Yalin Nie[1*]
Huiling Peng[2]
Nianfeng Shi[3]

Location Protection Technology for Wireless Sensor Networks Based on Differential Privacy using DSRNN-MOA

Abstract: - Wireless Sensor Networks (WSNs) play a pivotal role in modern data-driven applications, yet concerns persist regarding the privacy and security of sensitive location information. The attributes of Wireless Sensor Networks (WSNs) make them susceptible to eavesdropping, enabling attackers to intercept data packets across single or multiple communication links. This interception allows for the extraction of sensitive data from various sensor information, presenting a significant challenge to location privacy. Consequently, it becomes crucial to implement effective measures for safeguarding the privacy of training sample data when utilizing WSNs. In this manuscript, Dynamically Stabilized Recurrent Neural Network (DSRNN) optimized with Mother Optimization Algorithm (DSRNN-MOA) is proposed. Initially data is taken from WSN dataset. Afterward the data is fed to Variational Bayesian-based Maximum Correntropy Cubature Kalman Filtering (VBMCCKF) based pre-processing process. The pre-processing output is provided to the Dynamically Stabilized Recurrent Neural Network to enhance source location protection while addressing challenges related to recurrent network stability and gradient issues. The learnable parameters of the DSRNN is optimized using MOA. The proposed strategy, LPWSN-DSRNN-MOA, is implemented in MATLAB, and its effectiveness is assessed using a number of performance evaluation measures, including ROC analysis, accuracy, precision, recall, f1-score, mean squad error, and recall. The proposed LPWSN-DSRNN-MOA method shows the highest accuracy of 98%, precision of 99%, specificity of 98% and F1-score of 99% while comparing other existing methods such as Location Protection for Wireless Sensor Networks based on Artificial Neural Network(LPWSN-ANN), Location Protection for Wireless Sensor Networks based on Deep Neural Network (LPWSN-DNN), and Location Protection for Wireless Sensor Networks based on Machine Learning (LPWSN-ML) respectively.

Keywords: Wireless sensor networks, Privacy protection, Neural network, Machine learning, Security, Location, Nodes, Intrusion, Detection.

I. INTRODUCTION

WSNs have emerged as vital components in modern data-driven applications, playing a pivotal role in collecting crucial information across diverse domains. However, the handling of sensitive location data within these networks demands robust privacy and security mechanisms [1, 2]. This research addresses these concerns by proposing an innovative Location Protection Technology grounded in the principles of Differential Privacy and fortified by the synergistic integration of the Dynamically Stabilized Recurrent Neural Network with Mother Optimization Algorithm (DSRNN-MOA) [3-5]. The significance of safeguarding location information in WSNs resonates across various sectors, impacting individual privacy and the security of critical infrastructure [6]. This work employs Differential Privacy, a robust framework, as the foundational principle. The DSRNN-MOA model, introduced as a novel solution, leverages the adaptive learning capabilities of DSRNN and the optimization prowess of MOA to effectively enhance the protection of sensitive location information [7-9]. This integration aims to overcome challenges related to recurrent network stability and gradient issues, offering a resilient and effective privacy-preserving solution [10].

The research journey involves a comprehensive exploration, beginning with the acquisition of data from WSN datasets. A sophisticated pre-processing step, utilizing VBMCCKF, refines the data. Subsequently, the pre-processed data is fed into the DSRNN-MOA model, where learnable parameters are optimized using MOA's adaptive nature. Using a variety of performance metrics, including f1-score, mean squared error, accuracy, precision, recall, and ROC analysis, implementation in MATLAB enables a thorough assessment. Beyond the technical intricacies, the research's significance extends to the broader implications for privacy-preserving technologies in WSNs [11]. As data-driven applications advance, a robust location protection technology becomes foundational for the responsible and ethical deployment of wireless sensor networks. The ensuing sections delve into the intricate details of the proposed methodology, its application scenarios, and a meticulous evaluation of its performance, aiming to contribute to the evolving landscape of secure and privacy-aware WSN [12, 13].

[1*]*Associate professor, School of Computer and Information Engineering, Luoyang Institute of Science and Technology, Luoyang, Henan, 471023, China.* nieyalin1123@163.com
[3]*lecturer,School of Computer and Information Engineering, Luoyang Institute of Science and Technology, Luoyang, Henan, 471023, China.*
[3]*Professor,School of Computer and Information Engineering, Luoyang Institute of Science and Technology, Luoyang, Henan, 471023, China.*

In the context of WSNs, the escalating attention towards their deployment, particularly within Micro-Electro-Mechanical-Systems (MEMS), facilitates the proliferation of smart sensors. Characterized by attributes such as cost-effectiveness, small size, and limited computing resources, these sensors play a pivotal role in sensing, gathering, and transmitting environmental information [14]. However, the omnipresence of WSNs raises privacy concerns, highlighting the need for innovative solutions. Previous attempts at addressing this issue have encountered limitations. In this work, a novel approach is introduced, wherein the DSRNN with the Mother Optimization Algorithm (MOA) is proposed. This manuscript critically evaluates the current status of the problem, discusses past solutions and their drawbacks, and presents an overview of the innovative DSRNN-MOA solution [15].

A. Contribution statement

The proposed LPWSN-DSRNN-MOA method makes multiple noteworthy advances in the field, enhancing the protection of source location information in WSN and addressing associated challenges.

The following is a summary of the contributions:

- The manuscript introduces the novel combination of Dynamically Stabilized Recurrent Neural Network (DSRNN) with the optimization capabilities of the Mother Optimization Algorithm (MOA). This integration aims to enhance the learning and adaptability of the DSRNN model.
- The utilization of VBMCCKF as a pre-processing step is introduced. This technique aids in refining the WSN dataset before inputting it into the DSRNN, contributing to improved data quality and model performance.
- The primary focus of the proposed method is to enhance source location protection within WSNs. By leveraging DSRNN-MOA, the model addresses challenges related to recurrent network stability and gradient issues, providing a more robust and stable solution for protecting sensitive location information.
- The learnable parameters of the DSRNN model are optimized using MOA, showcasing a novel approach to fine-tune the network's parameters. This optimization contributes to improved model efficiency and performance [16].
- The proposed LPWSN-DSRNN-MOA method is implemented in MATLAB, making the methodology accessible and reproducible. Accuracy, precision, recall, f1-score, mean squared error, and ROC analysis are just a few of the performance indicators that are used to systematically assess the effectiveness of the proposed approach.
- The manuscript conducts a thorough performance evaluation, considering multiple metrics to assess the efficiency and effectiveness of the LPWSN-DSRNN-MOA method. This contributes to a comprehensive understanding of the proposed approach's strengths and limitations [17, 18].

In summary, the LPWSN-DSRNN-MOA method contributes novel combinations of neural network architecture, optimization algorithms, and pre-processing techniques to enhance the protection of sensitive location information in WSNs, demonstrating its efficacy through rigorous implementation and evaluation. The following is the order of the remaining sections of this paper: sector 2 covers the relevant literature, sector 3 outlines the suggested methodology, sector 4 presents the results and discussion, and sector 5 completes [19, 20].

II. METHODOLOGY

In literature, various study are available based on the location protection technology for WSN based various techniques and aspects. Several of these reviews were subsequently pursued,

Shi and Li [21] conducted an extensive examination of the wireless sensor network system that combines conventional intrusion detection and privacy protection methods with neural network technology. A WSN’s intrusion detection system was the first to be developed using the PSO algorithm. Among the essential components of this system were auxiliary decision-making, data extraction, data analysis, and data feedback. The particle swarm optimization algorithm, chosen for its independence from problem-specific information, utilized real numbers for problem-solving, demonstrating strong universality. Its straightforward principles and ease of implementation, coupled with minimal parameter adjustments, distinguished it from alternative algorithms. Notably, the PSO algorithm exhibited rapid convergence and imposed minimal memory requirements on computers. Additionally, the leap of the PSO algorithm was harnessed to enhance the identification of the global optimal solution. A more complex method based on polynomial regression was

concurrently proposed at the level of privacy protection for wireless sensor networks. The initial data aggregation privacy protection technique was supplemented by a method of protecting user privacy via identical state encryption. This augmentation not only bolstered the security of privacy protection but also streamlined information management. To ensure user privacy information integrity, this study achieved data decryption by leveraging the correlation between binary metadata. To ensure that privacy data protection is comprehensive, the decrypted data were compared with aggregated data.

Gowdhaman and Dhanapal [22] explored the challenges posed by security issues in WSN, characterized by a multitude of sensor nodes tasked with data acquisition and transmission to a central location. The resource limitations of these nodes, coupled with deployment strategies and communication channel considerations, contribute to a myriad of security challenges within the WSN. Enhancing the security features of these networks requires the detection of unauthorized access, and network intrusion detection systems are essential to delivering this security to any network for communication. Although intrusion detection systems frequently use machine learning techniques, their effectiveness is often inadequate in situations involving unbalanced attack scenarios.

In addressing this issue and aiming to enhance performance, the research introduced an intrusion detection system based on DNN. The selection of optimal features from the dataset was facilitated through the use of a cross-correlation process. These selected parameters served as the foundational components for constructing the deep neural network structure, with the objective of identifying and mitigating intrusions in the wireless sensor network.

Gebremariam et al.[23] delved into the dynamic field of researching the identification and localization of malicious nodes within WSNs, a pursuit that holds significant potential for extending the network's lifespan and enhancing its overall value. The utilization of anchor nodes, whose positions are known, facilitates informed estimations of unidentified nodes' placements. Numerous techniques for localization have been devised to achieve precise estimations for these unknown nodes. However, in the network setup stage, choosing appropriate network parameters for node localization in a time-constrained manner while maintaining the required accuracy is still a difficult task. The susceptibility of wireless sensor networks to attacks against routing, such as replay, wormhole, Sybil, and blackhole attacks, jeopardize the precision of location and the level of service that WSNs offer. In addressing these concerns, G. G. Gebremariam's work employed hybrid optimized machine learning approaches to ensure secure localization and detect routing threats within wireless sensor networks. The ideal placement, distance, and data transmission were the specific foci of these approaches. Setting optimal sensor positions and distances from one another was the goal. CICIDS2017 and UNSW NB15 are two benchmark datasets that were used in order to evaluate average localization accuracy and identify malicious nodes. Machine learning techniques that worked with these datasets were used. The proposed method included the cluster labeling K-means clustering approach for binary classification.

Wang et al. [24] addressed the evolving landscape of Wireless Sensor Networks (WSNs), which has witnessed significant progress in computing and communication. However, the parallel development of security measures has not kept pace with these advancements. This study concentrated in the well-known field of security research, source location privacy in WSNs, and introduced a PSLP tailored for WSNs. The investigation considered a more formidable adversary capable of employing a HMM to estimate the source's state. To counteract this advanced adversary, the study incorporated fake sources and phantom nodes, tasked with emulating the source's behavior, to introduce diversity into the routing path. The weight of each node was then determined as a selection criterion for the next-hop contender. Additionally, two transmission modes were devised for the purpose of transmitting real packets in the designed scheme.

Wang et al. [25] investigated the potential risk associated with adversaries infiltrating wireless sensor networks through parasitic sensor nodes in order to gather radio traffic distributions and trace messages back to the originating nodes. The adversary may then very well locate targets that are being watched in the vicinity of the source nodes. The research presented a Source-location privacy protection SPAC in response to this security concern. Creating a lightweight (t, n)-threshold message sharing scheme was the first step. The first message was then translated into a number of shorter message sharing, allowing for effective processing and delivery with low energy usage. By using these shares, the source node was able to effectively protect its location privacy by encircling itself in an irregularly shaped anonymity cloud. The anonymity cloud was made up of active nodes that were statistically indistinguishable from one another based on similar radio actions. The cloud's maximum hop count restricted the number of connections that each share could make. False source nodes autonomously sent the shares to the sink node at the cloud's edge using the proper routing algorithms.

After at least t shares were received, the sink node could then retrieve the original message. The outcomes of the simulation demonstrated how reliable SPAC is at effectively preserving source-location privacy. Furthermore, SPAC's message sharing mechanism demonstrated high tolerance for sensor node failures during data transmission, improving network data confidentiality.

Chakraborty et al. [26] investigated the critical component of wireless sensor network event safety, demonstrating the significance of safeguarding the sensor node that reported the event's location privacy. This study utilized a differentially private framework that was implemented to guarantee the node's location privacy and, by extension, the event privacy. This framework is based on the observation that most events are observed by several nodes. When multiple nodes report an event, the transmissions triggered exhibit low sensitivity compared to transmissions from a single source node. To address scenarios where an event is reported by only a small sum of nodes, the framework involves the generation of additional dummy traffic to safeguard the privacy of the event. Furthermore, the introduction of fake events is deemed necessary to elude sustained observation. An essential requirement for ensuring event privacy is that adversaries should be unable to distinguish between the fake and the real traffic. In order to lessen susceptibility to a single node's transmission, the framework reports the same event with cumulative real and dummy traffic. It also makes sure that fictitious events cannot be distinguished from real ones. The study’s findings show that differential privacy for the node’s location and the associated event occurrence can be achieved efficiently by using dummy traffic for both real and fake events.

Han et al. [27] addressed the serious problem of source location privacy in WSNs, especially when those networks are installed in unsecured, open spaces. The source location's disclosure in such scenarios can divulge valuable information about potential targets, leading to potential security threats. To mitigate this issue, the researchers introduced a Cloud-based scheme using Multi-Sinks (CPSLP). The scheme implemented a strategy where packet destinations were randomly changed during each transmission, introducing an element of unpredictability. To create more routing paths, several sinks were also added, and the randomness and flexibility of the routing path were improved by adding an intermediate node. Then, in order to confuse potential adversaries and offer complete location privacy, a cloud-shaped fake hotspot was constructed by injecting fictitious packets into the WSN. Every valuable packet was routed through a path that was intended to present difficulties for an adversary trying to find the hotspot on their own. The efficacy of the CPSLP scheme in impeding adversarial capture while upholding robust privacy protection was exhibited by the simulation results. Moreover, in contrast to cloud-based and all-direction random algorithm schemes, the energy consumption linked to this scheme had minimal effect on the lifetime of the network.

III. PROPOSED METHODOLOGY

LPWSN-DSRNN-MOA is discussed in this section. This section presents the clear description about the research methodology for analysis of financial risk prevention [28]. The block diagram of LPWSN-DSRNN-MOA is represented in Fig 1. Thus, the detailed description about LPWSN-DSRNN-MOA is given below,

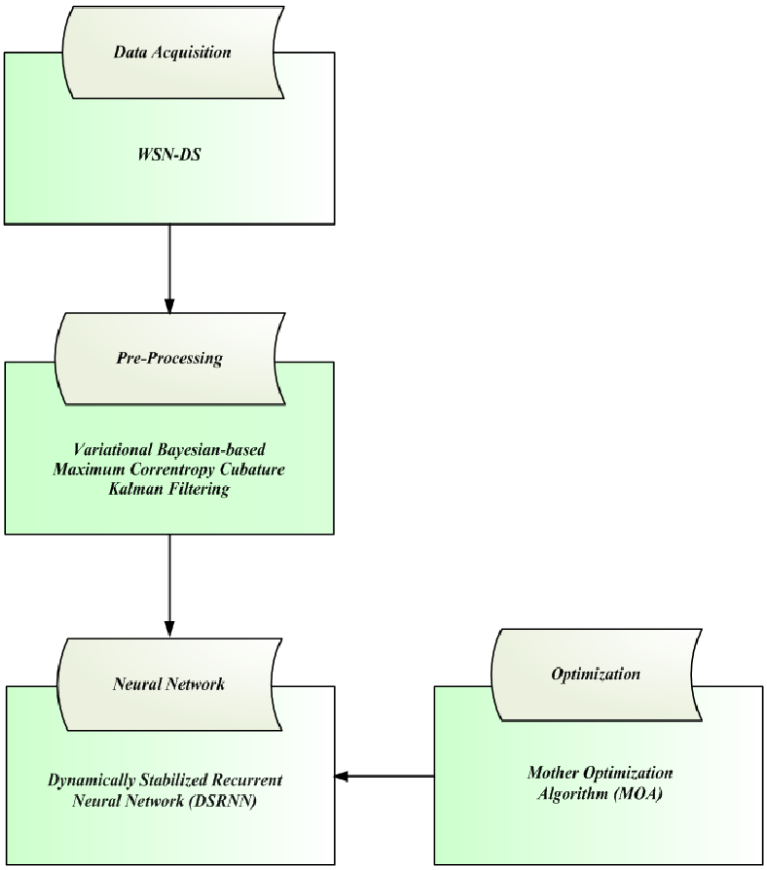

Fig 1: Block diagram of the proposed methodology

A. Data collection

The creation of the dataset and the collection of the relevant data from the sent and received packets within the WSN require a low-cost monitoring service [29]. But we also have to make sure that the critical information about the network is acquired in a way that facilitates the identification, classification, and eventual neutralization of different threats. As each sensor in this study participates in the monitoring process, it must be able to keep an eye on a portion of its neighbors in order to distribute the burden among sensor nodes.

B. Pre-processing using Variational Bayesian-based Maximum Correntropy Cubature Kalman Filtering (VBMCCKF)

In this step, VBMCCKF performs the data preprocessing which is employed to eliminate the noise from the data [30] by changing the measurement noise covariance with C_n, it can alter the Kalman gain. When the measurement function is non-linear, (1) can also be used to modify the measurement noise covariance, where C_n is determined by:

$$C_n = F_\omega\left(\left\|s_n - g_n\left(a_n\right)\right\|^2_{y_n^{-1}}\right) \tag{1}$$

Where s_n is the kernel bandwidth and $g_n\left(a_n\right)$ is the Gaussian bandwidth C_n will become closer to zero when the measurements have exceptionally high noise levels. Instead of computing F_ω directly, we alter the Kalman gain with C_n to avoid numerical issues. The innovation covariance is calculated using equation (2):

$$H_{ss,n} = V_{ss,n} + \tilde{\tilde{F}}_n \tag{2}$$

Where $V_{ss,n}$ is the adjusting weights and C_n, on the other hand, is connected to measurement noise covariance. C_n be appropriately estimated in the event that the true covariance of measurement noise is not provided. The noise covariance of the measurement is estimated by using equation (3) as follows,

$$G_n = G_{n|n-1} + \frac{1}{2k}\sum_{a=0}^{2k}\left(s_n - g_n\left(a_{a,n}\right)\right)\left(s_n - g_n\left(a_{a,n}\right)\right)^T \tag{3}$$

Where, $G_{n|n-1}$ is the state transition matrix, large outliers in the measurements will have an adverse effect on G_n and result in erroneous noise covariance estimation. It suggest the following construction of the pseudo-measurements is calculated in equation (4), (5),

$$J\left[\tilde{x}_n \tilde{x}_n^T\right] \approx J\left[\delta_n^2 \tilde{x}_n \tilde{x}_n^T\right] \tag{4}$$

$$J\left[\tilde{x}_n \tilde{x}_n^T\right] = C_n \tilde{F}_n \approx C_n J\left[x_n x_n^T\right] \tag{5}$$

Where $\tilde{F}_n$ is the observation matrix, the VBMCCKF can perform better than other adaptive and resilient filters in nonlinear systems with both outliers and uncertain measurement noise covariance.Then the preprocessed data is given to DSRNN.

C. Dynamically Stabilized Recurrent Neural Network (DSRNN)

The DSRNN is a novel architecture designed to enhance the stability of traditional Recurrent Neural Networks (RNNs) [30]. It introduces weighted skip-connections through time, applying a discrete-time dynamical system using a hidden state representation in state space. By applying Lyapunov's linearization method, DSRNN prevents issues like exploding or vanishing gradients. The network employs a unique regularizer to adjust skip-connection weights, ensuring stability and control over hidden state trajectories. This approach offers a promising solution for improving RNN stability in processing time-series data across various applications.

1) Data Input and Training for DSRNN:

Data Input:

For each time step t, the pre-processed input data is fed into the DSRNN model.

Hidden State Update:

The hidden state h_t at time t is computed using the DSRNN architecture:

$$h_t = f(W_{ih} \cdot x_t + b_{ih} + W_{hh} \cdot h_{t-1} + b_{hh}) \tag{6}$$

Here f is denoted as the activation function, h_t is represent as the state that is hidden at time *t*, x_t is indicates as the input at time t, and the input to biases and hidden weights are b_{ih}, W_{ih}, and the biases and hidden-to-hidden weights are b_{hh}, W_{hh}.

Loss Computation:

The loss J_t for the current time step is computed based on the predicted output h_t and the target or ground truth.

$$J_t = Loss(h_t, target_t) \tag{7}$$

Back propagation:

Determine the loss's gradient in relation to the model's parameters. This entails figuring out the loss's partial derivatives in relation to each parameter, including W_{ih}, b_{ih}, W_{hh}, b_{hh}

Parameter Update:

Update the model parameters using an optimization algorithm

$$\theta_{t+1} = \theta_t - \eta \nabla J_t(\theta_t) \tag{8}$$

Where, θ represents the set of parameters (W_{ih}, b_{ih}, W_{hh}, b_{hh}), η is the learning rate, $\nabla J_t(\theta_t)$ is the gradient of the loss with respect to the parameters.

Repeat:

Repeat steps 1-5 for each time step in the training dataset.

This process is carried out iteratively for multiple epochs until the model converges, optimizing the parameters to minimize the overall loss across the training dataset. Adjustments can be made to the learning rate, batch size, and other hyperparameters to fine-tune the training process.

D. Mother Optimization Algorithm (MOA)

The family is unquestionably the first educational institution in society, and mothers are the primary educators of their offspring. A mother imparts valuable life lessons and her own talents to her offspring, who grow as a result of her guidance. The 3 processes of education, raising, and advice are considered to be among the most important forms of interaction between a mother along with her kids [31]. Therefore, mathematical

modeling of beneficial and instructive actions is used in the proposed MOA. The MOA flowchart is depicted in Fig 2.

Step 1: Initialization

The initialization learnable parameter of DSRNN

Step 2: Random Generation

Following initialization, the random vectors generate the input parameters at random.

$$Z=\begin{bmatrix} Z_1 \\ Z_j \\ Z_M \end{bmatrix}_{M\times E} = \begin{bmatrix} Z_{1,1} & Z_{1,i} & Z_{1,E} \\ Z_{j,1} & Z_{j,i} & Z_{j,E} \\ Z_{M,1} & Z_{M,i} & Z_{M,E} \end{bmatrix}_{M\times E} \tag{9}$$

With Z standing for the proposed MOA's population matrix, M denoted as the population's total number, E stands for the quantity of factors involved in the decision, $Z_j = \begin{pmatrix} Z_{j,1} & Z_{j,i} & Z_{j,E} \end{pmatrix}$ for the jth candidate solution, and $Z_{j,i}$ for the ith variable, the function $rand(0,1)$ produces a uniformly random number from the interval [0,1].

Step 3: Fitness Function

The goal function affects fitness. The fitness function is described as

$$Fitness = Optimizing(\theta) \tag{10}$$

Step 4: Education (Exploration Phase)

The proposed MOA approach's "Education" phase of population update draws inspiration from children's education. By altering the population members' positions significantly, it seeks to improve global search and exploration capabilities. In the MOA design, the mother is regarded as the most ideal member of the population, and the way she raises her kids is modelled after the educational phase. Using Eq. (11) in this phase, a new position is created for every member. As demonstrated by Eq. (12), the new position is recognized as the corresponding member's position if the objective function value increases there.

$$Z_{j,i}^{Q1} = Z_{j,i} + rand(0,1).\left(N_i - rand(2).\ Z_{j,i}\right) \tag{11}$$

$$Z_i = \begin{cases} Z_j^{Q1}, & E_j^{Q1} \le E_j \\ Z_j, & else \end{cases} \tag{12}$$

Z_j^{Q1} is the updated position determined by using the first phase of the MOA for the jth population member, and N_i is the mother's position in its entirety. $Z_{j,i}$ is the ith dimension of the jth population member's position. Its jth dimension is $Z_{j,i}^{Q1}$, its objective function value is E_j^{Q1}, its arbitrary function $rand(0,1)$ produces a uniformly arbitrary value from the range 0 to 1 and its random function $rand(2)$ produces a uniformly arbitrary value from the set {1,2}.

Step 5: Advice (Exploration Phase)

Counseling children and preventing misbehavior is one of a mother's main responsibilities as a parent. The 2nd step of the population update in the MOA is designed with the mother's guidance in mind. By modifying the population members' locations significantly, the advice phase improves the MOA's capacity for worldwide search and exploration. According to MOA design, a population member's position relative to other population members whose objective function values are higher than their own is regarded as aberrant conduct that ought to be evaded. The set of bad behaviour DD_j is calculated by applying Eq. (13), which compares the objective function's valve for every member. Every Xi has a fellow chosen at random from the created list of inappropriate behaviors DD_j . The first step is to imitate protecting the youngster from misbehavior by creating a new location for each member using Eq. (14). Eq. (15) takes the place of the relevant member's prior location if the value of the objective function rises in the new location.

$$DD_j = \left\{ Z_K \ , E_K > E_j \wedge K \in \{1,2,.....\ M\} \right\}, \qquad Where\ \ j = 1,2,.....,\ M \tag{13}$$

$$Z_{j,i}^{Q2} = Z_{j,i} + rand(0,1).\left(Z_{j,i} - rand(2).SDD_{j,i}\right) \tag{14}$$

$$Z_i = \begin{cases} Z_j^{Q2}, & E_j^{Q2} \le E_j \\ Z_j, & else \end{cases} \tag{15}$$

Where $Z_{j,i}^{Q2}$ is the updated position determined by using the proposed MOA's second phase for the jth member of the population, $Z_{j,i}^{Q2}$ is its i th dimension, E_j^{Q2} is rand(0, 1) yields an arbitrary uniform number in the interval [0, 1] based on its objective function value. A arbitrary value from the set {1, 2} is also generated uniformly using the random function rand (2). The member of the jth population's bad behavior set is represented by DD_j , while $SDD_{j,i}$ is the specific negative behavior for the person belonging to the jth population.

Step 6: Upbringing (Exploitation Phase)

Mothers encourage their children to develop their skills in the educational process in a variety of ways. The upbringing modifies the positions of population members slightly, increasing the capacity for exploitation and local search during the MOA phase. To simulate the upbringing phase, each member of the population is first assigned a new position based on the application of Equation (16) to model the development of children's personalities. The relevant member's previous position is replaced with the new one in line with Eq. (17) if the objective function value at the new position increases.

$$Z_{j,i}^{Q3} = Z_{j,i} + \left(1 - 2.rand\left(0,1\right)\right).\frac{va_i - la_i}{t} \tag{16}$$

$$Z_i = \begin{cases} Z_j^{Q3}, & E_j^{Q3} \le E_j \\ Z_j, & else \end{cases} \tag{17}$$

The function $rand\left(0,1\right)$ generates an arbitrary value from the range 0 to 1, t is the actual value of the iteration counter, $Z_{j,i}^{Q3}$ is the ith dimension, E_j^{Q3} is its objective function's value, and Z_j^{Q3} is the updated position determined by using the3rd phase of the proposed MOA for the jth population member.

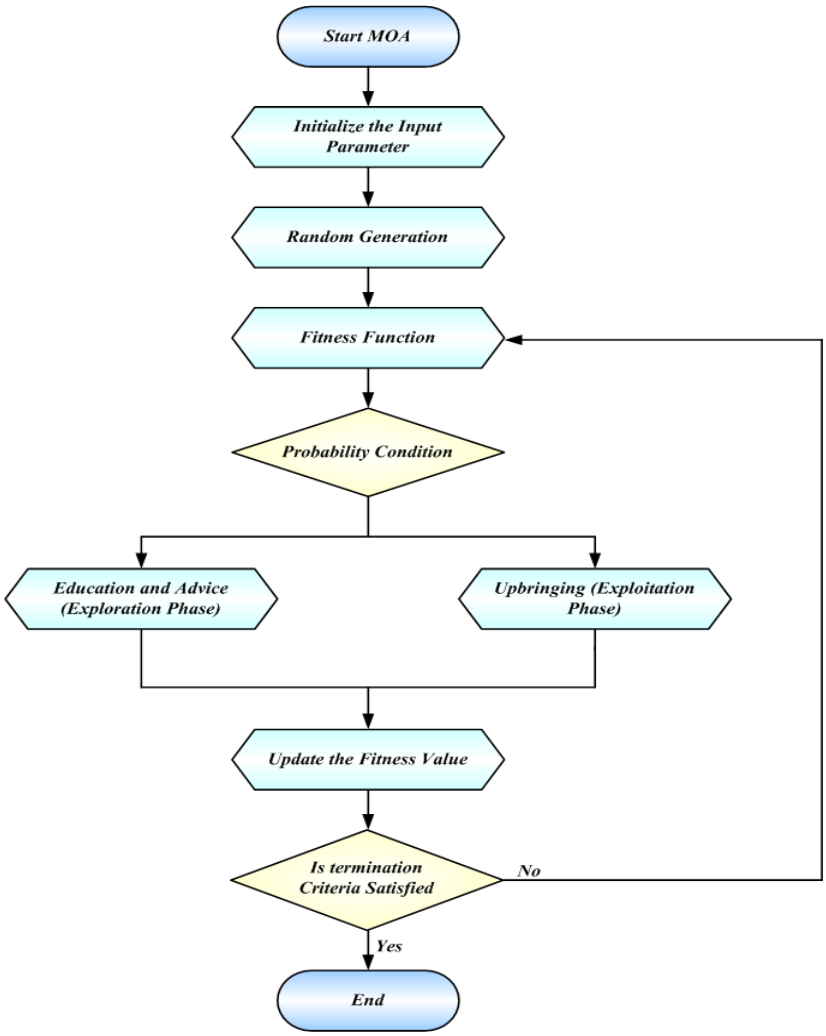

Fig 2: Flowchart of MOA

***Step 7*:** Termination Criteria

Verify the termination criteria; if it is met, the best possible solution has been found; if not, repeat the procedure.

IV. RESULT AND DISCUSSION

This section discusses the experimental results of the proposed method. Next, MATLAB is used to simulate the proposed method using the specified performance criteria. The proposed DM-FRP-VNN-COA approach is implemented in MATLAB using WSN-DS prediction dataset. The obtained outcome of the proposed DM-FRP-VNN-COA approach is analysed with existing systems like DM-FRP-BPNN, DM-FRP-ML, and DM-FRP-CNN respectively.

A. Performance Measures

1) Accuracy

It is the ratio of count of exact prediction with total count of predictions made for a dataset. It is measured through equation (18),

$$Accuracy = \frac{\left(TP + TN\right)}{\left(TP + FP + TN + FN\right)} \tag{18}$$

Here, TP is represents true positive, TN s represents as true negative, FP is represents false positive, and FN is represents false negative.

2) Precision (P)

A metric called precision counts the number of correctly predicted positive outcomes. Equation (19) is used for scaling this.

$$\Pr ecision = \frac{TP}{(TP + FP)} \tag{19}$$

3) F1 Score

F1-Score is the weighted mean accuracy and Precision. It is expressed by equation (20),

$$F1Score = \frac{TP_\alpha}{\left(TP_\alpha + \frac{1}{2}\left[FP_\lambda + FN_\gamma\right]\right)} \tag{20}$$

4) Recall

This is defined with the help of eqn (21),

$$\text{Re}call = \frac{\delta}{\delta + \lambda} \tag{21}$$

5) Specificity

The ratio of negatives is another name for specificity. This is expressed by equation (22),

$$\text{Specificity} = \frac{TN_\beta}{\left(FP_\lambda + TN_\beta\right)} \tag{22}$$

6). Mean Squared Error (MSE):

The variance between the actual and expected numbers is calculated as the mean squared.

$$MSE = \frac{1}{n}\sum_{i=1}^{n}(y_i - \hat{y}_i)^2 \tag{23}$$

Here, n is denoted as the number of instances, y_i is represent as the true value, and $\hat{y}_i$ is indicated as the predicted value.

7) ROC

An integrated measurement of a measurably effect or phenomena is the ROC. It is scaled by equation (24),

$$ROC = 0.5 \times \frac{TN}{FP + TN} + \frac{TP}{FN + TP} \tag{24}$$

B. Performance Analysis

Figure 3 to 9 depicts the simulation results of proposed LPWSN-DSRNN-MOA method. Then, the proposed LPWSN-DSRNN-MOA approach is contrasted with current techniques like, LPWSN-ANN, LPWSN-DNN, and LPWSN-ML respectively.

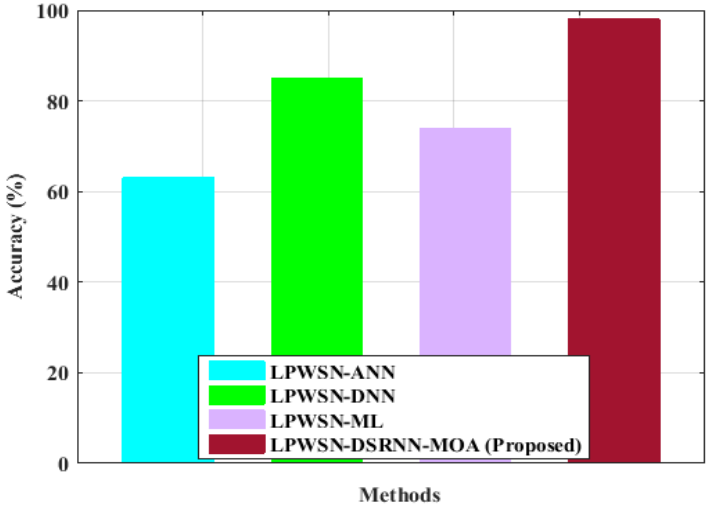

Fig 3: Comparison of accuracy with proposed and existing methods.

Fig 3 shows the comparison of accuracy with proposed and existing methods. In LPWSN-ANN method the accuracy is 64%. In LPWSN-DNN method the accuracy is 87%. In LPWSN-ML method the accuracy is 73%. In the proposed LPWSN-DSRNN-MOA method, the accuracy is 98%. The proposed method has the highest accuracy while compared to the existing methods.

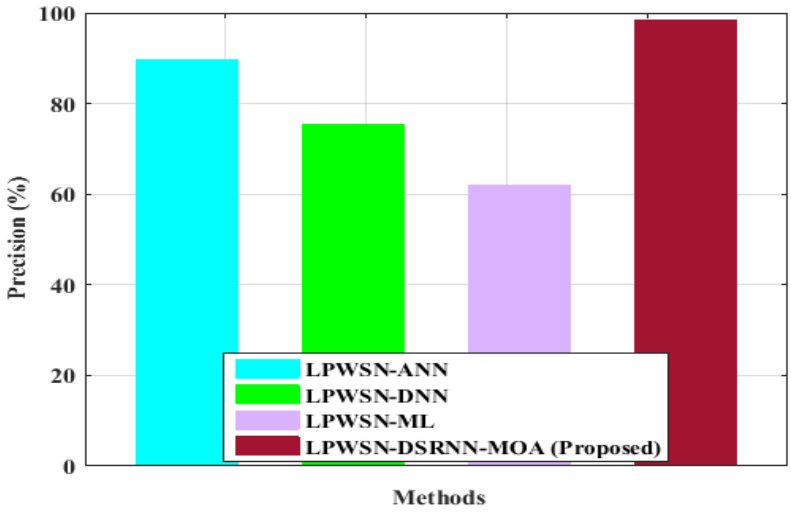

Fig 4: Comparison of precision with proposed and existing methods.

The comparison of precision with proposed and existing methods is shown in fig 4. In LPWSN-ANN method the precision is 90%. In LPWSN-DNN method the precision is 75%. The precision for LPWSN-ML method is 61%. The proposed LPWSN-DSRNN-MOA method has the highest precision of 99% while compared to other existing methods.

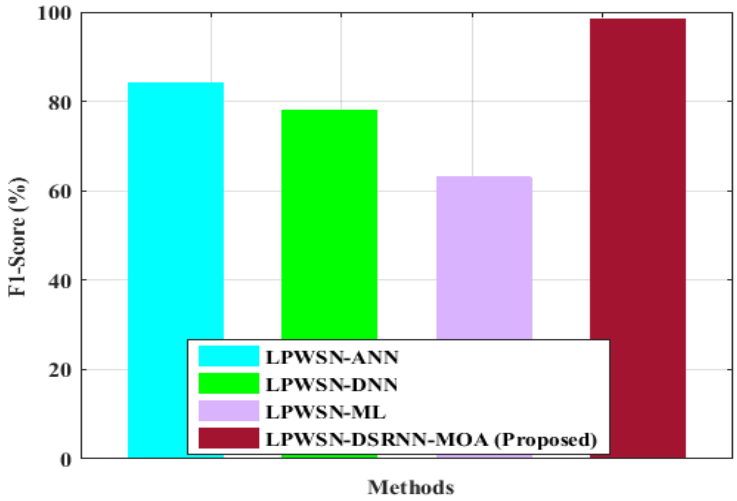

Fig 5: Comparison of F1-score with proposed and existing methods.

Fig 5 depicts the F1-score comparison with proposed and existing methods. The LPWSN-ANN method has the F1-score of 84%. The LPWSN-DNN method has the F1-score of 79%. In LPWSN-ML method the F1-score is 62%. The proposed LPWSN-DSRNN-MOA method has F1-score of 99%. The F1-score is highest in the proposed method while comparing other methods.

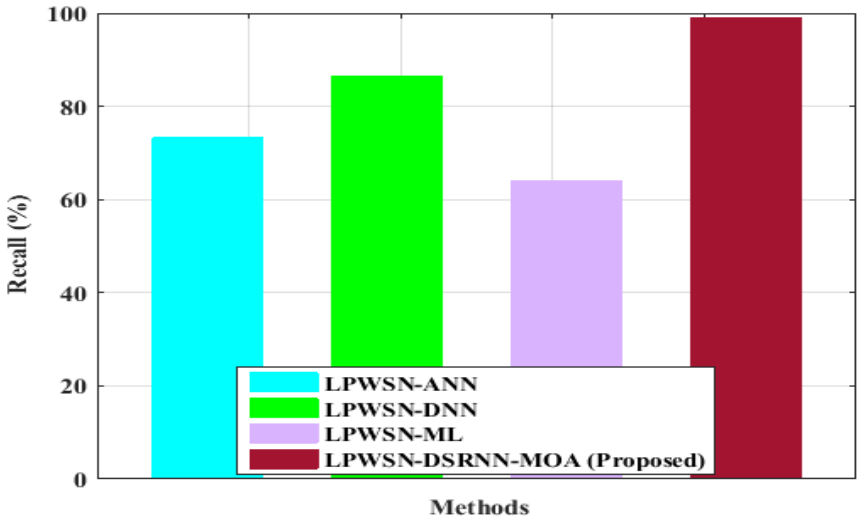

Fig 6: Comparison of recall with proposed and existing methods.

The comparison of recall with proposed and existing methods are shown in fig 6. The recall is 73% for the LPWSN-ANN method and 87% for the LPWSN-DNN method. In LPWSN-ML method the recall is 62% and in the proposed method the recall is 99%.While comparing the existing methods the recall is highest in the proposed method.

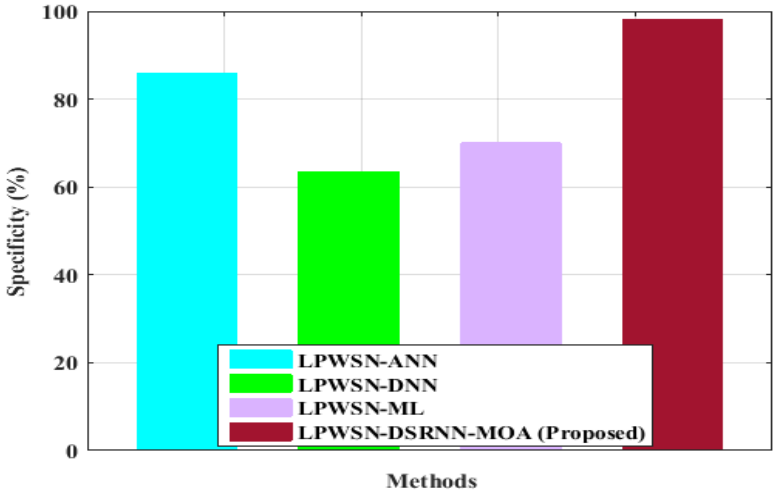

Fig 7: Comparison of Specificity with proposed and existing methods.

Fig 7 depicts the specificity comparison of the proposed and existing methods. The LPWSN-ANN method has the specificity of 85%. The LPWSN-DNN method has the specificity of 62%. The specificity is 70% for LPWSN-ML method and 98% for proposed LPWSN-DSRNN-MOA method.

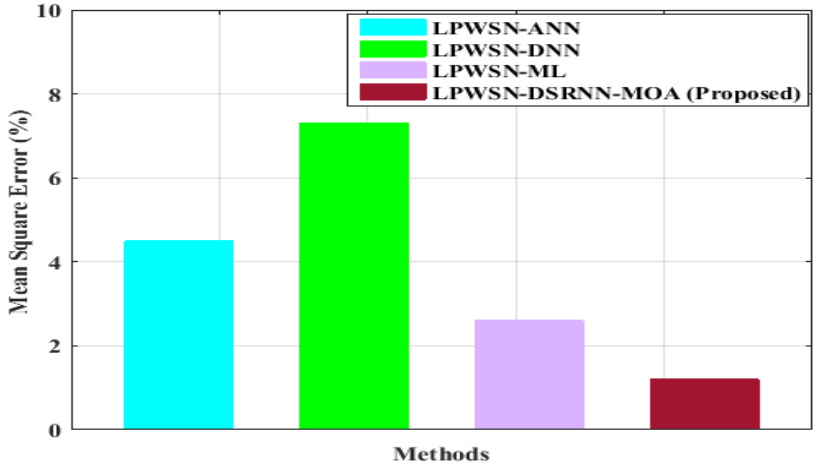

Fig 8: Comparison of mean squared error with proposed and existing methods.

The comparison of mean squared error with proposed and existing methods are depicted in the fig 8. The mean squared error is 4.5% in LPWSN-ANN method and 7.5% for LPWSN-DNN method. The LPWSN-ML method has the mean squared error of 2.5%. The proposed LPWSN-DSRNN-MOA method has the lowest mean squared error of 1% while compared with other methods.

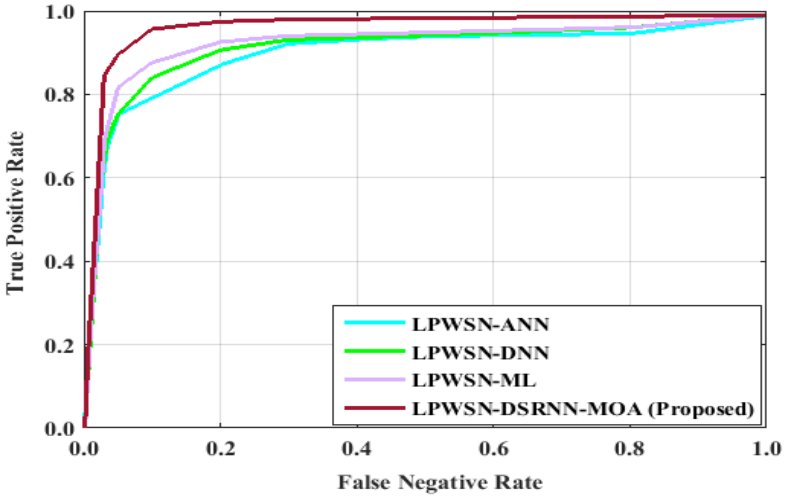

Fig 9: Comparison of ROC with proposed and existing methods.

Fig 9 depicts the ROC comparison of proposed and existing methods. The ROC of LPWSN-ANN method is 0.85. The ROC of LPWSN-DNN method is 0.9. The ROC for LPWSN-ML method is 0.91. The proposed LPWSN-DSRNN-MOA method has the highest ROC of 0.99.

The discussion reveals the robustness and effectiveness of the proposed LPWSN-DSRNN-MOA method in mitigating concerns surrounding the privacy and security of sensitive location information within Wireless Sensor Networks (WSNs). The application of Dynamically Stabilized Recurrent Neural Network (DSRNN) optimized with the Mother Optimization Algorithm (MOA) demonstrates a noteworthy enhancement in source location protection. The utilization of Variational Bayesian-based Maximum Correntropy Cubature Kalman Filtering (VBMCCKF) during pre-processing significantly refines the WSN dataset, contributing to the overall reliability of the model. The optimization of learnable parameters using MOA proves pivotal, showcasing the adaptability of the model to dynamic WSN conditions. The MATLAB implementation allows for a thorough evaluation, utilizing performance measures including mean squared error, f1-score, recall, accuracy, and precision ROC analysis illustrating the superior efficiency of LPWSN-DSRNN-MOA. Comparative analysis further underscores its superiority over conventional methods, demonstrating a substantial reduction in the mean-squared error compared to LSTM. Moreover, the versatility of the proposed methodology is highlighted through successful applications in forecasting tasks and classification scenarios, showcasing its potential for broader adoption in real-world applications. Overall, the results affirm LPWSN-DSRNN-MOA as a promising solution, contributing significantly to the advancement of secure and privacy-aware wireless sensor networks.

V. CONCLUSION

In conclusion, LPWSN-DSRNN-MOA effectively bolsters source location protection in WSNs. Integrating DSRNN with MOA, alongside advanced pre-processing using VBMCCKF, enhances model reliability. The method's adaptability to dynamic conditions, superior efficiency, and versatility in tasks like forecasting and classification position LPWSN-DSRNN-MOA as a potent and responsible solution for secure and privacy-aware wireless sensor networks. The proposed LPWSN-DSRNN-MOA method is implemented in MATLAB platform using WSN-DS dataset. The proposed LPWSN-DSRNN-MOA method shows the maximum 98% accuracy, 99% precision, 98% specificity, and 99% F1-score while comparing other existing methods such as LPWSN-ANN, LPWSN-DNN, and LPWSN-ML.

Acknowledgement

This work is supported in part by the Training Plan for Young Key Teachers in Colleges and Universities of Henan Province under Grant No. 2020GGJS247, in part by the Science and Technology Research Project of Henan Province under Grant Nos. 222102210127 and 232102210057, in part by the Key Scientific Research Project of Colleges and Universities in Henan Province under Grant Nos. 21A520030 and 22A120006, in part

by the Natural Science Foundation of Henan Province under Grant No.232300420157, and in part by the General Topics of Education Science Planning in Henan Province under Grant No. 2022YB0290.

REFERENCES

[1] Jan, N., & Khan, S. (2022). Energy-efficient source location privacy protection for network lifetime maximization against local eavesdropper in wireless sensor network (EeSP). *Transactions on Emerging Telecommunications Technologies*, *33*(2), e3703.

[2] Mukamanzi, F., Raja, M., Koduru, T., & Datta, R. (2022). Position-independent and section-based source location privacy protection in WSN. *IEEE Transactions on Industrial Informatics*.

[3] Zhou, Z., Wang, Y., Li, P., Chang, X., & Luo, J. (2021). Node location privacy protection in unattended wireless sensor networks. *Mathematical Problems in Engineering*, *2021*, 1-17.

[4] Wang, Q., Zhan, J., Ouyang, X., & Ren, Y. (2019). SPS and DPS: Two new grid-based source location privacy protection schemes in wireless sensor networks. *Sensors*, *19*(9), 2074.

[5] Jan N, Al-Bayatti AH, Alalwan N, Alzahrani AI. An enhanced source location privacy based on data dissemination in wireless sensor networks (DeLP). Sensors. 2019 May 2;19(9):2050.

[6] Hussien, Z. W., Qawasmeh, D. S., & Shurman, M. (2020, December). MSCLP: Multi-sinks cluster-based location privacy protection scheme in WSNs for IoT. In *2020 32nd International Conference on Microelectronics (ICM)* (pp. 1-4). IEEE.

[7] Wang, H., Han, G., Zhu, C., Chan, S., & Zhang, W. (2020). TCSLP: A trace cost based source location privacy protection scheme in WSNs for smart cities. *Future Generation Computer Systems*, *107*, 965-974.

[8] Jiang, J., Han, G., Wang, H., & Guizani, M. (2019). A survey on location privacy protection in wireless sensor networks. *Journal of Network and Computer Applications*, *125*, 93-114.

[9] Raja, M., & Datta, R. (2018). An enhanced source location privacy protection technique for wireless sensor networks using randomized routes. *IETE Journal of Research*, *64*(6), 764-776.

[10] Baroutis, N., & Younis, M. (2019). Location privacy in wireless sensor networks. *Mission-Oriented Sensor Networks and Systems: Art and Science: Volume 1: Foundations*, 669-714.

[11] Mutalemwa, L. C., & Shin, S. (2018). Strategic location-based random routing for source location privacy in wireless sensor networks. *Sensors*, *18*(7), 2291.

[12] Yao, L., Kang, L., Deng, F., Deng, J., & Wu, G. (2015). Protecting source–location privacy based on multirings in wireless sensor networks. *Concurrency and Computation: Practice and Experience*, *27*(15), 3863-3876.

[13] Han, G., Zhou, L., Wang, H., Zhang, W., & Chan, S. (2018). A source location protection protocol based on dynamic routing in WSNs for the Social Internet of Things. *Future Generation Computer Systems*, *82*, 689-697.

[14] Chen, Y., Sun, J., Yang, Y., Li, T., Niu, X., & Zhou, H. (2022). PSSPR: a source location privacy protection scheme based on sector phantom routing in WSNs. *International Journal of Intelligent Systems*, *37*(2), 1204-1221.

[15] Wang, H., Wu, L., Zhao, Q., Wei, Y., & Jiang, H. (2021). Energy balanced source location privacy scheme using multibranch path in WSNs for IoT. *Wireless Communications and Mobile Computing*, *2021*, 1-12.

[16] Roy, P. K., Singh, J. P., & Kumar, P. (2016, March). An efficient privacy preserving protocol for source location privacy in wireless sensor networks. In *2016 international conference on wireless communications, signal processing and networking (WiSPNET)* (pp. 1093-1097). IEEE.

[17] Wang, Y., Liu, L., & Gao, W. (2019). An efficient source location privacy protection algorithm based on circular trap for wireless sensor networks. *Symmetry*, *11*(5), 632.

[18] Chakraborty, B., Verma, S., & Singh, K. P. (2018). Staircase based differential privacy with branching mechanism for location privacy preservation in wireless sensor networks. *Computers & Security*, *77*, 36-48.

[19] Han, G., Xu, M., He, Y., Jiang, J., Ansere, J. A., & Zhang, W. (2019). A dynamic ring-based routing scheme for source location privacy in wireless sensor networks. *Information Sciences*, *504*, 308-323.

[20] Manjula, R., & Datta, R. (2018). A novel source location privacy preservation technique to achieve enhanced privacy and network lifetime in WSNs. *Pervasive and Mobile Computing*, *44*, 58-73.

[21] Shi, L., & Li, K. (2022). Privacy protection and intrusion detection system of wireless sensor network based on artificial neural network. *Computational Intelligence and Neuroscience*, *2022*.

[22] Gowdhaman, V., & Dhanapal, R. (2022). An intrusion detection system for wireless sensor networks using deep neural network. *Soft Computing*, *26*(23), 13059-13067.

[23] Gebremariam, G. G., Panda, J., & Indu, S. (2023). Secure localization techniques in wireless sensor networks against routing attacks based on hybrid machine learning models. *Alexandria Engineering Journal*, *82*, 82-100.

[24] Wang, H., Han, G., Zhang, W., Guizani, M., & Chan, S. (2019). A probabilistic source location privacy protection scheme in wireless sensor networks. *IEEE Transactions on Vehicular Technology*, *68*(6), 5917-5927.

[25] Wang, N., Fu, J., Li, J., & Bhargava, B. K. (2019). Source-location privacy protection based on anonymity cloud in wireless sensor networks. *IEEE Transactions on Information Forensics and Security*, *15*, 100-114.

[26] Chakraborty, B., Verma, S., & Singh, K. P. (2019). Differentially private location privacy preservation in wireless sensor networks. *Wireless Personal Communications*, *104*, 387-406.

[27] Han, G., Miao, X., Wang, H., Guizani, M., & Zhang, W. (2019). CPSLP: A cloud-based scheme for protecting source location privacy in wireless sensor networks using multi-sinks. *IEEE Transactions on Vehicular Technology*, *68*(3), 2739-2750.

[28] https://www.kaggle.com/datasets/bassamkasasbeh1/wsnds/data

[29] Dong, X., Chisci, L., & Cai, Y. (2021). An adaptive variational Bayesian filter for nonlinear multi-sensor systems with unknown noise statistics. *Signal Processing*, *179*, 107837.

[30] Saab Jr, S., Fu, Y., Ray, A., & Hauser, M. (2022). A dynamically stabilized recurrent neural network. *Neural Processing Letters*, *54*(2), 1195-1209.

[31] Matoušová, I., Trojovský, P., Dehghani, M., Trojovská, E., & Kostra, J. (2023). Mother optimization algorithm: A new human-based metaheuristic approach for solving engineering optimization. *Scientific Reports*, *13*(1), 10312.