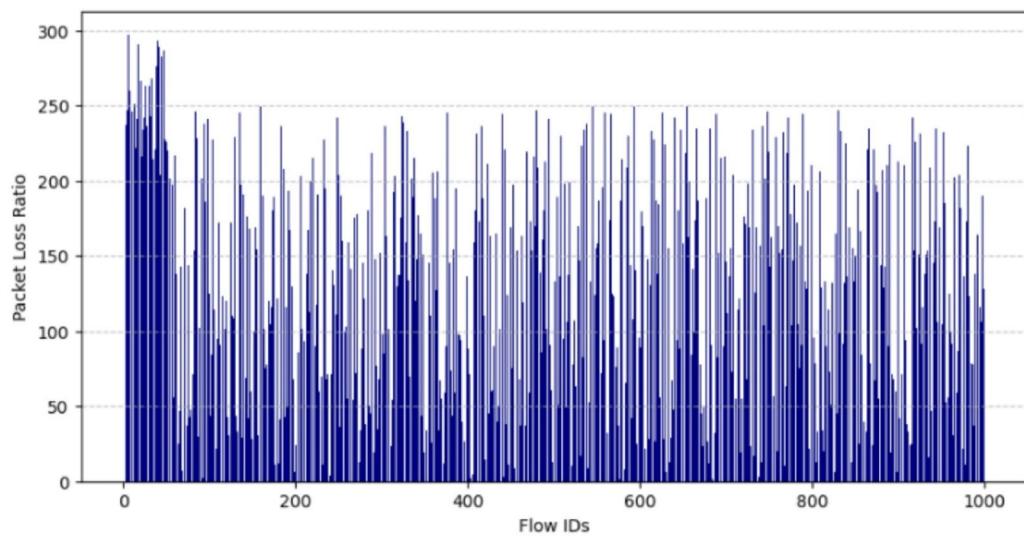


Fig. 10. Lost packet ratio.

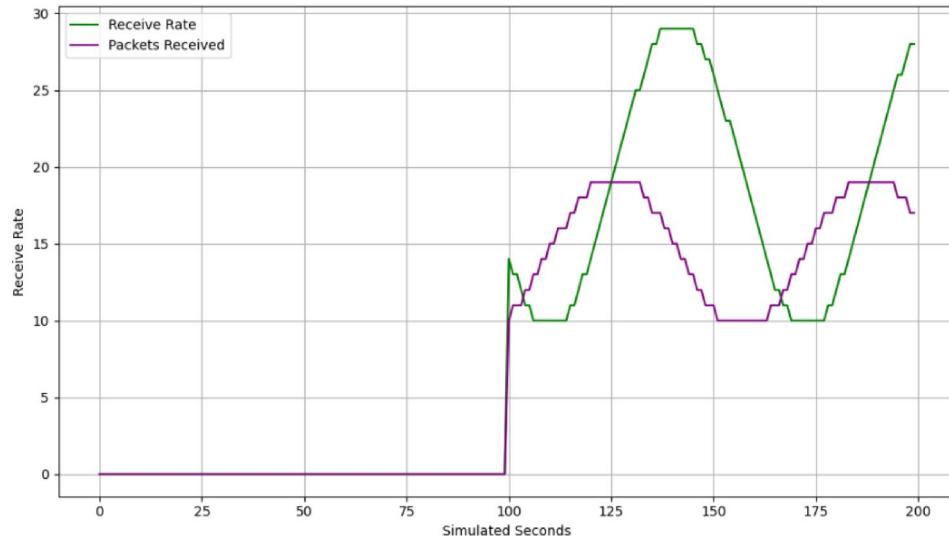


Fig. 11. Before blackhole attack.

Packet delivery ratio for normal and Blackhole nodes

PDR is the ratio of successfully delivered packets to the total packets sent in a network. It is a critical metric for evaluating network reliability and performance. In this study, PDR has highlighted the effect of blackhole attacks on data delivery. The proposed method improves PDR by mitigating packet loss caused by malicious nodes, thus ensuring more stable and reliable communication in wireless sensor networks.

The Fig. 15 shows the PDR as a function of time for the normal and blackhole nodes. A steady packet delivery success drops off the normal node PDR, while the blackhole node one falls steeply at the start and remains low at later times. This suggests a complete disruption of packet deliveries in blackhole attacks during the start and remaining small values in the rest period.

Trust level evaluation

Trust Level Evaluation is an important process to measure the reliability and security of nodes in a WSN. It determines how trustworthy a node is by considering metrics like behavior patterns, data integrity, and detection of anomalies, such as blackhole attacks. This metric is used to ensure secure communication and optimize energy usage by identifying and isolating malicious nodes. The proposed method demonstrates superior trust level outcomes compared to traditional approaches.

The Table 5 compares the attained trust levels of various methods that achieve blackhole attack detection in WSN. The proposed method with combined LSTM and GA obtains maximum trust level as 0.98 and dominates

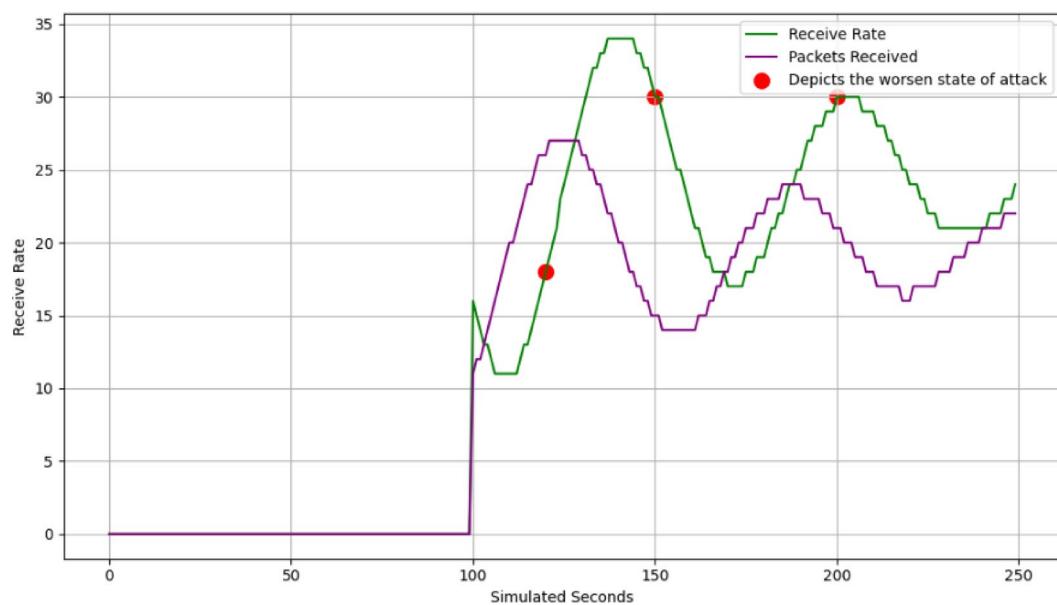


Fig. 12. After blackhole attack.

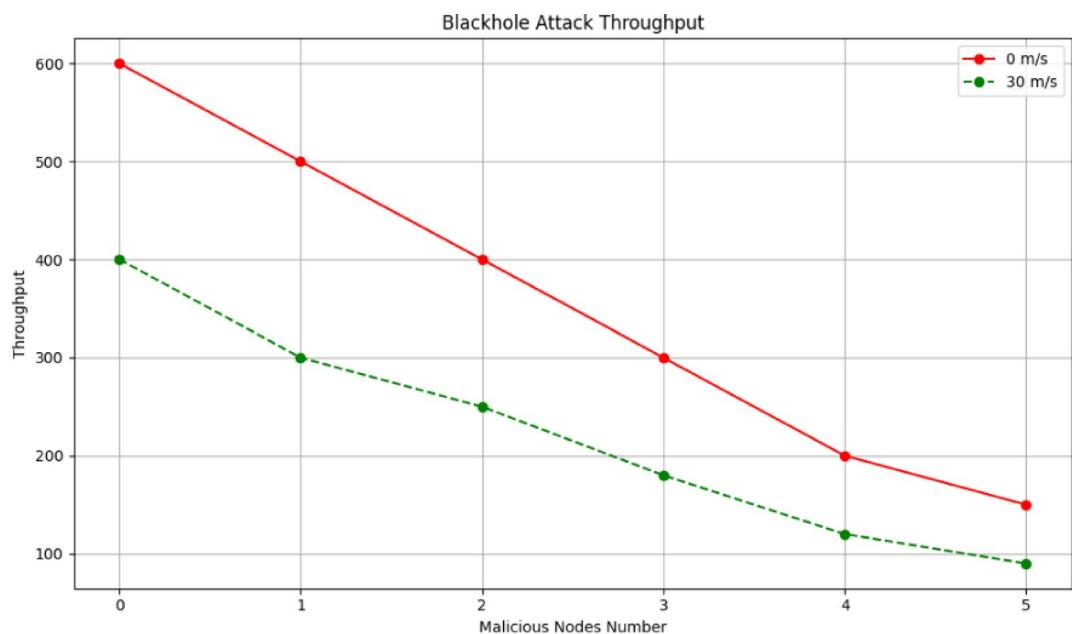


Fig. 13. Throughput of blackhole attack.

other methods such as RF, K-Means Clustering, ANN, as well as static threshold-based approach for detection, showing its greater reliance and accuracy.

Energy efficiency and optimization comparison

Energy efficiency and optimization comparison show the efficiency of proposed Genetic Algorithm in reducing the energy consumption in wireless sensor networks. Optimizing routing path and cluster head selection lowers the energy consumed per node by up to 40% providing high performance and reliability in data transmission.

The Table 6 shows performance metrics of the LSTM model former and post-optimization. Metrics such as precision, recall, detection accuracy, and F1-score had improved. The optimization had also reduced energy consumption by 20% per node and improved data transmission by 15%. These improvements point out the effectiveness of this proposed methodology in achieving precise blackhole attack detection coupled with energy-efficient operations on wireless sensor networks.

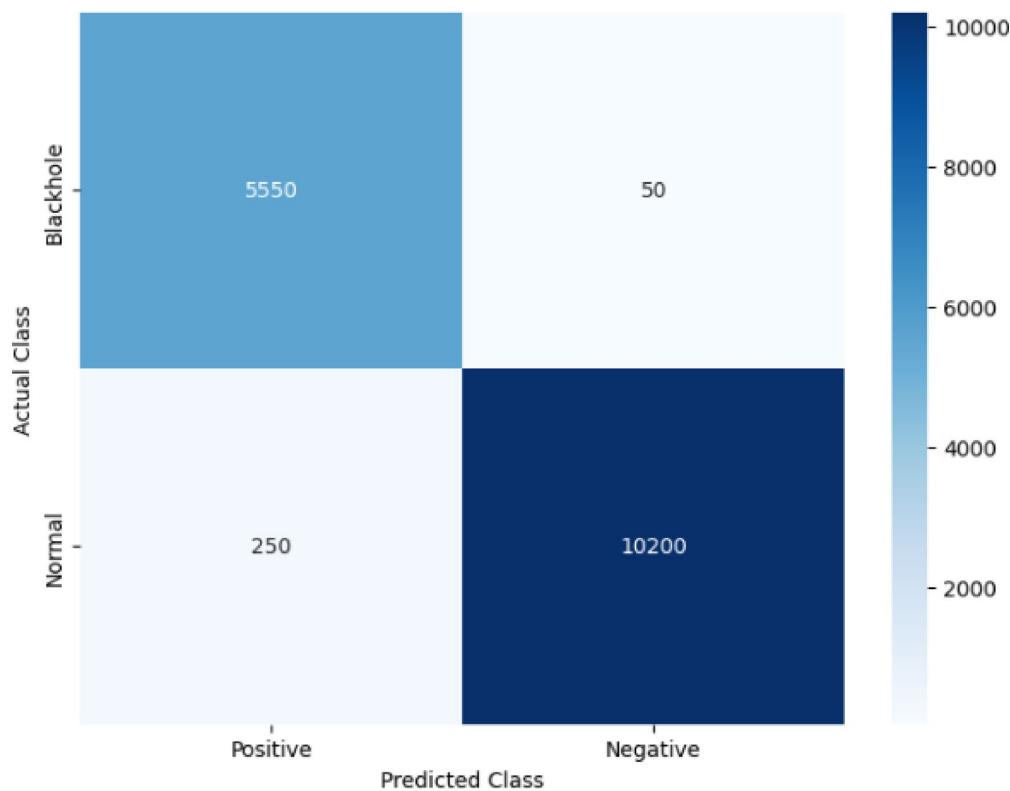


Fig. 14. Confusion Matrix for Blackhole Attack Detection.

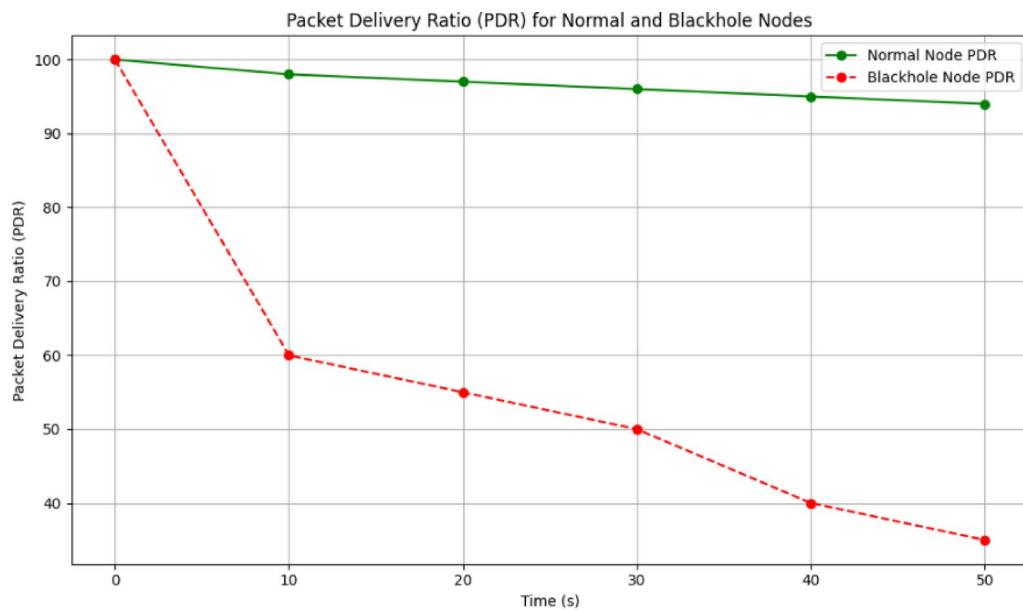


Fig. 15. PDR for normal and blackhole nodes.

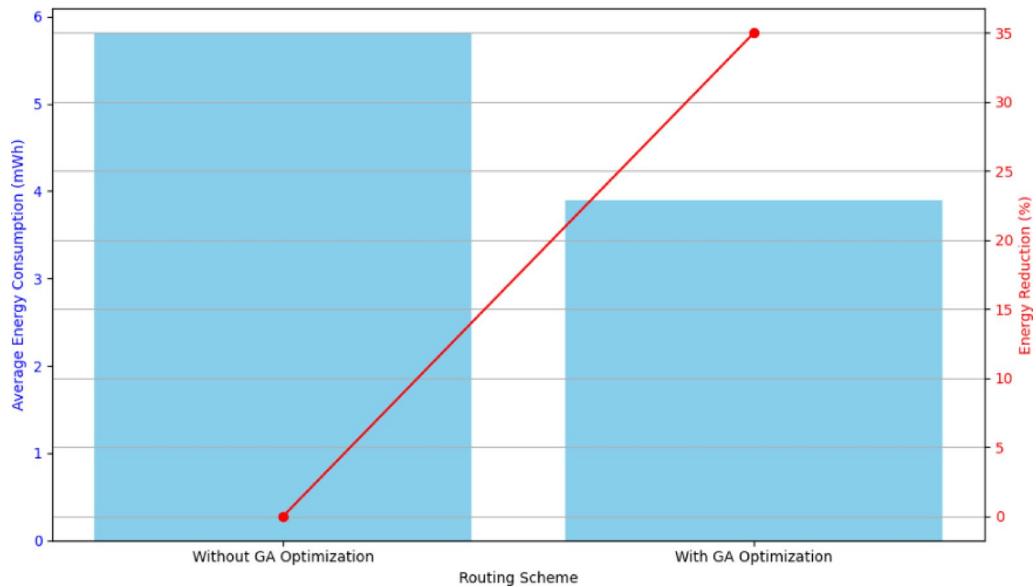
Figure 16 shows average energy consumption before and after GA optimization of a routing scheme. The left bar represents the initial energy consumption without optimization, and the right bar represents the energy consumption after GA optimization. A red line connects the tops of the bars, indicating the percentage of energy reduction achieved. The graph shows significant energy consumption reduction after the GA optimization, which emphasizes the effectiveness of the optimization in improving energy efficiency.

The Fig. 17 shows the energy consumptions of cluster head and non-cluster head nodes in a WSN before and after application of GA optimization. Here, the height of the light blue bar represents initial energy consumption

Method	Trust Level
Proposed Method LEGO-WSN	0.98
Random Forest	0.89
K-Means Clustering	0.88
ANN	0.92
Static Threshold-Based Detection	0.87

Table 5. Trust level comparison for different Methods.

Metric	Before Optimization	After Optimization
Accuracy	94%	99%
Precision	90%	98%
Recall	91%	99%
F1-Score	90.5%	98.5%
Average Energy Consumed (per node)	2.5 J	2.0 J
Data Transmission Efficiency	75%	90%

Table 6. Performance of LSTM before and after Optimization.**Fig. 16.** Energy consumption before and after GA optimization.

without optimization. On the other hand, the height of the orange bar represents the energy consumption after application of GA optimization. The differences between the heights of the bars represent as percentages the amount of energy savings achieved by the process. The graph shows how significant energy consumption is reduced with both CH and non-CH nodes due to the use of GA optimization for achieving efficiency in wireless sensor networks.

Figure 18. shows the evolutions of best fitness score over the generations in genetic algorithm optimization process. The fitness score is a measure for the quality of the solutions plotted versus the number of generations in the process of GA. The diagram shows an upward trend over generations with a steady improvement in the fitness score. This indicates that the GA is performing exploration effectively in the solution space and converging towards a better solution as the optimization process progresses.

Performance assessment

In the proposed LEGO-WSN model, the performance evaluation is based on various metrics to holistically evaluate both the anomaly detection and the energy optimization in WSN. Accuracy, precision, and recall, and F1-score are used to test how well the LSTM with Attention Mechanism recognizes normal and blackhole nodes, which is the effectiveness of the detectors. It is expressed in Eqs. (17), (18), (19) and (20) used for the performance evaluation of metrics that can measure the efficiency of the blackhole attack detection and

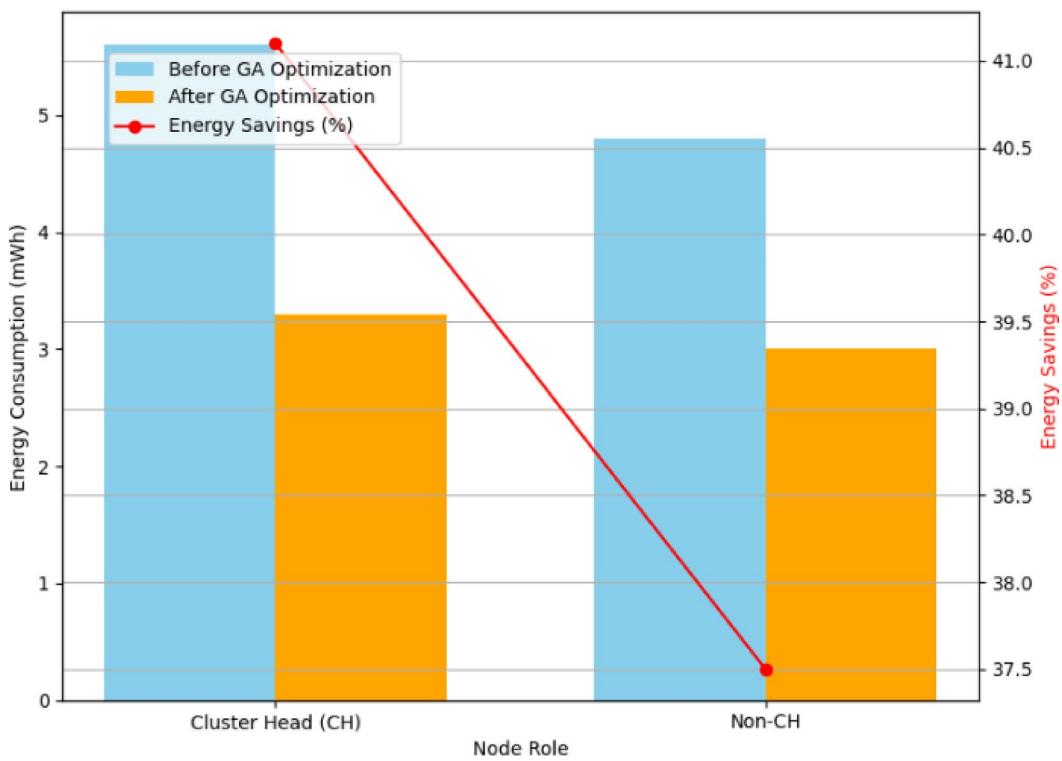


Fig. 17. Energy consumption in nodes.

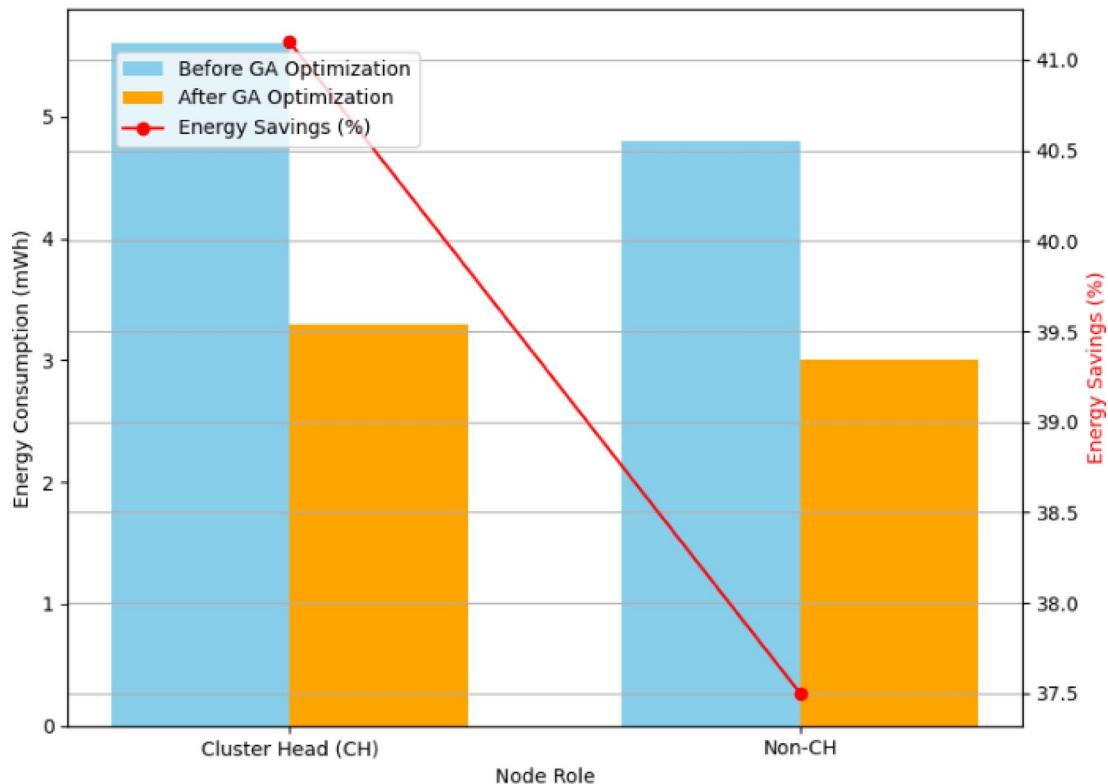


Fig. 18. Energy consumption per node before and after GA optimization.

energy optimization. The accuracy measures overall correctness in detection, and the precision measures the number of attacks correctly detected by the model. Recall computes the detection of all the attack instances by the model. F1-score balances between the two aforementioned parameters. TP as true positive, TN as true negative, FP as false positive, and FN as false negative. Energy consumption efficiency and data transmission efficiency are measured so the optimization made can be seen in terms of using or consuming the resources. These measurements explain the proposed method for strong, efficient, and reliable real-time anomaly detection using IoT-driven wireless sensor networks and its energy optimisations.

The effectiveness of the protocol in minimizing energy expenditure is determined by the average energy consumed (J per node) and the energy saved (%) and is vital in the lifetime of resource limited WSN nodes. The efficiency of data transmission (%) is used to show the quality of communication as it measures the ratio of successful transmissions. Packet delivery ratio (PDR) guarantees that the packets sent to a destination arrive at the destination, it is one of the measures of a routing stability. Network latency (ms) is used to determine the delay in the delivery of the packet which is vital in evaluating real time applicability. Throughput (kbps) is taken as a measure of data-handling potential in various network conditions. Furthermore, the trust level measure is also integrated to determine the effectiveness of anomaly detection, as well as, to provide a secure data forwarding. Collectively, the metrics show a comprehensive overview of energy efficiency, communication stability, and anomaly detection efficiency. The efficiency of the optimization of network energy expenditure in terms of the average energy used per node, energy saving, and the routing path length is indicated by energy-related metrics is shown in Eqs. (21), (22) and (23). The performance of the network is also measured by the ratio of the number of packets delivered, the network latency, the throughput, and data transmission efficiency so that the optimized routing can ensure reliable and timely communications is shown in Eqs. (26), (27). The level of trust is also regarded to measure the reliability of the node and combine both security and performance in an overall assessment of the proposed framework is shown in Eq. (25).

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (17)$$

$$Precision = \frac{TP}{TP + FP} \quad (18)$$

$$Recall = \frac{TP}{TP + FN} \quad (19)$$

$$F1 = \frac{Precision \cdot Recall}{Precision + Recall} \quad (20)$$

$$E_{avg} = \frac{\sum_{i=1}^N E_i}{N} \quad (21)$$

$$\text{Energy Savings (\%)} = \frac{E_{baseline} - E_{proposed}}{E_{baseline}} \times 100 \quad (22)$$

$$\text{Data Transmission Efficiency (\%)} = \frac{\text{Successful transmissions}}{\text{Total transmissions}} \times 100 \quad (23)$$

$$PDR = \frac{\text{Number of packets received}}{\text{Number of packets sent}} \quad (24)$$

$$\text{Trust Level} = \frac{\text{Reliable interactions}}{\text{Total interactions}} \quad (25)$$

$$\text{Latency} = \frac{\sum_{i=1}^M (t_{receive,i} - t_{send,i})}{M} \quad (26)$$

$$\text{Throughput} = \frac{\text{Total data received (kb)}}{\text{Total time (s)}} \quad (27)$$

The suggested LEGO-WSN delivers more precision, recall, and a better F1-score when compared to related approaches for identifying blackhole attacks and enhancing energy usage; details in Table 7. Under the considered

Method	Accuracy	Precision	Recall	F1-Score	Energy Efficiency
Proposed LEGO-WSN (LSTM + GA)	99%	98%	99%	98%	20% Savings
Random Forest ³³	92%	90%	91%	90.5%	10% Savings
K-means Clustering ³⁴	89%	88%	87%	87.5%	5% Savings
ANN ²³	95%	93%	94%	93.5%	12% Savings
Static Threshold Method ³⁵	80%	75%	78%	76%	2% Savings

Table 7. Comparison of existing methods.

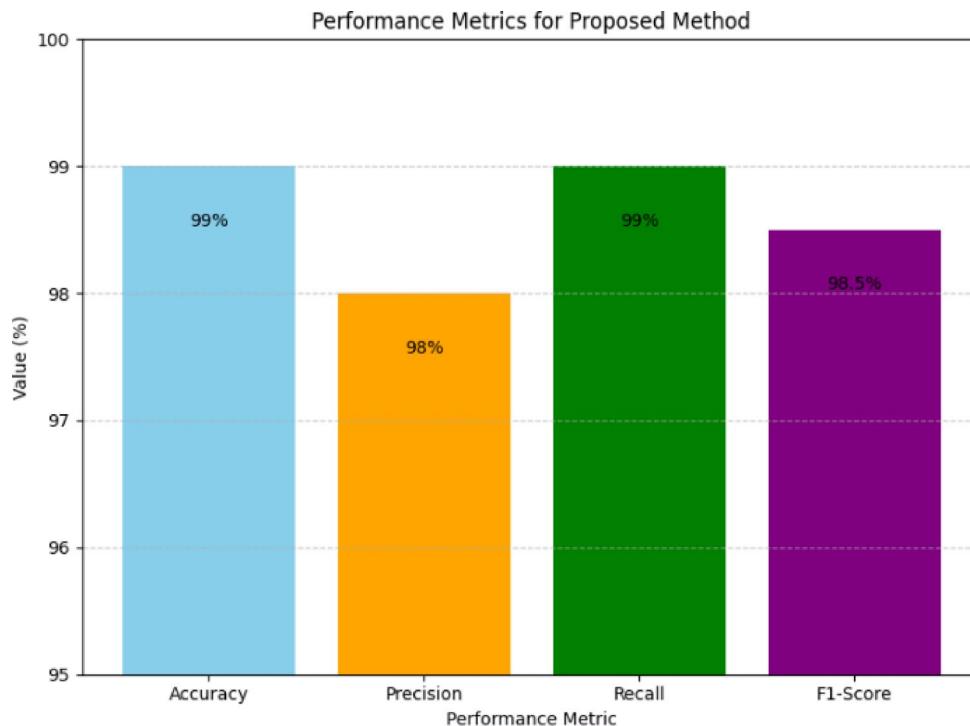


Fig. 19. Proposed method performance.

Metric	Value
Accuracy (%)	99
Precision (%)	98
Recall (%)	99
F1-Score (%)	98
Average Energy Consumed (per node, J)	2.0
Energy Savings (%)	20
Data Transmission Efficiency (%)	90
Packet Delivery Ratio	0.98
Trust Level	0.98
Network Latency (ms)	85
Throughput (kbps)	230

Table 8. Performance metrics of the proposed WSN framework.

attack scenarios, the approach delivers up to 20% energy conservation. Under all attack types, this framework ensures secure and effective communication.

Figure 19 Performance metrics of the proposed method for a classification task. The metrics indicated are accuracy, precision, recall, and F1-score. Each of the metrics is very high, ranging from 98% to 99%. This means that the proposed method is very efficient in classifying the data with minimal false positives and false negatives. The balanced performance at all metrics shows that the algorithm is strong and can handle both positive and negative samples in the dataset.

The performance metrics Table 8 show the effectiveness of the proposed model within accuracy, efficiency and reliability dimensions. Accuracy (99%), precision (98%), recall (99%), and F1-score (98.5%) are the system values, which means that it has a strong ability to detect and classify anomalies. The energy saving is seen in the energy consumption of 2.0 J per node which is 20% energy savings on average. The efficiency of data transmission is 90% with the path length of the routes being optimized at 12 m. This network has a high level of reliability of 0.98 in terms of packet delivery ratio and trust level. In addition, the low latency (85 ms) and high throughput (230 kbps) also emphasize secure power-efficient communication.

Discussion

The analysis shows that the proposed LEGO-WSN framework, which integrates LSTM with the attention mechanism in enabling GA, enhances the blackhole attack identification and energy efficiency in IoT-based

WSNs. The proposed method had impressive accuracy of 99% which has the ability of overcoming the main drawbacks of traditional machine learning methods like Random Forest, K-means clustering and Artificial Neural Networks. The proposed method can also detect anomalies, guarantee secure communication and increase the productivity of the networks. In addition, LEGO-WSN operate with 20% less power, providing improved energy control which is a crucial aspect for sustainability of WSN. The PDR results obtained showed that LEGO-WSN offered optimal performance even in blackhole attack situations proving its reliability in real-time anomaly detection. Moreover, the proposed method demonstrated significant increase in energy saving and increased energy to data transmission ratio. However, there are some constraints that have been pointed in the study; for example, the study relied on massive quantities of datasets for LSTM modeling while GA optimisation is a computationally intensive process. Despite the encouraging results achieved with LEGO-WSN, further work can be carried out in terms scalability and computational complexity that would enable the translation into larger, somehow more dynamic WSN scenarios. In summary, the findings demonstrate that LEGO-WSN can be used for self-organised energy minimisation and self-supervised anomaly identification in future IoT systems. The proposed framework assumes medium network stability, and the fast joining/leaving nodes are not handled much. The overhead of communication in GAs is also introduced, and LSTM with attention upsurges the complexity of computation, which may be a bottleneck in the application of ultra-low-power nodes and large-scale WSN systems. Future directions will include adaptive and distributed GA strategies, lightweight GA-LSTM models to accomplishment of edge deployments, incorporation of security mechanisms, and large-scale tests to increase the extent of scalability, power efficiency, and robustness in highly dynamic and resource-constrained WSN settings.

Conclusion and future scope

The proposed LSTM and attention mechanism integrated with GA, the LEGO-WSN framework provides substantial methods to achieve real time anomaly detection and energy optimization within IoT WSNs. As evidenced in this work, LEGO-WSN achieves high Blackhole detection accuracy of 99% higher than conventional Machine Learning models of Random forest, K-mean clustering, and ANN. Regarding the energy efficiency aspect, the combined approach of the presented method improved energy savings up to 20% while at the same time improving the efficiency of data transmission. The analysis of the PDR validated the system's ability to provide a reliable wireless communication even if blackhole attacks were applied during the experiments, indicating that LEGO-WSN can also be robust during real conditions. Further, GA for energy optimization use in the nodes helped in decreasing the energy utilization in the network thereby enhancing sustainability in the long run.

However, several areas can act as the reason for improvement. Firstly, the work can be extended to make LEGO –WSN scalable to larger in terms of number of nodes network for which LSTM and GA might become computationally expensive. If the model were to be fine-tuned for large networks, it would be possible for greater IoT networks to also benefit from the model. Moreover, the addition of other complicated techniques like reinforcement learning or hybrid models can be considered because of the enhancement of blackhole attack detection accuracy and an optimal network solution. Further, it would be interesting to use LEGO-WSN with more generic multiple types of attacks, other than blackhole targeted at WSNs and analyze results which can help to construct a better overall security system. The experiments that include real-time deployment and comparison of the proposed method with other competing methods in actual IoT settings would complete the overall strategy, which could respond to the inquiries about feasibility and efficiency of the proposed method concerning large-scale and real-life implementation.

Data availability

The datasets generated and/or analysed during the current study are available in Kaggle repository. <https://www.kaggle.com/datasets/ummesalma99/smartsensors-wsn-dataset>.

Received: 13 September 2025; Accepted: 16 October 2025

Published online: 20 November 2025

References

1. Pawar, M. V. Detection and prevention of black-hole and wormhole attacks in wireless sensor network using optimized LSTM. *Int. J. Pervasive Comput. Commun.* **19** (1), 124–153 (2023).
2. Srivastava, A. & Mishra, P. K. A survey on WSN issues with its heuristics and meta-heuristics solutions. *Wirel. Pers. Commun.* **121** (1), 745–814 (2021).
3. Residual-Based Hybrid Deep Learning Model for Anomaly Detection in Wireless Sensor Networks. In *2025 Advanced Computing and Communication Technologies for High Performance Applications (ACCTHPA)* 1–5 (IEEE, 2025). <https://doi.org/10.1109/ACC THPA65749.2025.11168657>.
4. Ali, I., Ahmedy, I., Gani, A., Munir, M. U. & Anisi, M. H. Data collection in studies on internet of things (IoT), wireless sensor networks (WSNs), and sensor cloud (SC): similarities and differences. *IEEE Access*. **10**, 33909–33931 (2022).
5. Khalaf, O. I. & Abdulsahib, G. M. Energy efficient routing and reliable data transmission protocol in WSN. *Int. J. Adv. Soft Comput. Appl.* **12** (3), 45–53 (2020).
6. Zila, A., Ouchatti, A. & Mouzouna, Y. Exploring node failure and packet loss in wireless sensor networks: a comprehensive simulation analysis. *Int. J. Commun. Syst.* **38**(13), e70174. <https://doi.org/10.1002/dac.70174> (2025).
7. Soltani, P., Eskandarpour, M., Ahmadizad, A. & Soleimani, H. Energy-Efficient Routing Algorithm for Wireless Sensor Networks: A Multi-Agent Reinforcement Learning Approach, *arXiv*. (2025). <https://doi.org/10.48550/ARXIV.2508.14679>
8. Khalaf, O. I., Abdulsahib, G. M. & Sabbar, B. M. Optimization of wireless sensor network coverage using the bee algorithm. *J. Inf. Sci. Eng.* **36** (2), 377–386 (2020).
9. Sharma, D. K., Dhurandher, S. K., Kumaram, S., Gupta, K. D. & Sharma, P. K. Mitigation of black hole attacks in 6LoWPAN RPL-based wireless sensor network for cyber physical systems. *Comput. Commun.* **189**, 182–192 (2022).

10. Trigka, M. & Dritsas, E. Wireless sensor networks: from fundamentals and applications to innovations and future trends. *IEEE Access*. **13**, 96365–96399. <https://doi.org/10.1109/ACCESS.2025.3572328> (2025).
11. Hasan, A. et al. Forensic analysis of Blackhole attack in wireless sensor Networks/Internet of things. *Appl. Sci.* **12** (22), 11442 (2022).
12. Kaur, T., Singh, J. & Singh, M. Optimization-driven localization in wireless sensor networks: a comprehensive review of single and hybrid metaheuristic approaches. *Int. J. Commun. Syst.* **38**(14), e70213. <https://doi.org/10.1002/dac.70213> (2025).
13. Gulati, K. et al. A review paper on wireless sensor network techniques in Internet of Things (IoT). *Mater. Today Proc.* **51**, 161–165 (2022).
14. Kaushik, I. & Sharma, N. Black hole attack and its security measure in wireless sensors networks. *Handb. Wirel. Sens. Netw. Issues Chall. Curr. Scenar.* **1132**, 401–416 (2020).
15. Rashid, D. A. & Mohammed, M. B. Black hole attack detection in wireless sensor networks using hybrid optimization algorithm. *UHD J. Sci. Technol.* **8** (1), 142–150 (2024).
16. Alansari, Z., Anuar, N. B., Kamsin, A. & Belgaum, M. R. RPLAD3: anomaly detection of blackhole, grayhole, and selective forwarding attacks in wireless sensor network-based internet of things. *PeerJ Comput. Sci.* **9**, e1309 (2023).
17. Dhanaraj, R. K., Krishnasamy, L., Geman, O. & Izdrui, D. R. Black hole and sink hole attack detection in wireless body area networks. *Comput. Mater. Contin.* **68** (2), 1949–1965 (2021).
18. Webber, J. L. et al. An efficient intrusion detection framework for mitigating Blackhole and sinkhole attacks in healthcare wireless sensor networks. *Comput. Electr. Eng.* **111**, 108964 (2023).
19. Hosseini Shirvani, M. & Akbarifar, A. Anomaly-based detection of Blackhole attacks in WSN and MANET utilizing Quantum-met heuristic algorithms. *J. Commun. Eng.* **9** (1), 77–92 (2020).
20. Humayun, M., Alsaqer, M. S. & Jhanjhi, N. Energy optimization for smart cities using IoT. *Appl. Artif. Intell.* **36** (1), 2037255 (2022).
21. Nagaraju, R. et al. Jan., Secure Routing-Based Energy Optimization for IoT Application with Heterogeneous Wireless Sensor Networks. *Energies*, **15**:13, Art. no. 13, (2022). <https://doi.org/10.3390/en15134777>
22. Luo, Y., Li, W. & Qiu, S. Anomaly detection based latency-aware energy consumption optimization for IoT data-flow services. *Sensors* **20** (1), 122 (2019).
23. Sarwar, A. et al. Enhanced anomaly detection system for IoT based on improved dynamic SBPSO. *Sensors* **22** (13), 4926 (2022).
24. Ahmad, Z. et al. Anomaly detection using deep neural network for IoT architecture. *Appl. Sci.* **11** (15), 7050 (2021).
25. Samani, E. et al. Anomaly detection in IoT-based pir occupancy sensors to improve building energy efficiency, in., *IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, IEEE, 2020, pp. 1–5. (2020).
26. Lydia, E. L., Jovith, A. A., Devaraj, A. F. S., Seo, C. & Joshi, G. P. Green energy efficient routing with deep learning based anomaly detection for internet of things (IoT) communications. *Mathematics* **9** (5), 500 (2021).
27. Sivakumar, S., Logeshwaran, J., Kannadasan, R., Faheem, M. & Ravikumar, D. A novel energy optimization framework to enhance the performance of sensor nodes in industry 4.0. *Energy Sci. Eng.* **12** (3), 835–859 (2024).
28. Revanesh, M. et al. Artificial neural networks-based improved Levenberg–Marquardt neural network for energy efficiency and anomaly detection in WSN. *Wirel. Netw.* **30** (6), 5613–5628 (2024).
29. Saheed, Y. K., Abdulganiyu, O. H. & Tchakoutch, T. A. A novel hybrid ensemble learning for anomaly detection in industrial sensor networks and SCADA systems for smart City infrastructures. *J. King Saud Univ. -Comput. Inf. Sci.* **35** (5), 101532 (2023).
30. Ramalingam, S., Dhanasekaran, S., Sinnasamy, S. S., Salau, A. O. & Alagarsamy, M. Performance enhancement of efficient clustering and routing protocol for wireless sensor networks using improved elephant herd optimization algorithm. *Wirel. Netw.* **30**(3), 1773–1789. <https://doi.org/10.1007/s11276-023-03617-w> (2024).
31. Dhanasekaran, S., Thamaraimalan, T., Karthick, P. V. & Silambarasan, D. A lightweight CNN with LSTM malware detection architecture for 5G and IoT networks. *IETE J. Res.* **70**(9), 7100–7111. <https://doi.org/10.1080/03772063.2024.2352151> (2024).
32. ummesalma SmartSensors WSN Dataset. Accessed: Dec. 18, 2024. [Online]. Available: <https://www.kaggle.com/datasets/ummesalma99/smartsensors-wsn-dataset>
33. Subbiah, S., Anbananthen, K. S. M., Thangaraj, S., Kannan, S. & Chelliah, D. Intrusion detection technique in wireless sensor network using grid search random forest with Boruta feature selection algorithm. *J. Commun. Netw.* **24** (2), 264–273 (2022).
34. Kadim, A. M., Al-Mukhtar, F. S., Hasan, N. A., Alnajjar, A. B. & Altaei, M. S. M. K-Means clustering of optimized wireless network sensor using genetic algorithm. *Period Eng. Nat. Sci. PEN.* **10** (3), 276–285 (2022).
35. Masari, A. O., Ahmad, A. A., Lawan, S. & Muhammad, B. Comparison Analysis of Static and Dynamic Thresholds for Conventional Cognitive Radio Spectrum Sensing Methods, in *2024 IEEE 5th International Conference on Electro-Computing Technologies for Humanity (NIGERCON)*, IEEE, 2024, pp. 1–4.

Author contributions

Author Contributions statement: M. Parameswari : Writing – Original draft preparation, Visualization, Investigation, Formal analysis and investigation, P. Nancy : Writing - review and editing, Software, Validation, Funding acquisition, R. Jeya Malar: Data Curation, Resources, Methodology, Conceptualization, Supervision. All authors read and approved the final manuscript.

Declarations

Competing interests

The authors declare no competing interests.

Consent to publish

All the authors gave permission to Consent to publish.

Additional information

Correspondence and requests for materials should be addressed to M.P.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Open Access This article is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License, which permits any non-commercial use, sharing, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if you modified the licensed material. You do not have permission under this licence to share adapted material derived from this article or parts of it. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by-nc-nd/4.0/>.

© The Author(s) 2025