RESEARCH ARTICLE

INTERNATIONAL RESEARCH JOURNAL OF MULTIDISCIPLINARY TECHNOVATION

Asian Research Association

DOI: 10.54392/irjmt2625

Deep Learning-Based Secure Routing Framework for Blockchain-Enabled Autonomous Military Wireless Sensor Networks

D. Rekha [a,*], K. Baalaji [a]

[a] Department of Computer Science and Engineering, Bharath Institute of Higher Education and Research, Selaiyur, Tambaram, Chennai-600073, India

* Corresponding Author Email: rekhadharma23@gmail.com

DOI: https://doi.org/10.54392/irjmt2625

Received: 06-11-2025; Revised: 05-02-2026; Accepted: 17-02-2026; Published: 10-03-2026

Abstract: Military deployment of Wireless Sensor Networks (WSNs) demands high security, communication facilities, and energy efficiency. Failing to provide secure and dynamic data transmission is a major challenge in such networks because there are no centralized base stations, an open distributed architecture, and various security threats. The research introduces a deep learning based secure routing infrastructure to blockchain-enabled autonomous military WSN that focuses on decentralized trust and flexible intrusion detection (ID). The WSN-DS data was used to analyze the research. For ID, a Seven-Spot Ladybird Optimization Enhanced Bidirectional Long Short-Term Memory with Attention Mechanism (SSLO-Bi-LSTM-ATT) model is applied. The Blockchain Enabled Secured Routing Protocol (BESRP) ensures trustworthy routing transactions by combining decentralized blockchain authentication with Bi-LSTM-ATT-driven anomaly detection. To authenticate node-to-node transfers, the protocol creates dynamic lightweight blockchains, lowering energy overhead and ensuring data confidentiality and integrity. By integrating the proposed structure of the proposed structure, energy consumption reduces and optimizes routing performance by integrating the proposed structure, by integrating the BI-LSTM-Att for decentralized authentication and BI-LSTM-night. Simulation results show that the proposed system improves existing approaches when it comes to the use of low energy, reduces package loss and improvement in throwing. Overall, the integration of deep learning with blockchain in the autonomous military WSN provides a promising approach to ensure safe operations, and addresses important defense requirements.

Keywords: Wireless Sensor Networks, Military Sensor Networks, Blockchain, Secured Routing, Intrusion Detection, a Seven-Spot Ladybird Optimization Enhanced Bidirectional Long Short-Term Memory with Attention Mechanism (SSLO-Bi-LSTM-ATT).

1. Introduction

WSN has become an important tool for modern military operations, letting data be sent, sensed, and monitored over large and complicated areas [1]. Wireless sensor networks (WSNs) rely on sensors that are deployed throughout heterogeneous locations, allowing to capture a variety of physical parameters, such as velocity, vibration, temperature and acoustic signals [2].The ability to report in real time, telling the truth through WSN helps significantly boost surveillance capacity, assist in strategic decision-making and be sure that the defense infrastructure is secure. Unlike traditional communication systems, WSNs possess adaptive features and can meet various requirements by reorganizing, growing organically and adapting to environmental variations. This flexibility is especially helpful in applications where mobile mission critical is required [3, 4]. Cooperative sensor modalities within the operational environment are a key to providing timely intelligence to recalibrate strategic decisions [5]. The distributed architecture of WSNs provides benefits of enabling continuous data acquisition even under unpredictable operation conditions; thereby reducing the dependency on centralized systems and facilitating increased speed of information dissemination [6]. WSNs have enough flexibility to be used in various deployment scenarios such as urban areas and hazardous zones where traditional infrastructure might not exist or be impaired [7]. As digital technologies increase in importance within the Armed Forces, the role of WSNs is undergoing a change at an accelerated pace [8]. WSNs do not just improve the military capabilities, they aid in early detection and probability-based threat detection in real time [9]. The superior sensing capabilities and natural wireless communication abilities of WSN make them a part of modern military planning. WSNs serve as a technological basis for enhancing operational flexibility and accountability to support

national security and defense readiness [10, 11]. The challenge of secure and reliable communication in military WSN applications in the face of hostile, distributed, and dynamic operating environments. These networks are open to threats like computer programs and rare energy resources, nodes, and problems with infiltration attempts when there is no central control. This makes it hard to keep skills and safety at the same time.

Research aims to mitigate the risks associated with infiltration and decentralized design in military wireless sensor networks by creating a secure, dependable, and energy-efficient routing system. It connects a block chain-competent Safe Routing Protocol (BESP), which appoints mild block chain for decentralized authentication and secure node-to-node communication, with a deep learning model (SSLO-Bi-LSTM-ATT) for adaptive ID. The research's key contributions are as follows:

- The WSN-DS dataset, which includes 374,661 instances and 19 characteristics for WSN ID, serves as a large-scale benchmark.
- A prototype of a lightweight blockchain-based authentication and trustful routing protocol developed to be implemented in autonomous military WSNs.
- Developed the SSLO-Bi-LSTM-ATT model, which was optimized using Seven-Spot Ladybird Optimization to identify intrusions in a changing battlefield setting.
- Applied z-score normalization of the recorded sensor data to enhance the stability in the training process and the accuracy of the anomaly detection.

The research initially identifies gaps in the literature by reviewing relevant studies on blockchain applications, ID, and safe routing in WSN. Next, it describes the suggested approach, which combines secure routing for military sensor nodes enabled by blockchain technology with ID based on deep learning. Following a conclusion that summarizes contributions and prospects, the simulation findings are examined and contrasted with current practices.

2. Related Review Articles

Blockchain-based security measures, ID techniques, and routing protocols have been examined in previous research on WSN. Nevertheless, the majority of methods encounter difficulties, including excessive energy usage, restricted flexibility, and inadequate robustness in military environments.

Table 1. Dataset Samples features of WSN-DS

Authors & Year	Key Method/Approach	Main Contributions	Limitations
Rajasoundaran *et al.*, 2021 [12]	GBCRP (GAN-based Blockchain routing with FDGAN for ID)	Enhanced routing performance, security, energy efficiency in DMSNs	High computational complexity and overhead 1.-Article-Military-Wireless-Sensor-Networks-1.docx
Singh *et al.,* 2023 [13]	Deep ANN for k-barrier prediction using Monte Carlo features	High accuracy, low RMSE for border surveillance ID	Limited scalability in real-time large-scale deployments 1.-Article-Military-Wireless-Sensor-Networks-1.docx
Subotha & Femila, 2024 [14]	VMRF (Modified red fox optimization + SIEVC for path selection)	Improved malicious node detection, energy efficiency, latency in border monitoring	Scalability and complexity in large dynamic networks 1.-Article-Military-Wireless-Sensor-Networks-1.docx
Zibetti *et al.,* 2022 [15]	IoT-based context-aware environmental monitoring for battlefield	Optimized resource usage, robust communication in LPWAN	Large-scale implementation and security challenges 1.-Article-Military-Wireless-Sensor-Networks-1.docx
Okine et *al.,* 2024 [16]	Distributed MADRL routing against jamming attacks	Improved PDR, reduced latency, energy efficiency	Computational complexity in highly dynamic environments 1.-Article-Military-Wireless-Sensor-Networks-1.docx
Shanmathi *et al.,* 2024 [17]	CNN-Fuzzy Logic + NGO-LEACH for rogue node detection	Longer lifetime, higher PDR, low delays, energy efficiency	Model complexity and data processing deficiencies 1.-

			Article-Military-Wireless-Sensor-Networks-1.docx
Kaur *et al.,* 2025 [18]	Deep learning + blockchain DV-hop for DDoS mitigation	Reduced location errors, high accuracy, low FPR/FNR	High computation costs, scalability in dynamic contexts 1.-Article-Military-Wireless-Sensor-Networks-1.docx
Raj & Babu, 2022 [19]	Situation-aware selective resource algorithm for surveillance	Reduced transmissions, increased longevity, better resource use	Limited focus on control message overhead 1.-Article-Military-Wireless-Sensor-Networks-1.docx
Almaslukh, 2021 [20]	Deep learning with ANNs and entity embedding for ID	Outperformed SOTA on feature representation	Restricted to single dataset 1.-Article-Military-Wireless-Sensor-Networks-1.docx
Pathak & Yadav, 2025 [21]	Hybrid DT-KNN for anomaly detection	High accuracy, reduced false alarms	High processing cost and scalability issues 1.-Article-Military-Wireless-Sensor-Networks-1.docx
Singh *et al.,* 2022 [22]	SVR for k-barrier prediction with log transform/scaling	High accuracy (R=0.98), low RMSE	Simulation-based validation only 1.-Article-Military-Wireless-Sensor-Networks-1.docx
Pathak & Yadav, 2025 [23]	Fault-tolerant self-organized authentication with DT	98-99% PDR, 20-25% energy savings	Scalability, real-world validation, complex attacks 1.-Article-Military-Wireless-Sensor-Networks-1.docx

2.1 Research gap

Notwithstanding considerable strides made in the area of secure routing and identity provision for military wireless sensor networks (WSNs), the conventional paradigms still struggle with high computational cost, scalability issues and energy consumption concerns. The GAN-based blockchain routing protocol (GBCRP) improved the security and operational energy-efficiency in) decentralized military sensor networks; however, it came with significant computational overhead and pressure, thus to reduce its feasibility for practical implementation. Similarly, the ANN based career ID model has shown a high prediction accuracy, but there are still uncertainties about the scale to operate the model in real-time and in large environments. These shortcomings highlight the need for a safe routing architecture that is by default adaptable, scalable and lightweight. Adaptable, by mixing a mild block chain for decentralized authentication with SSLO-BI-LSTM-Att for adaptable, scalable IDs and BRP, the proposed architecture outside its deficiencies is proposed. It reduces the use of energy, improves scalability and reduces calculation overhead. It is ideal for dynamic military sensor networks due to the benefits, including increase in safety, reliable data integrity, increased throws, low package loss and reasonable energy use.

3. Methodology

The system employs self-sustained sensor nodes for instantaneous tracking of battlefield parameters and identification of intrusion. The WSN-Ds dataset is employed in this context. Afterwards, the unlabelled dataset is pre-processed through z-score normalization. An SSLO-Bi-LSTM-ATT model optimized carries out an analysis of data patterns for the identification of anomalies for adaptive and accurate identification of threats. For secure routing, the BESRP protocol uses a lightweight blockchain to authenticate node-to-node communication. Together, these provide decentralized trust, enhance data integrity, reduce energy consumption, and optimize routing performance. Figure 1 shows the Blockchain-Enabled SSLO-Bi-LSTM-ATT for Secure and Efficient Battlefield Anomaly Detection in WSN.

3.1 Dataset

The WSN-DS dataset for ID in WSN contains 374,661 instances with 19 attributes. Time, node tasks, proximity to the cluster head, energy usage, data transmission, and communication of control packets are some of its features. The data can be used to conduct research on IoT security and anomaly detection with annotations of traffic as normal or belonging to numerous attacker types, like flooding, scheduling, blackhole, and grayhole. Table 2 shows samples of data features.

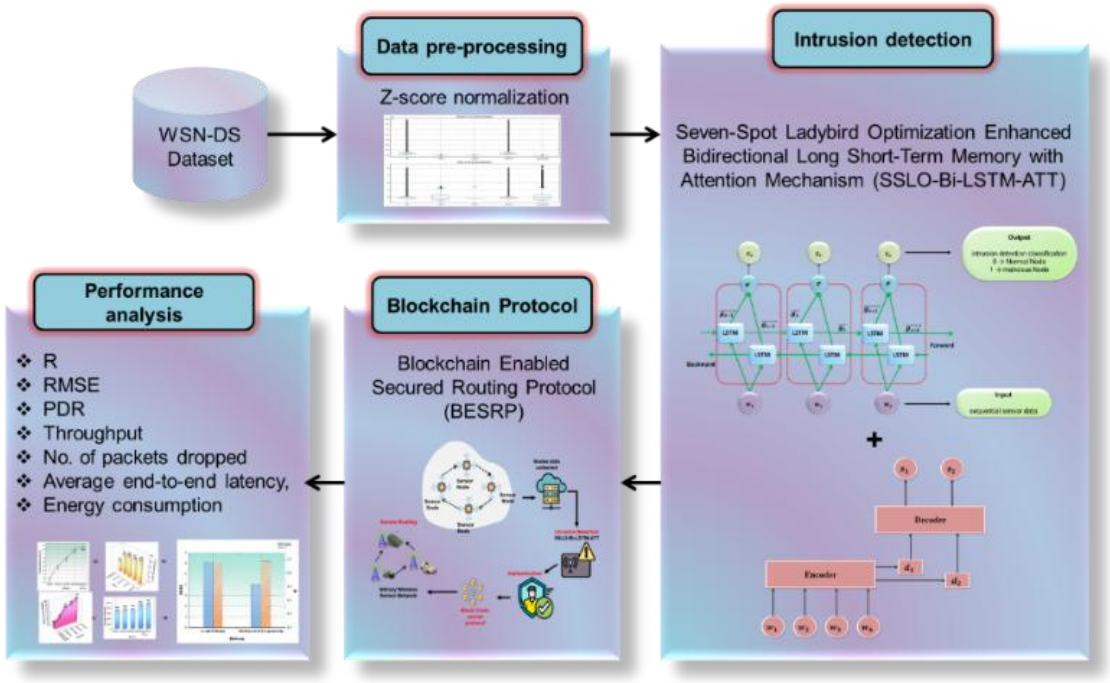

Figure 1. The SSLO-Bi-LSTM-ATTFramework with Blockchain Technology for Secure and Effective Military Anomaly Diagnosis in WSN

Table 2. Dataset sample features of WSN-DS

id	Time	Is_CH	who CH	Dist_To_CH
101000	50	1	101000	0
101001	50	0	101044	75.32345
101002	50	0	101010	46.95453
101003	50	0	101044	64.85231
101004	50	0	101010	4.83341
101005	50	0	101010	31.91198

Source: https://www.kaggle.com/datasets/bassamkasasbeh1/wsnds

3.2 Data pre-processing

Energy consumption, distance to cluster head, and data transmission rate features are levelled to a standard level in the context of the ID of WSN by the use of Z-score normalization. It transforms feature values by turning down the effect of the various units and ranges to get a mean of 0 and a standard deviation (std) of 1, which enhances the work of deep learning models. The mathematical expression is given in equation (1), where W' is the normalized value, and W is the original feature value.

$$W' = \frac{W - mean}{std} \quad (1)$$

Figure 2 shows the before and after normalization, clearly showing how the values are standardized around mean = 0 and sdt = 1.

3.3 Intrusion detection using SSLO-Bi-LSTM-ATT

To provide secure and energy-efficient routing in blockchain-enabled military WSNs, the suggested SSLO-Bi-LSTM-ATT technique combines optimization, deep learning, and attention methods. To ensure rapid convergence and higher detection accuracy, the SSLO algorithm first optimally optimizes the Bi-LSTM parameters. BI-LSTM involves all temporary addiction to identify reliable deviations by processing the front and rear sensor data. The attention mechanism improves the detection of harmful activity by providing high -weight important sensor functions to further improve performance.

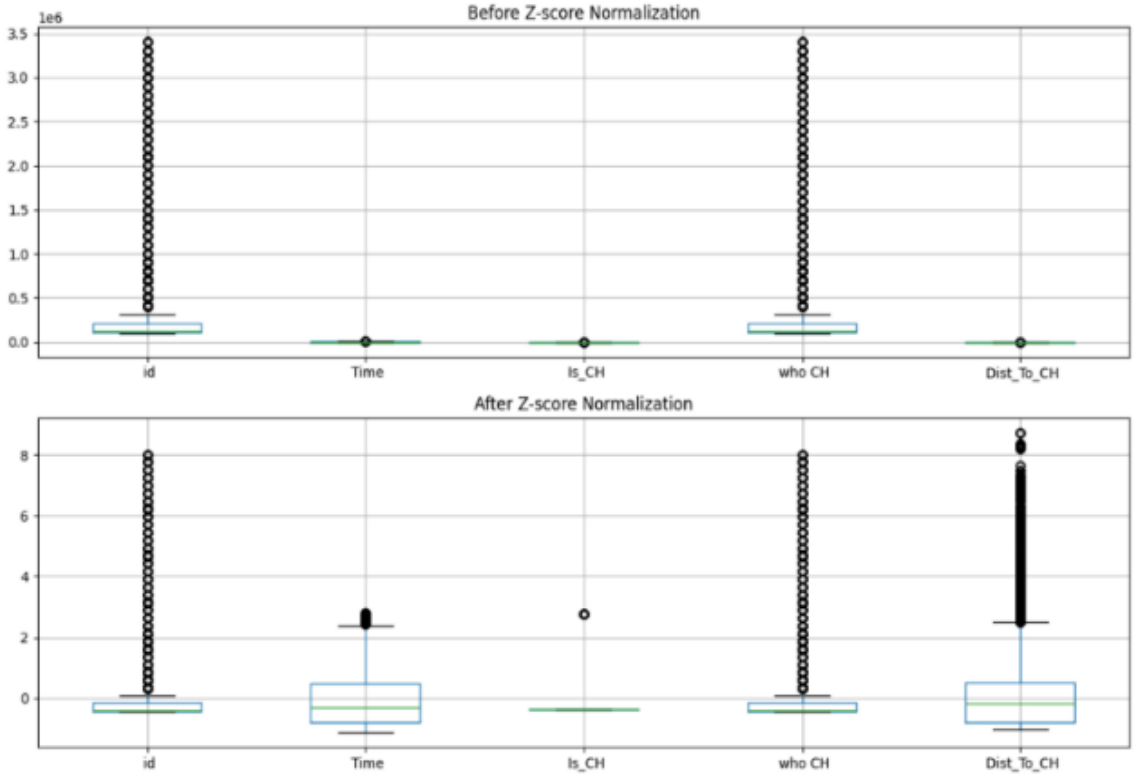

Figure 2. Before and After Z-score normalisation of the Data feature.

Proclaimed, reliable and energy efficient data transfer was secured by the proposed structure, combined with blockchain-based decentralized authentication. Overall, SSLO-Bi-LSTM-ATT improved ID, lowered energy usage, minimized packet loss, and offered robust routing appropriate for complex and difficult military environments. Algorithm 1 illustrates the SSLO-Bi-LSTM-ATT method process.

Algorithm 1. Process of SSLO-Bi-LSTM-ATT

Input: WSN_Data (*sensor readings, node states, routing inf*
Output: *Intrusion_Status, Secure_Routing_Path*
Begin
Preprocessing
Normalize WSN_Data *using* $Z-score$ *normalization*
Extract features: *time, energy, distance, traffic, control pa*
Initialize SSLO Optimization
Define search space for Bi $-$ *LSTM parameters* (*weights, biases, learning rate*)
Divide into patches (*subspaces*)
Initialize ladybird population W_j *in each patch*
Evaluate fitness for each ladybird:
Fitness $= f(Energy\_Efficiency, Detection\_Accuracy, Packet\_Loss)$
$Bi-LSTM$ *Anomaly Detection*
Initialize $Bi-LSTM$ *with Optimized_Parameters*
For each sequence in WSN_Data:
$Forward\_Hidden \leftarrow BiLSTM\_Forward(sequence)$
$Backward\_Hidden \leftarrow BiLSTM\_Backward(sequence)$
Combined_Output $G\_s \leftarrow Merge(Forward\_Hidden, Backward\_Hidden)$
End For
Attention Mechanism
For each hidden state g_j in Combined_Output:
$v_j \leftarrow tanh(W * g_j + b)$
$\alpha_j \leftarrow exp(v_j^T * v_x) / \Sigma(exp(v_j^T * v_x))$
End For
$Context\_Vector \leftarrow \Sigma(\alpha_j * g_j)$
$Intrusion\_Status \leftarrow Classifier(Context\_Vector)$
SSLO Parameter Optimization
While termination condition not met:
For each ladybird:
Update position using local/global search equations
Compute new fitness
If improved $\rightarrow$ *update self* $-$ *best, local* $-$ *best, global* $-$ *best*
End For
End While
$Optimized\_Parameters \leftarrow global-best\ solution$
STEP 6: $Blockchain-based\ Secure\ Routing$
If $Intrusion\_Status = "Normal"$:
Generate transaction record
Verify node via blockchain consensus
Route packets via BESRP protocol
Else
Mark node as malicious
Block routing through compromised path
End If
Output Results
Return Intrusion_Status, Secure_Routing_Path
End

3.3.1 Bidirectional LSTM

To identify intrusions in the suggested architecture for safe routing in military WSN enabled by blockchain, it is essential to record both past and future context in sequential data. Two hidden layers are used by BiLSTM to process sensor data both forward and backward, combining them into a single output. By ensuring that past and future signal dependencies are taken into account, in military contexts, this dual-directional learning increases anomaly detection's precision and reliability. The activation results from the forward and backward layers are included in the BiLSTM hidden layer output. The following formulae provide their expressions in equations (2-4).

$$\vec{g}_s = \sigma\left(X_{\overrightarrow{wg}} w_s + X_{\vec{g}\vec{g}} \overrightarrow{g_{s-1}} + a_{\vec{g}}\right) \quad (2)$$

$$\overleftarrow{g}_s = \sigma\left(X_{\overleftarrow{xg}} w_s + X_{\overleftarrow{g}\overleftarrow{g}} \overleftarrow{g_{s-1}} + a_{\overleftarrow{g}}\right) \quad (3)$$

$$G_s = X_{\overrightarrow{wg}} \vec{g} + X_{\overleftarrow{xg}} \overleftarrow{g} + a_z \quad (4)$$

The input at time step s was w_s. The forward hidden state at time s is defined as $\vec{g}_s$. $\overleftarrow{g}_s$ was the backward hidden state at time s. The forward hidden value from the past time step was $\overrightarrow{g_{s-1}}$. The backward hidden value from the subsequent time step (reverse direction) was indicated by $\overleftarrow{g_{s-1}}$. The forward and backward layers' input weight matrices were denoted by $X_{\overrightarrow{wg}}$ and $X_{\overleftarrow{xg}}$. σ was the activation function. The recurrent weight matrices for the forward and backward layers are denoted by $X_{\vec{g}\vec{g}}$ and $X_{\overleftarrow{g}\overleftarrow{g}}$. Bias phrases for forward and backward layers were indicated by the symbols $a_{\vec{g}}$ and $a_{\overleftarrow{g}}$. The result for ID was G_s, which was the integrated hidden state at time s. Weight matrices for merging forward and backward hidden states were developed by $X_{\overrightarrow{wg}}$ and $X_{\overleftarrow{xg}}$. BiLSTM incorporates all temporal connections by analyzing sequential sensor data in both the direction of forward motion and backward motion. Concurrently learning patterns from previous and imminent sensor activities improved the accuracy of ID in military WSNs. Figure 3 illustrates the architecture of Bi-LSTM.

3.3.2 Attention (ATT) mechanism

High detection accuracy is attained when the ATT mechanism is used for the military WSN ID task. It provides the attention technique to extract the most important characteristics from the data, improving anomaly recognition and secure routing performance, as each sensor feature has a different level of value in detecting intrusions. The Bi-LSTM model for ID in military WSNs is made more effective by using the attention mechanism. Since variables in sensor data have different levels of significance, the attention mechanism enables the model to give key features that readily demonstrate incursions of higher weights.

The attention mechanism consist of two primary modules: the encoder, which processes the raw sensor inputs and extracts hidden representations, and the decoder, which creates the output (normal or intrusive) by focusing on the most crucial elements using the attention weights. The following equations (5-7) control the attention mechanism:

$$v_j = \tanh\left(X_j g_j + a_j\right) \quad (5)$$

$$\alpha_j = \frac{\exp\left(v_j^S v_x\right)}{\sum_j \exp\left(v_j^S v_x\right)} \quad (6)$$

$$g_j = \sum_j \alpha_j g_j \quad (7)$$

The g_j stands for the hidden state vector, which represents characteristics that were taken from the sensor data series at the j^{th} time step. X_j was the weight matrix that mapped hidden states into the attention space throughout the attention calculation process.

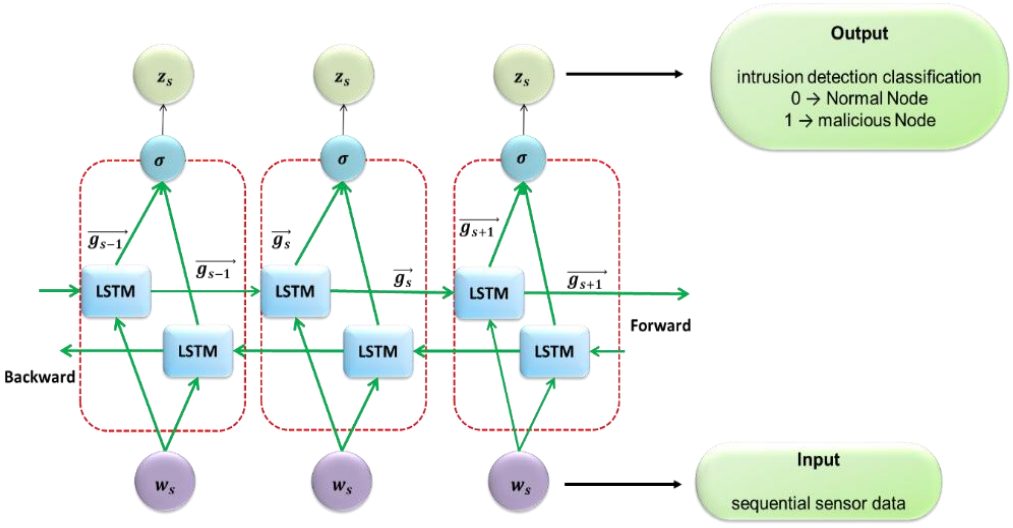

Figure 3. Bi-LSTM framework of Backward and Forward motion

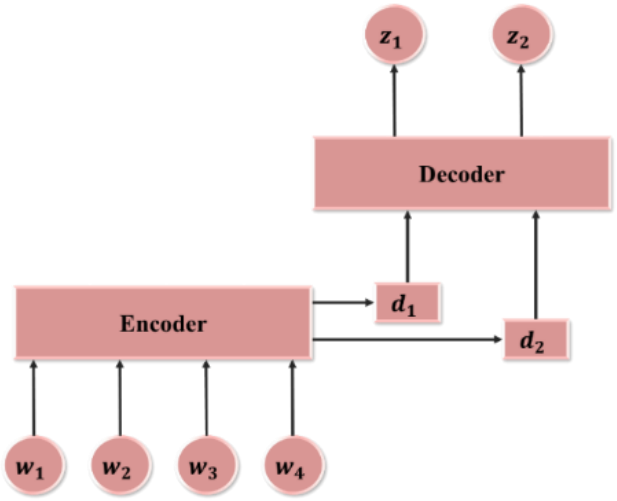

Figure 4. Attention mechanism framework

a_j defines the bias concept related to the change of attention. v_j is the intermediary attention expression for the j^{th} input feature and s was the transpose operators, calculated with the hidden state and trainable weights. v_x was the context vector (randomly initialized and modified throughout training), which represented the overall relevance of features in the dataset. α_j is the attention score (normalized weight) for the j^{th}characteristic, which indicates its relevance. $tanh(\cdot)$ is the non-linear activation function that ensures feature transformations are limited. The exponential function used to score significance is represented by $exp(\cdot)$. $\sum_j$ defined the summation over all features to normalize attention weights into probabilities. Figure 4 depicts the ATT mechanism architecture.

The Bi-LSTM model uses the attention mechanism to ignore redundant information and prioritize the most pertinent sensor properties for ID. This reduces false alarms and increases detection accuracy.

3.3.3 Seven-spot ladybird Optimization (SSLO)

The adaptive ID in military WSNs, the parameters are optimized using the SSLO method. The technique offers safe routing with small energy overhead and improved detection accuracy by optimizing the procedure. The ecological efficacy and social habits of the seven-spot ladybird, Coccinella septempunctata, have drawn the attention of an increasing number of expert entomologists. They communicate and pass on information to others mostly by pheromones, comparable to most types of insects. Some of the seven-spot ladybirds' chemical ecologies, with a focus on semiochemicals that are important for their social interactions and feeding habits. The followings were the primary steps:

Dividing Patches: A D-dimensional environment is considered the search space, representing the potential values of the model parameters. The m-dimensional space is divided into m_j subspaces for each dimension, as shown in equation (8).

$$m = \prod m_j \tag{8}$$

Subspaces (patches) represent a region of potential parameter solutions.

Initializing Population: A potential solution is represented by each seven-spot ladybird (parameter vector). The symbol for the j^{th} ladybird was described in equation (9).

$$\mathrm{W_j} = (\mathrm{w_{j1}}, \mathrm{w_{j2}}, \ldots, \mathrm{w_{jD}}) \tag{9}$$

Where $\mathrm{W_j}$ is an optimized parameter search vector in D dimensions. When initializing n ladybirds in a patch, M was the overall population, which was defined as follows in equation (10).

$$M = n \times m \tag{10}$$

Calculating Fitness: The fitness function assesses each ladybird's solution based on the WSN's energy efficiency, routing dependability, and ID accuracy.

Choosing the Best Ladybird: The present position of each ladybird was compared to its self-best. Local-best was contrasted with the patch's optimal location. The best locations across all patches (representing the overall optimal solution) were contrasted with the global-best (h_{best}).

Dispersal: A new position is created close to the global best (h_{best}) to preserve variety if a ladybird's position does not improve within a predetermined number of cycles (limit).

$$W'_{j,i} = w_{h_{best,j}} + \emptyset \mathrm{x} \tag{11}$$

The equation (11) j^{th} ladybird's new location in the i^{th} dimension was $W'_{j,i}$. The i^{th} element of the global best solution was specified by $w_{h_{best,j}}$. The h_{best}

neighborhood search space was x. $\emptyset$ is the random number in the interval $[-1,1]$.

Updating Positions: Ladybirds update their positions depending on intensive search (exploring local optima) or extensive search (exploring globally). Intensive search equations (12-13). A ladybird transitions to extended search after performing an intense search. The following equations (14-15) were used to modify the position:

$$U_j(s) = d * q_1 * \left(T_j(s) - W_j(s)\right) + \epsilon_1 \quad (12)$$

$$W_j(s+1) = W_j(s) + U_j(s), \left|U_j(s)\right| \leq U_{max} \quad (13)$$

$$U_j(s) = d * q_2 * \left(K_j(s) - W_j(s)\right) + \epsilon_2 \quad (14)$$

$$W_j(s+1) = W_j(s) + U_j(s), \left|U_j(s)\right| \leq U_{max} \quad (15)$$

Where $W_j(s)$ was the j^{th} ladybird's location at iteration s, and $W_j(s+1)$ was its updated position. The velocity of the j^{th} ladybird at iteration s was specified as $U_j(s)$. Ladybird I's self-best posture is represented by $T_j(s)$. $K_j(s)$ displays the patch's local-best location. The step size was controlled by the positive constant d. The random integers in [0, 1] were q_1, q_2. The small random noise terms were specified by ϵ_1 and ϵ_2. Search precision control's maximum velocity is denoted by U_{max}. The equation (16) defined the velocity constraint.

$$U_{max} = 0.2(ub - lb) \quad (16)$$

Where ub is the search space's upper bound and lb defines the search space's lower bound.

Inspecting Termination Condition: Optimization is terminated if the termination condition has been satisfied. If not, the procedure goes back to calculated fitness.

The proposed SSLO-Bi-LSTM-ATT method optimizes ID and secure routing in blockchain-enabled military WSNs. SSLO's algorithm optimizes the parameters of a bidirectional (Bi-) long short term memory (LSTM) network in order to be computationally efficient while the Bi-LSTM network architecture learns both historical and prospective dependency from the context at the same time, and in parallel, an attention mechanism will make the most important features of the obtained sensor data stand out. When interfaced with the blockchain-based authentication, this type of composite system attains better detection accuracy, strengthened security schemes, energy efficiency, significant reduction of packet losses, and reliable data transmissions inside the hostile military operational environment.

3.4 Blockchain Enabled Secured Routing Protocol (BESRP)

In order to ensure the secure and effective routing in autonomous military wireless sensor networks, a novel protocol called BESRP has been proposed. By virtue of collaborative resources of adaptive anomaly detection and lightweight blockchain implementation, BESRP: Obviates the need for centralized control that is the hallmark of conventional routing methodologies; Allows reliable inter-node communication; and Eliminates the comparison of round-trip delay-time from outgoing and returning packets to the host machine. Figure 5 shows the BESRP architecture of military wireless sensor networks.

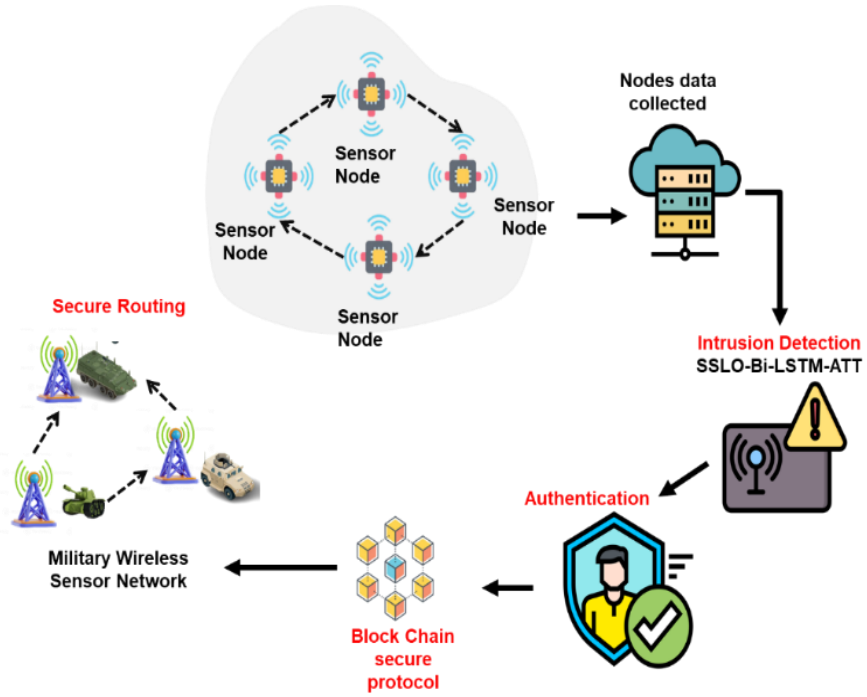

Figure 5. BESRP architecture for ID and secure routing for military WNS

Authentication Mechanism: Every sensor node is included on the blockchain ledger with a distinct digital identity. When two nodes want to communicate, consensus verification is used to confirm their identities. This prevents any malicious nodes from accessing the routing path. Equation (17) definition of the authentication function is $Auth(M_j, M_i)$.

$$Auth(M_j, M_i) = \begin{cases} 1, if\ Hash(M_j \| M_i \| S) = valid \\ 0, otherwis \end{cases} \quad (17)$$

The nodes that were in communication were M_j and M_i. S represents the transaction's timestamp. The blockchain hash verification was specified by $Hash(\cdot)$. Output 1 indicates that the transmission was authenticated, whereas 0 indicates that it was denied.

Routing Process: After successful authentication, BESRP creates dynamic routing paths using Bi-LSTM-ATT based anomaly detection and blockchain-verified trust scores. Suspicious activity nodes are removed from the routing table. The routing decision $\left(Route(M_j, M_i)\right)$ can be described as follows in equation (18):

$$Route(M_j, M_i) = \arg\max(Trust(M_l) - Energy\ (M_l)) \quad (18)$$

Where the blockchain-verified trust score of node M_l is denoted by $Trust(M_l)$. Node M_l remaining energy was denoted by $Energy(M_l)$. This approach is chosen to minimize energy costs and increase trustworthiness.

- Lightweight blocks are produced by BESRP on every routing transaction.
- Node IDs, trust scores, timestamps, and digital signatures are all included in each block.
- Consensus validation ensures the route records' integrity and immutability.

Decentralized trust in the absence of centralized power. A lightweight, dynamic blockchain uses less energy. Routing over vulnerable nodes is avoided by integration with Bi-LSTM-ATT. Ensures energy-efficient, secure, and dependable routing in challenging military environments.

4. Result Analysis

The result shows the performance assessment of the suggested framework, emphasizing how well it ensures data transfer that is reliable, secure, and energy-efficient. It demonstrates how the integration of deep learning and blockchain strengthens military wireless sensor network operations. Python 3.9 was used to implement the experimental setup. The 100 sensor nodes are used in the evaluation.

The relationship between distance to Cluster Head (CH) on the x-axis and distance from CH to Base Station (BS) on the y-axis under different attack types. Most of the normal nodes are clustered within distances from 0 to 200 units with respect to the cluster head and 50 to 175 units with respect to the base station. On the other hand, some anomalous conditions, namely Flooding, TDMA, Grayhole and Blackhole occur at a distance of approximately zero from the base station, thus representing different intrusion patterns. Figure 6 shows the spatial relationships of distances between nodes and the cluster head and the base station for different attack modalities.

The numerical features of the network have strong correlations. JOINR and SCHS (0.61) and JOINS and SCHR (0.90) exhibit strong positive relations while inverse dosages are suggested by negative correlations between SCHR and distCHToBS (0.68) and between JOINS and distCHToBS (0.76).

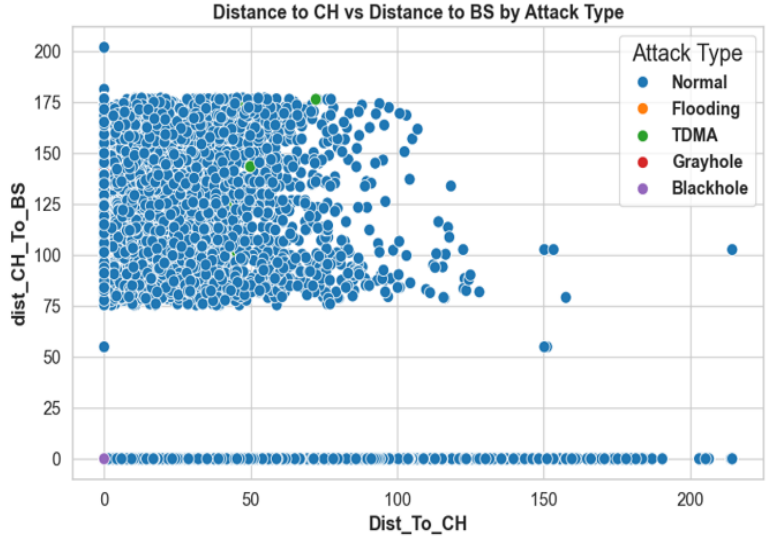

Figure 6. Node Distances to Cluster Head and Base Station under Various Attack Types

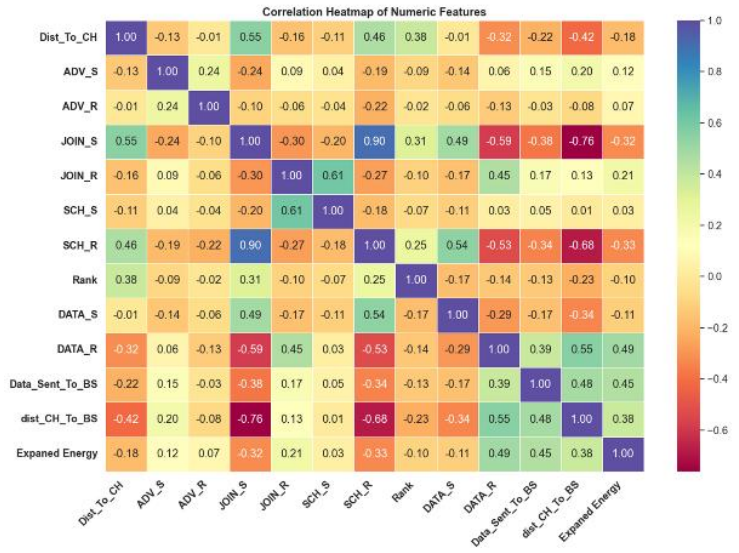

Figure 7. Correlation Heatmap of Network Performance Features

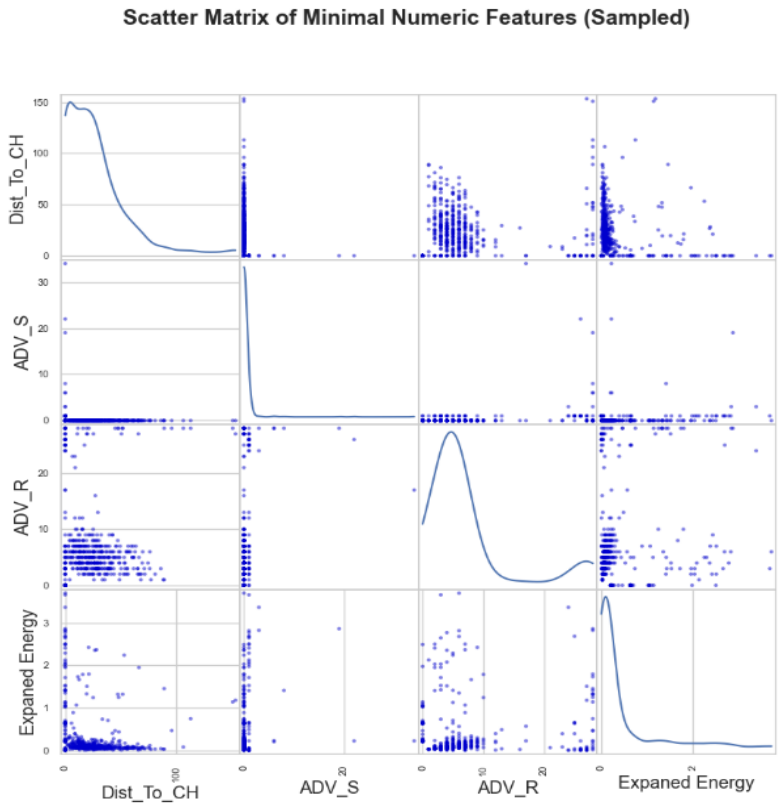

Figure 8. Scatter Matrix of Key Network Parameters

Communication interdependence is highlighted by data transmission indicators, i.e. DATAR and Data Sent to BS (0.39) and DATAS with SCH_R (0.54). As a whole, the interrelation between energy, scheduling and distances in network activities can be seen in Figure. 7.

The correlation between the terms Dist_To_CH, ADV_S, ADV_R, and Expanded Energy was tested. Most Dist_To_CH values were clustered in the interval 0-150 while both ADV_S and ADV_R were concentrated in the interval 0-20. Expanded Energy was by far mostly below 2 units with only some scattered outliers. Distribution patterns can be seen in figure 8 where a strong reduction in the frequency of ADV_S values of approximately 10 and a clustering of ADV_R values of less than 15 are evident. Overall the chart defines a density, spread and correlations between these network parameters.

Differences in DATAR values at different time periods are documented. Temporal values range from 0 to 3600 units while DATAR values range closer to 1500. Figure 9 shows that there are frequent fluctuations, with values lying mostly in the range of 200 to 1200 and periodically reaching 1400.

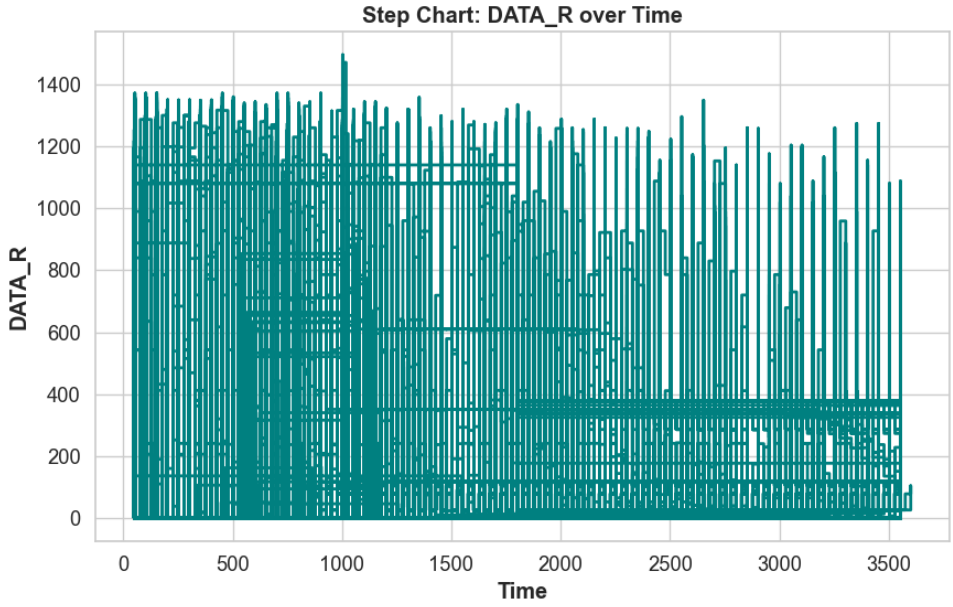

Figure 9. DATA_R Variation over Time

These patterns tip off a continual data psychology as well periodic in between and just ways indicates in between intervals, which may be interpreted as suggestive of network activity as well as load processing efficiency.

4.1 Comparative Analysis Result

Wireless sensor networks (WSNs) which are used in military situations require high levels of security, reliable connectivity and low-power consumption in harsh and resource-constrained environments. The current technique has major shortcomings in terms of ensuring secure and energy-efficient routing. LT -ZM - FFNN [24] faces unreasonable calculation complexity, not adaptable to the dynamic environment, and energy consumption is higher, which is not as applicable to the real-time wireless sensor networks for military purposes. DSR [25] suffers from the heavy routing overhead, frequent route discovery and malicious node attack vulnerability to reduce the efficiency and security in military sensor networks. AODV [25] is challenged by frequent route failures, high levels of packet loss, and flooding attacks making it unfavorable for critical applications with respect to reliability and energy efficiency. QAODV [25] provides better performance at the cost of increased complexity, resource usage, and failure in high mobility environments, which eliminates it from being considered in the energy-constrained, rapidly evolving military wireless environment. SRABC is plagued by slow convergence and a high degree of control message overhead and insufficient security implementation, making it unsuitable for large scale, hostile, and energy sensitive military sensor deployments. Taylor C,-SSA [26] shows poor scalability, high computational cost and difficulty in balancing the exploration and exploitation process, which leads to increased delay and diminished energy-efficiency in military WSN routing. QIEAC - QI Amid the premises of the wireless sensor networks in the field of military activities, QIEAC - QIEAC - CSSBO [26] is limited by premature convergence, weak resistance to intrusion, and great energy consumption, which limits its effectiveness for secure and long-lasting military wireless sensor network operations.

Performance differences between proposed SSLO-Bi-LSTM-ATT technique and current methods are illustrated. Correlation coefficient (R), root mean square error (RMSE), packet delivery ratio (PDR), throughput, number of dropped packets, average end-to-end latency, energy consumption and delay are the metrics used for comparison.

The correlation coefficient measures the degree of mutual accordance between the proposed model and actual decision making for routing decisions and intrusion patterns in military WSNs by comparing the predicted and actual values. RMSE measures the prediction errors of the actual and estimated outcomes, and hence helps to evaluate the accuracy and reliability of the proposed framework compared to other routing and detection methods that exist in the literature. Table 3 and Figure 10 show the particular models being compared and specify the evaluation metrics.

Various technologies have been suggested to enhance the performance of WSN routing. The comparison illustrates how accurate two predictive methods are in comparison. The LT-ZM-FFNN achieved the correlation value of R = 0.95 with an RMSE value 6.15 while the proposed SSLO-Bi-LSTM-ATT achieved the better correlation value of R = 0.97 with the lowest error value of 4.02, indicating better and efficient prediction results.

Table 3. Performance Evaluation of Different Models on the basis of R and RMSE

Methods	*R*	RMSE
LT-ZM-FFNN [24]	0.95	6.15
SSLO-Bi-LSTM-ATT [proposed]	0.97	4.02

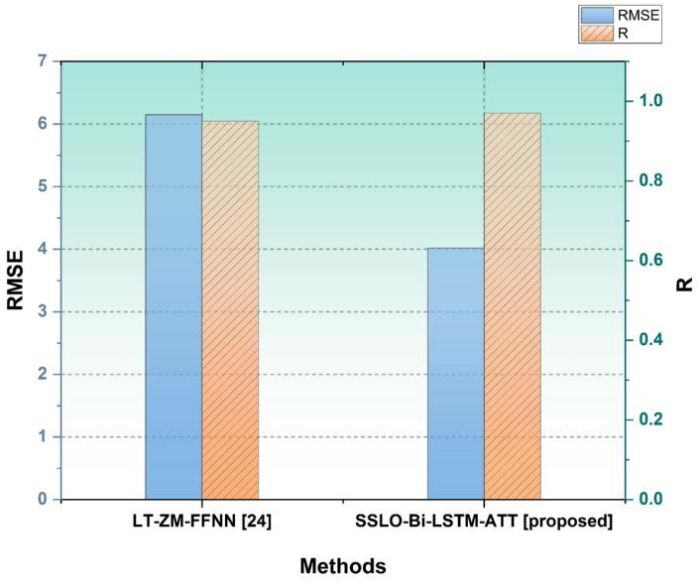

Figure 10. Assessment of Predictive Capability in Wireless Sensor Network Routing Using R and RMSE

Table 4. Evaluation of Routing Efficiency and Reliability for Various WSN Environments methods

Methods	Packet delivery ratio (%)	Throughput(Packets)	Number of packets dropped	Average end to end delay(s)
DSR [25]	91	6500	100	0.219
AODV [25]	94	6800	89	0.21
QAODV [25]	96	7000	87	0.208
SRABC [25]	98	8500	69	0.20
SSLO-Bi-LSTM-ATT [proposed]	98.7	9000	60	0.11

Packet Delivery Ratio (PDR) represents the ratio between the successfully delivered packets, hence to have a reliable communication in military WSNs, the packet loss should be minimized during the secure and energy-efficient data transmissions. Throughput is a measurement of successful packets delivered per unit of time, which is an indication of system efficiency to handle large data flows in secure and hostile battlefield environments. The quantity of packets dropped measures dropped packets in transmission, and hence it is a direct measure of reliability of the network and effectiveness of routing strategies in network management of data losses in military scenarios. Delay considers the amount of time between the time when data originates and the time when data reaches its end destination and that the proposed data protocol will aid in making military decisions in a timely manner with minimal time delays. Energy consumption is an indicator of the efficiency of power utilization of sensor nodes, the key factor for enabling long term deployments of WSN in the military environment with limited resources.

The proposed methods have been compared against the existing protocols namely DSR, AODV, QAODV and SRABC. Table 4 and Figure 11 (a-d) show the comparative study of the suggested approach with the current approaches based on several calculated parameters.

The proposed SSLO- Bi-LSTM-ATT approach possesses significantly superior performance compared to the state-of-the-art routing approaches in all major aspects. Figure 11(a) shows the packet delivery ratio (PDR) which achieves 98.7%, which is much higher than SRABC (98%), QAODV (96%), AODV (94%) and DSR (91%) and achieves more reliable data transmission.

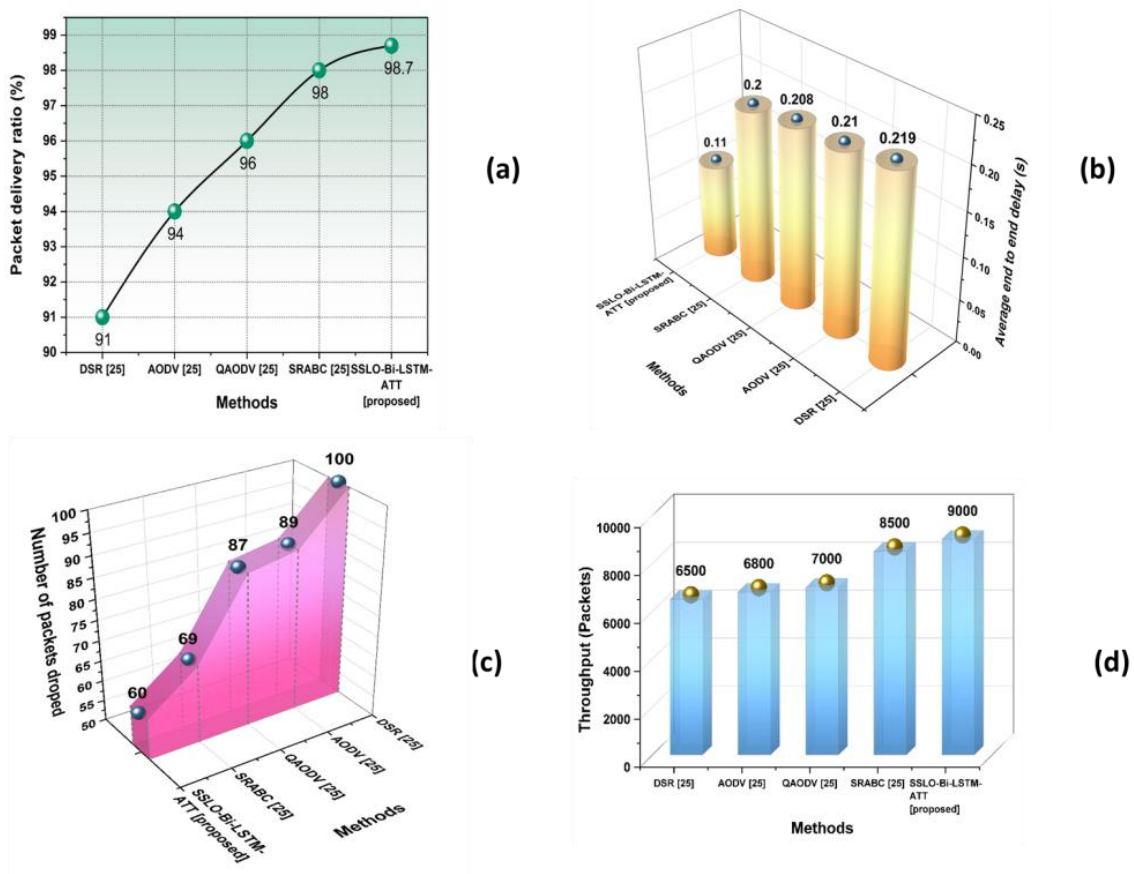

Figure 11. Comparison Assessment of WSN Scenarios models term of different metrics **(a)** Packet delivery ration, **(b)** Delay, **(c)** No. of packet dropped and **(d)** Throughput

Table 4. Performance Evaluation of Routing Techniques in a 100-Node Scenario Based on Metrics.

Methods	Energy consumption (J)	Delay (ms)	Throughput (bps)
Taylor C-SSA [26]	17	14	782
QIEAC-CSSBO[26]	15	12	865
SSLO-Bi-LSTM-ATT [proposed]	12	11	952

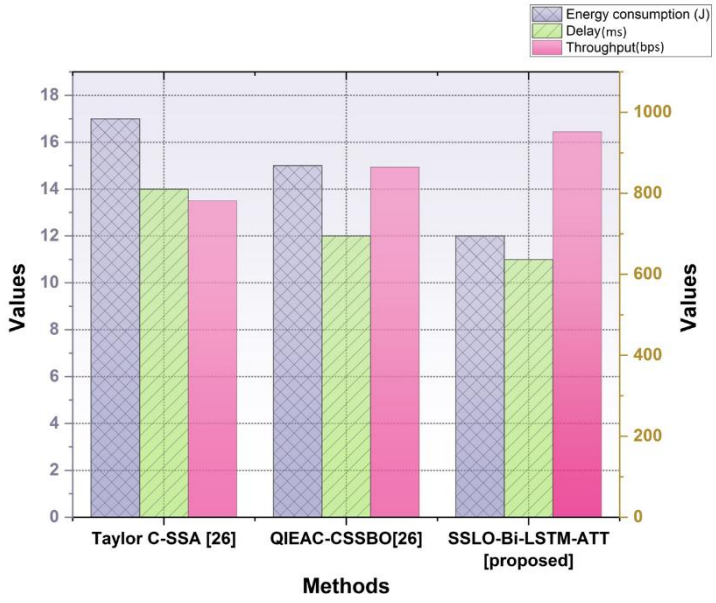

Figure 12. Network Efficiency and Communication Performance across Different Techniques in a 100-Node Environment

As throughput is given in Figure 11(d), it reaches 9000 packets that exceed SRABC 8500, QAODV 7000, AODV 6800 and DSR 6500, and this proves its efficiency to cope with larger data flows. Moreover, Figure 11(c) presents the number of dropped packets according to the proposed method which is only 60, lower than SRABC (69), QAODV (87), AODV (89) and DSR (100) which enrich the reliability of the proposed method. Finally, Figure 11(b) reveals that the proposed method has the shortest end to end delay of 0.11 s that surpasses SRABC (0.20 s) and QAODV (0.208 s), AODV (0.21 s) and DSR (0.219 s) and it shows that the proposed method achieves faster and more responsive communication. Overall, the results confirm that the proposed method provides greater reliability, efficiency and timeliness compared with the traditional approaches.

The performance of the SSLO - Bi - LSTM - ATT method is tested in a network scenario which contains 100 nodes and compared with the prevailing Taylor C - SSA [26] and QIEAC - CSSBO [26] techniques. Table 4 and Figure 12 show a comparative analysis of the various methods under 100 node configuration.

The SSLO-Ray Results of the model SSLO Bi-LSTM-ATT are superior in terms of energy consumption (12 J) of the electronic device when compared with QIEAC-CSSBO (15 J) and Taylor C-SSA (17 J). Concerning delay, proposed approach is the fastest having latency of 11 ms compared to 12 ms of QIEAC-CSSBO and 14 ms of Taylor-C-SSL, hence allowing faster communication. Moreover, the method is able to achieve the highest throughput of 952 bps, which is higher than 865 bps in QIEAC - CSSBO and 782 bps in Taylor - CSSA, indicating a higher data - transfer capacity. These enhancements collectively show that the presented solution is superior in terms of energy consumption, latency and capacity compared to existing alternatives.

The proposed SSLO,-Bi,-LSTM,-ATT scheme contains energy efficient secure routing, lightweight blockchain authentication and adaptive identity management, hence overcoming the limitations of existing schemes. It lower routing cost, packet loss and accuracy of anomaly detection is improved. Such characteristics are especially useful for military wireless sensor networks that have to work autonomously, reliably and efficiently under dynamically changing combat conditions, therefore requiring good communication and strong security and reliability.

5. Discussion

When wireless sensor networks (WSNs) are implemented in military scenarios, they require advanced security measures, high-quality communication, decentralized working processes and strict energy management. Such military grade networks need to operate successfully in hostile environments where dependence on centralised infrastructure is impractical due to vulnerability and geographical limitations to targeted attacks. This requirement is very different than the design considerations found in the typical civilian WSN deployment. The present study aims to deal with these challenges by presenting a Blockchain Enabled Secured Routing Protocol (BESRP) along with the SSLO-Bi-BLSTM-ATT, a deep learning-based intrusion detection model. The combination of these parts helps to establish decentralized trust relationships and at the same time to adaptively detect anomalies.

Empirical results show that the integration of blockchain technology in the routing infrastructure delivers stronger privacy and integrity in data thanks to removing single points of failure. Traditional routing systems require well-known coordinators or key distribution centers as rule, which not only add some extra communication overhead but also offer exploitable bottlenecks. BESRP overcomes these limitations by dynamically building lightweight ledgers to validate transactions among sensor nodes, and thus preventing malicious nodes from injecting control data that is not in line with the system requirements without detection. This capability is especially important in a military application, where compromised data routes can compromise the confidentiality of a mission and make real-time decision-making impossible.

The incorporation of the SSLO -- Bi -- LSTM -- ATT model is invariable for detecting complex intrusion patterns during packet transmission. Deep-learn based intrusion detection, particularly the sequence learning models such as Bi-LSTM, is able to also capture any hidden correlations as well as temporal dependencies that are often missed by static detection models. The proposed model improves the classification performance using an attention mechanism that gives more weight to most salient features in a sequence. The Seven-Spot Ladybird Optimization algorithm further improves accuracy of detections and reduces false positives which are critical in mission critical settings where decisions can have a huge adverse impact on the outcome of the operation.

This research also contributes to the optimization of energy. Simulation results show that the proposed architecture outperforms the conventional alternatives in that it reduces the packet loss, limits energy consumption and increases the throughput. These benefits are due to the fact that the resource-conscious consensus mechanism on the blockchain gelled with the routing decisions based on authentication of nodes taking into account the constraints of operation. This leads to the observed increases in mission life and makes sensor deployment more sustainable, especially for military remote field deployments where life is typically maintained by battery power or other energy scavenging devices.

6. Conclusion

This research uses blockchain-enabled Safe Routing Protocol (BAKP) with deep learning-based infiltration detection system to solve the challenges of safe, skilled, and autonomous military wireless sensor networks (WSNs). The SSLO-Bi,-LSTM-ATT framework ties in lightly with the Blockchain authentication back with the model of verifying the proposed system offers the effectively secure routing; still the system is robust even with trust formed, realtime detecting deviations, and with the dangers being identified in the Simulation results show that this architecture uses low energy, has fewer packet losses, has a higher throughput compared to other methods, and provides both data confidentiality and integrity.

The novelty to a dual-layer security architecture. The routing part with blockchain removes the disadvantages of the centralized control, while the Bi-Lstm with attention mechanism enables the flexible recognition of complicated intrusion patterns. This synergistic combination creates an imposing infrastructure that is appropriate for military situations when resources are limited and missions are critical. The approach presents a scalability without reducing the quality of communication. While the empirical outcomes are promising, the practical deployment of them may face challenges like operational latency in a dynamic environment, challenges in synchronization of nodes, and Mixing up between the integration of real-world military communication data into training data sets.

The method takes advantage of the SSLO - Bi - LSTM - ATT architecture with an optimization strategy of Seven Spot Ladybird Optimization and BESRP Framework. Information is gathered by a network of sensor nodes that observe acoustic, thermal, motion - vibrational parameters in a military zone. In order to improve model stability, pre-processing was performed in the form of Z-score normalization. Experimental results show correlation coefficient (R) equals to 0.97, root-mean-square error (RMSE) equals to 4.02, packet delivery ratio equals to 98.7 %, and throughput equals to 9000 packets, packet drop equals to 60 and average delay equals to 0.11 seconds. In addition, the proposed method provides lower energy consumption (12 J), low latency (11 ms) and high throughput (952 bps) compared to existing state-of-the-art methods. The proposed framework would ultimately ensure resilience, efficiency, and secure data transfer in military wireless sensor networks.

The method may have some problems, such as trouble scaling, making computations more complicated, and dealing with latency issues when managing large, dynamic military networks. The next step is to use light deep learning models, advanced adaptation and edge computing to make process faster and more scalable. A secure block chain-based model will be able to monitor the important signs of patients in the health care system and keep their privacy and communication safe. Adaptive routing will be improved with the help of adaptive deep learning in the smart transportation sector to guarantee efficient data transmission and threat detection in real time.

References

[1] S. Pragadeswaran, S. Madhumitha S. Gopinath, Certain investigation on military applications of wireless sensor networks. International Journal of Advanced Research in Science, Communication and Technology, 3(1), (2021) 14-19.

[2] M. Chaudhary, N. Goyal, A. Benslimane, L.K. Awasthi, A. Alwadain, A. Singh, Underwater wireless sensor networks: Enabling technologies for node deployment and data collection challenges. IEEE Internet of Things Journal, 10(4), (2022) 3500-3524. https://doi.org/10.1109/JIOT.2022.3218766

[3] F. Horita, J. Baptista, J.P. De Albuquerque, Exploring the use of IoT data for heightened situational awareness in centralised monitoring control rooms. Information Systems Frontiers, 25(1), (2023) 275-290. https://doi.org/10.1007/s10796-020-10075-8

[4] J. Smith, Autonomous wireless sensor networks: A path to self-organizing systems. American Journal of Sensor Networks and Wireless Communications, 6(1), (2025) 10-18.

[5] Y. Ko, J. Kim, D.G. Duguma, P.V. Astillo, I. You, G. Pau, Drone secure communication protocol for future sensitive applications in military zone. Sensors, 21(6), (2021) 2057. https://doi.org/10.3390/s21062057

[6] S. Khriji, Y. Benbelgacem, R. Chéour, D.E. Houssaini, O. Kanoun, Design and implementation of a cloud-based event-driven architecture for real-time data processing in wireless sensor networks. The Journal of Supercomputing, 78(3), (2022) 3374-3401. https://doi.org/10.1007/s11227-021-03955-6

[7] R. Priyadarshi, Efficient node deployment for enhancing coverage and connectivity in wireless sensor networks. Scientific Reports, 15(1), (2025) 29052. https://doi.org/10.1038/s41598-025-14252-0

[8] S. Sheeja, An optimized intrusion detection model for wireless sensor networks based on MLP-CatBoost algorithm. Multimedia Tools and Applications, 83(25), (2024) 66725-66755. https://doi.org/10.1007/s11042-023-18034-6

[9] M. Aminu, A. Akinsanya, D.A. Dako and O. Oyedokun, Enhancing cyber threat detection through real-time threat intelligence and adaptive defense mechanisms. International Journal of Computer Applications Technology and Research, 13(8), (2024) 11-27.

https://doi.org/10.7753/IJCATR1308.1002

[10] A. Kesavmoorthy, M. Ramalingam, Enhanced weight-based clustering algorithm for secure transmission in military vehicle communication in VANET. TPM–Testing, Psychometrics, Methodology in Applied Psychology, 32(S3), (2025) 428-435.

[11] U. Jain, M. Hussain, Security mechanism for maritime territory and frontier surveillance in naval operations using wireless sensor networks. Concurrency and Computation: Practice and Experience, 33(17), (2021) e6300. https://doi.org/10.1002/cpe.6300

[12] S. Rajasoundaran, S.S. Kumar, M. Selvi, S. Ganapathy, R. Rakesh, A. Kannan, Machine learning based volatile blockchain construction for secure routing in decentralized military sensor networks. Wireless Networks, 27(7), (2021) 4513-4534. https://doi.org/10.1007/s11276-021-02748-2

[13] A. Singh, J. Amutha, J. Nagar, S. Sharma, A deep learning approach to predict the number of k-barriers for intrusion detection over a circular region using wireless sensor networks. Expert Systems with Applications, 211, (2023) 118588. https://doi.org/10.1016/j.eswa.2022.118588

[14] S.P. Subotha, L. Femila, VMRF: Revolutionizing military border surveillance with extensive coverage and connectivity. Telecommunication Systems, 86(3), (2024), 481-502. https://doi.org/10.1007/s11235-024-01125-6

[15] G.R. Zibetti, J.A. Wickboldt, E.P. De Freitas, Context-aware environment monitoring to support LPWAN-based battlefield applications. Computer Communications, 189, (2022) 18-27. https://doi.org/10.1016/j.comcom.2022.02.020

[16] A.A. Okine, N. Adam, F. Naeem, G. Kaddoum, Multi-agent deep reinforcement learning for packet routing in tactical mobile sensor networks. IEEE Transactions on Network and Service Management, 21(2), (2024) 2155-2169. https://doi.org/10.1109/TNSM.2024.3352014

[17] M. Shanmathi, A. Sonker, Z. Hussain, M. Ashraf, M. Singh, M. Syamala, Enhancing wireless sensor network security and efficiency with CNN-FL and NGO optimization. Measurement: Sensors, 32, (2024) 101057. https://doi.org/10.1016/j.measen.2024.101057

[18] B. Kaur, D. Prashar, L. Mrsic, A. Almogren, A.U. Rehman, A. Altameem, S. Hussen, Enhancing the reliability and accuracy of wireless sensor networks using a deep learning and blockchain approach with DV-HOP algorithm for DDoS mitigation and node localization. EURASIP Journal on Wireless Communications and Networking, 2025(1), (2025) 46. https://doi.org/10.1186/s13638-025-02465-w

[19] S.D. Raj, H.S. Babu, Identification of intelligence requirements of military surveillance for a WSN framework and design of a situation aware selective resource use algorithm. Revue d'Intelligence Artificielle, 36(2), (2022) 251-261. https://doi.org/10.18280/ria.360209

[20] B. Almaslukh, Deep learning and entity embedding-based intrusion detection model for wireless sensor networks. Computers, Materials & Continua, 69(1), (2021) 1343-1360. https://doi.org/10.32604/cmc.2021.017914

[21] A.N. Pathak, A.R. Yadav, Securing and optimizing wireless sensor military networks: A hybrid KNN-decision tree model for anomaly detection and false alarm reduction. Fusion: Practice & Applications, 20(1), (2025) 114-130.

[22] A. Singh, J. Amutha, J. Nagar, S. Sharma, C.C. Lee, LT-FS-ID: Log-transformed feature learning and feature-scaling-based machine learning algorithms to predict the k-barriers for intrusion detection using wireless sensor network. Sensors, 22(3), (2022) 1070. https://doi.org/10.3390/s22031070

[23] A.N. Pathak, A.R. Yadav, Optimizing security and energy in military sensor networks: A fault-tolerant self-management approach. Engineering Research Express, 7(3), (2025) 035228. https://doi.org/10.1088/2631-8695/adeee6

[24] S. Muruganandam, R. Joshi, P. Suresh, N. Balakrishna, K.H. Kishore, S.V. Manikanthan, A deep learning based feed forward artificial neural network to predict the k-barriers for intrusion detection using a wireless sensor network. Measurement: Sensors, 25, (2023) 100613. https://doi.org/10.1016/j.measen.2022.100613

[25] N. Ghodichor, D. Sahu, G. Borkar, A. Sawarkar (2023). Secure routing protocol to mitigate attacks by using blockchain technology in MANET. arXiv Preprint, arXiv:2304.04254. https://doi.org/10.48550/arXiv.2304.04254

[26] J. Paruvathavardhini, B. Sargunam, Stochastic bat optimization model for secured WSN with energy-aware quantized indexive clustering. Journal of Sensors, 2023(1), (2023) 4237198. https://doi.org/10.1155/2023/4237198

Authors Contribution Statement

D. Rekha: Conceptualization, Methodology, Writing-Original Draft. Baalaji K: Investigation, Formal Analysis, Visualization, Supervision. Both Authors Read and Approved Final version of the manuscript.

Funding

The authors declare that no funds, grants or any other support were received during the preparation of this manuscript.

Competing Interests

The authors declare that there are no conflicts of interest regarding the publication of this manuscript.

Data Availability

The data supporting the findings of this study can be obtained from the corresponding author upon reasonable request.

Has this article screened for similarity?

Yes

About the License