Knowledge-Based Systems

Optimized Physics-Informed Neural Networks for Advanced Attack Detection and Security Enhancement in Wireless Sensor Networks

--Manuscript Draft--

Manuscript Number:	KNOSYS-D-25-10996
Article Type:	Full Length Article
Keywords:	Gazelle Optimization Algorithm, Physics-Informed Neural Networks, Trust-based Distributed Set Membership Fusion Filtering, Triangulation Topology Aggregation Optimizer Algorithm
Abstract:	Humans are being driven to expand their borders and seize the natural resources of others due to their insatiable desire for political and military dominance. They may employ a variety of strategies to accomplish this goal including learning about military installations the quantity of military personnel stationed there, areas with abundant natural resources, weaknesses of authorities that they can take advantage of. Other pressing issues that need to be addressed right away include illegal immigration drug smuggling, and the cross-border smuggling of other prohibited goods. This manuscript presents an Enhanced Security and Attack Detection Framework leveraging Optimized Physics-Informed Neural Networks (PINN-FFEM-IDS) respectively. Initially, input data is collected from KDD Cup 1999 dataset After preprocessing, the pre-processed data is given to Gazelle Optimization Algorithm (GOA) for selecting optimized features. These features are classified by Physics-Informed Neural Networks (PINNs) for precise detection of attack types including normal, probe, denial of service, remote to local, user to root intrusions. To enhance detection reliability Triangulation Topology Aggregation Optimizer (TTAO) fine-tunes the PINN's parameters ensuring superior performance under constrained WSN conditions. The proposed method demonstrates substantial improvements in accuracy, precision, network lifetime and reduced false positive rate when compared to existing systems such as artificial neural network basis deep learning method to forecast Intrusion Detection in WSN (ANN-ID-WSN), deep neural network base intrusion identification for WSN (DNN-FID-WSN) and feature fusion ensemble meta-classifier method depending on recurrent neural network for intelligent network IDS in WSN (INS-WSN-DNN) respectively.

Author Agreement

Corresponding Author

Dr B Meenakshi

Professor,

Department of Electrical and Electronics Engineering,

Sri Sairam Engineering College , Chennai, Tamil Nadu, India.

Email: profmeenakshib@gmail.com

Co Author

Dr D Karunkuzhali

Professor,

Department of Information Technology,

Panimalar Engineering College, Chennai, India.

19-July-2025

Dear Editors in chief,

We declare that this manuscript is original, has not been published before and is not currently being considered for publication elsewhere.

We confirm that the manuscript has been read and approved by all named authors and that there are no other persons who satisfied the criteria for authorship but are not listed. We further confirm that the order of authors listed in the manuscript has been approved by all of us.

We understand that the Corresponding Author is the sole contact for the Editorial process.

He is responsible for communicating with the other authors about progress, submissions of revisions and final approval of proofs.

Thank you for your consideration.

Sincerely,
Dr B Meenakshi

Optimized Physics-Informed Neural Networks for Advanced Attack Detection and Security Enhancement in Wireless Sensor Networks

Dr.B.Meenakshi [1*],Dr.D. Karunkuzhali [2]

[1]Professor, Department of Electrical and Electronics Engineering, Sri Sairam Engineering College, Chennai, Tamil Nadu, India.*

[1]Email: profmeenakshib@gmail.com*

[2]Professor, Department of Information Technology, Panimalar Engineering College, Chennai, Tamil Nadu, India.

Abstract

Humans are being driven to expand their borders and seize the natural resources of others due to their insatiable desire for political and military dominance. They may employ a variety of strategies to accomplish this goal including learning about military installations the quantity of military personnel stationed there, areas with abundant natural resources, weaknesses of authorities that they can take advantage of. Other pressing issues that need to be addressed right away include illegal immigration drug smuggling, and the cross-border smuggling of other prohibited goods. This manuscript presents an Enhanced Security and Attack Detection Framework leveraging Optimized Physics-Informed Neural Networks (PINN-FFEM-IDS) respectively. Initially, input data is collected from KDD Cup 1999 dataset After preprocessing, the pre-processed data is given to Gazelle Optimization Algorithm (GOA) for selecting optimized features. These features are classified by Physics-Informed Neural Networks (PINNs) for precise detection of attack types including normal, probe, denial of service, remote to local, user to root intrusions. To enhance detection reliability Triangulation Topology Aggregation Optimizer (TTAO) fine-tunes the PINN's parameters ensuring

superior performance under constrained WSN conditions. The proposed method demonstrates substantial improvements in accuracy, precision, network lifetime and reduced false positive rate when compared to existing systems such as artificial neural network basis deep learning method to forecast Intrusion Detection in WSN (ANN-ID-WSN), deep neural network base intrusion identification for WSN (DNN-FID-WSN) and feature fusion ensemble meta-classifier method depending on recurrent neural network for intelligent network IDS in WSN (INS-WSN-DNN) respectively.

Keywords: *Gazelle Optimization Algorithm, Physics-Informed Neural Networks, Trust-based Distributed Set Membership Fusion Filtering, Triangulation Topology Aggregation Optimizer Algorithm.*

1. Introduction

WSNs are composed of hierarchically dispersed micro sensor nodes in the field connected by multihop wireless communication technologies. The sensor nodes are equipped by processing, storage, wireless communication components [1]. Among the things that WSNs monitor and collect data about are network condition and data flow [2]. The most dangerous routeing assault is called the Sybil attack, which lowers service quality by creating and destroying several false identities to launch a malicious attack against the genuine node [3, 4]. It is the primary investigates challenge in WSNs, similar to other applications such as synchronisation, architecture, quality of service deployment, healthcare, disaster management, and calibration [5-7]. Wireless sensor nodes monitor and collect environmental data, transmitting it to cluster head for processing through aggregation[8-10].The localisation of sensor nodes is necessary for two emerging uses of WSNs: item tracking and traffic management [11]. Sensor node location estimate is important for effective routeing, location-aware services [12]. The location of the sensor determines the usefulness of the data that WSN collects. Localisation strategies broadly classified into two groups depend on the

information needed [13-15]. Range-free strategies, which base location estimates on the proximity of several reference nodes, and range-depend methods that depend on known angles or distances among nodes to determine their locations [16]. Owing tocheaper hardware and computational requirements, range-free algorithms are gradually replacing range-depend techniques in WSN localisation. Since the clustering and localisation process estimates node's own location by utilising positions of nearby reference nodes, it is well known illustration of range-free method [17-19]. Reference nodes' initial coordinates are either computed or hard coded during the setup phase [20].

Despite the growing use of Wireless Sensor Networks (WSNs) in mission-critical domains like military, healthcare, and environmental monitoring, ensuring their security remains important challenge. These networks are highly susceptible to different sophisticated attacks, particularly Sybil and denial-of-service attacks due to their open architecture, constrained computational resources, and lack of centralized oversight. Conventional Intrusion Detection Systems struggle to maintain high detection accuracy under these dynamic and resource-limited conditions, often suffering from high false positive rates, poor attack localization and inadequate adaptability to evolving threats. Furthermore many existing approaches depend on static feature selection and lack integration with the physical principles governing WSN behavior, limiting their generalizability and effectiveness. Manual or heuristic-based detection methods are often inefficient and computationally intensive, leading to delayed threat responses and compromised data integrity. Therefore there is an urgent need for a robust, intelligent and adaptive IDS that exactly detect, categorize multiple kinds of attacks in real time, even under noisy and sparse data conditions.

The novelty of the lies in innovative integration of Physics-Informed Neural Networks with a robust multi stage optimization pipe line for intelligent intrusion detection in WSN. The synergy continues with the Triangulation Topology Aggregation Optimizer which fine

tunes the PINN parameters to adaptively detect diverse cyberattacks including Sybil DoS and probe attacks with higher accuracy and reduced false positives. This bio inspired physics informed architecture represents a novel convergence of domain knowledge and machine learning advancing the field of secure real time and energy efficient intrusion detection for dynamic WSN environments.

Main contribution of this work,

- To address the challenges of manuscript presents an Enhanced Security and Attack Detection Framework leveraging Optimized Physics-Informed Neural Networks PINN-FFEM-IDSis proposed.
- The TDSMFF enhances data quality by removing noise and normalizing input, while the Gazelle Optimization Algorithm (GOA) selects the most relevant features.
- This framework synergizes the physical modeling capability of PINNs with optimized feature selection and hierarchical localization to enhance detection accuracy, minimize false positives, extend network lifetime.
- The TTAO is employed to fine-tune weights and biases of PINN, ensuring efficient and scalable threat detection under dynamic WSN conditions.

Rest of this manuscript is arranged as: part 2 explains literature survey, part 3 deliberates proposed method, part 4 presents results with discussion, part 5 conclusion.

2. Literature review

Several investigates previouslypresented in the literature related to IDS for WSN depend upon data mining, some recent researches are reviewed here,

Singh,et al., [21] have suggested ANN basis deep learning method to forecast Intrusion Detection (ID) inWSN. The suggested method uses ANN with complete connectivity and feed-forward learning in a deep learning predict count of k-barriers with high accuracy for quick ID and prevention.With 4 potential attribute size of circular area, sensors sensing level

and unique sensorsdeliverywhere trained and assessed the feed-forward ANN method.It employs critical features such as sensor ranges and area, resulting in high performance. The model employs only a few features, which may not encompass all elements influencing intrusion detection.

Gowdhaman, et al., [22] have suggested DNN-base intrusion identification for WSN.The better features from data were selected with a cross-correlation method, and selected parameters employed building block of DNN architecture to appear for intrusion. Findings demonstrated introduced DNN detects attacks effectively and outperforms Support Vector Machine. DNNs can reduce false positives, resulting in more accurate intrusion detection. It may not scale well for large deployments. The ensemble approach complicates the model making it difficult to execute and maintain.

Ravi, et al., [23] have presented feature fusion ensemble meta-classifier technique depending on RNN for intelligent network IDS in WSN. An E2E model utilising DL-base recurrent models for network attack detection and categorization. By extracting features from hidden layers of recurrent methods, the suggested model finds best features by using kernel-depend principal component analysis feature selection technique. Over time, model may react to new types of assaults and network behaviour changes, increasing its robustness and accuracy. Deep RNNs were prone to overfitting, especially if they were not sufficiently regularised or have a short training dataset.

Khedr, et al., [24] have presented Time Synchronized Multivariate Regressive Convolution Deep Neural Network for Sinkhole Attack identification in WSN. To minimise detection delays, the TSMR-CDNN technique combines reverse time synchronisation for its ability to offer accurate clock offsets and skews. By adjusting the threshold value, the Broken-stick regression approach was used to analyse multivariate data, including energy and clock variables, to improve detection skills. The method effectively manages fluctuations in

clock skews, which were typical in WSNs. Obtaining perfect time synchronisation in WSNs can be difficult, particularly in dynamic or large-scale networks.

Subbiahetal.,et al., [25] have presented Boruta feature selecting method and grid search RF are coupled to identify intrusions in wireless sensor networks. Effectiveness of BFS-GSRF was evaluated in comparison to ML techniques, such as Linear Discriminant Analysis, Classificationand Regression Tree. The suggested technique was evaluated on Network Security Laboratory Knowledge on Discovery database. Boruta selects only the most important features, increasing the Random Forest model's accuracy in identifying intrusions. Borate’s iterative feature selection approach can extend the model creation phase and increase its complexity.

Darvishi.,et al., [26] have presented Deep Recurrent Graph Convolutional Structure in Digital Twins. The suggested approach addresses the issue of sensor error identification, isolation, accommodation in huge-size network system. It suggested a deep recurrent graph convolutional structure-dependent technique for sensor validation was presented that concurrently learns the network structure and spatiotemporal interdependencies.Effectively detects and isolates sensor faults, increasing overall system dependability. Difficult to create and implement; requires extensive skill.

Darvishi, et al., [27] have presented a ML structure for sensor fault recognition, accommodationand isolationin digital twins.To create dependable digital twins, the proposed approach seeks to instantly detect abnormalities in sensor readings, identify the problematic ones, and accommodate them with appropriate approximated data. It provided higher precision and high computational time. But inaccurately identify or fail to detect defects, resulting in potential inaccuracies. Comparison table of literature review is displayed in Table 1.

Table 1: Comparison Table of Literature Survey

Author	Methods	objective	Merits	Demerits
Singh et al., [21]	To forecast intrusion detection in WSN using ANN.	Fully connected feed-forward ANN with limited input attributes.	It provides higher accuracy	It attains low sensitivity
Gowdhaman et al., [22]	To identify intrusions in WSN using deep learning.	DNN with cross-correlation-based feature selection.	It provides higher precision	It attains low sensitivity
Ravi et al., [23]	To detect and classify attacks in WSN using deep RNN.	Feature fusion ensemble with RNN and kernel PCA.	It provides low error rate	It attains low precision
Khedr et al., [24]	To detect sinkhole attacks in WSN via time-synchronized deep learning.	TSMR-CDNN with broken-stick regression and reverse time sync.	It provides low error rate reduction	It attains low precision.
Subbiah et al., [25]	To detect intrusions in WSN using feature selection and ensemble learning.	Boruta feature selection with grid search random forest.	It attains higher accuracy	It provides low recall

Darvishi et al., [26]	To detect and isolate sensor faults in large-scale networks.	Deep recurrent graph convolutional structure in Digital Twins.	It attains low residual	It provides low network
Darvishi et al., [27]	To recognize and accommodate digital twins.	Machine learning framework for real-time fault handling.	It provides higher FI-measure	It provides low network lifetime.

3. Proposed Methodology

This section, PINN-FFEM-IDS is proposed. These phases endure main 5 processes like Network model, feature selection, data acquisition, pre-processing, classification, optimization. The network model faces risks from wormhole and assumes uniform capabilities among legitimate nodes, adopting hierarchical clustering to conserve energy and extend network longevity. The KDD Cup 1999 dataset is utilized benchmark for IDS. Data normalisation is achieved via the TDSMFF technique. The Gazelle Optimisation Algorithm is used here to choose the best subsets of characteristics for discriminating between different sorts of attacks in the dataset. The final outcomes display that PINN-based technique optimised by TTAO The following figure 1 shows block diagram of PINN-FFEM-IDS model.

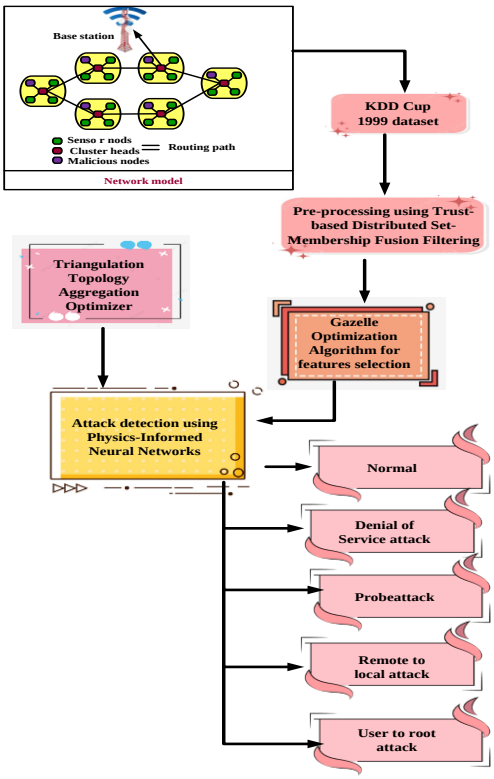

Figure 1: Block diagram of PINN-FFEM-IDS

3.1 Network Model

The simulated network includes sink, sensor, cluster head, attacker nodes shown. Throughout the system the sensor nodes have a tendency to cluster together. Each cluster selects a cluster head node to serve hub for cluster while delivering data to beacon nodes and base station. Using an optimisation technique depend on fitness function, beacon nodes determine the best routeing path. Through the creation of node clusters with one cluster head for allgroup the localisation system provides an exact position, location for sensor nodes. Periodically, sensor nodes provide system with an updated location.

3.1.1 Cluster formation with data aggregation

By grouping collection of sensors into clusters, network's resilience and power efficiency can be improved. Groups of related devices comprise sensor nodes inside the network. The sensor nodes that comprise cluster as a whole collect data, forward it to cluster coordinator.

- The sensor node's signal quality as it was received

- The amount of energy left in the node prior to activation
- The distance vector protocol's minimum required to reach base station. The distance vector method is utilized to calculate distance G among any two sensor nodes, as illustrated below equation (1).

$$G = \sqrt{(v_i - v_j)^2 + (r_i - r_j)^2} \tag{1}$$

Here, i *and* j denotes the nodes, the coordinates are r and v, respectively. The cluster head is probably determined by calculating the distance between any nodes with a short distance from the base stations. The energy transmission cost for k-bit data transfer over the G distance and the G_o threshold distance is provided as in equation (2)

$$F_{HY} = \begin{cases} h \times F_f + h \times F_k \times G^2, & if\ G \le G_o, \\ h \times F_f + h \times F_n \times G^4, & if\ G \le G_o, \end{cases} \tag{2}$$

Where, for single-bit data transmission, F_{HY} denotes transmitted energy, F_k signifies received energy, F_f signifies power discarded in transmitter. Channel-coding, filtering, modulation, and signal spreading all affect how much energy is lost. Defined a h length data transfer, the threshold distance for transmission G_o is defined by equation (3)

$$G_o = \sqrt{\frac{F_h}{F_n}} \tag{3}$$

The energy used by receiving node to receive message in k-bits is shown in equation (4)

$$F_{PY(f)} = f \times F_f \tag{4}$$

Where, $F_{PY(f)}$ denotes the energy used by the receiving node; F_h represents the power discarded in the receiver and F_n power discarded in number of nodes.

3.1.2 Localization Techniques

The localisation process is used in many WSN applications to locate target by comparing signal intensities of transmitters,receivers that have previously been installed in the region of interest. The precise location of WSN is assessed by distance vector hop localisation method and received signal strength indicator. To calculate coordinates of cluster heads,sensor nodes utilizing beacon nodes, distance vector localisation process is necessary and minimum hop count provided by following equation (5)

$$LC = \frac{\sum_{i \neq j} \sqrt{(v_i - v_j)^2 + (r_i - r_j)^2}}{\sum_{i \neq j} k_{ij}} \tag{5}$$

Here, LC denotes average distance hop for anchor node, v and r are the coordinate nodes, i *and* j represents the nodes and k is the data transmission node. After transmitting its data, the anchor node calculates the hop-size. It provided hop-size information, distance calculated among sensor node, anchor is given by equation (6)

$$G_{Qf} = L_Q Ci_{i\times} kr_{rf} \tag{6}$$

Here, G_{Qf} denotes sensor node, anchor, L_Q denotes position of anchor , $Ci_{i\times}$ is the area between the anchor and indeterminate nodes, k is the location of unknown node, Q spot of unidentified node. To make the system linear, can obtain set of expressions by subtracting from first equations, as shown in following equation (7).

$$W = \left(X'X\right)^{-1} X'D. \tag{7}$$

Here, W is represents achieving node localization, $\left(X'X\right)$ denotes real distances among one-hop neighbour nodes, leveraging such distances, X'represents the location of the node, D distances for precise localization in massive-scale WSN.Node localisation can be achieved in an easy and affordable way, both in terms of hardware and software. To achieve more

accurate localisation in large-scale WSNs, distance vector hop approach, however, completely omits calculating actual distances among one-hop neighbour nodes.

3.2 Data Acquisition

The input data are collected from KDD 99 dataset [28]. Every instance in the KDD 99 dataset has features that belong to a certain type of network data. Attack or normal are the labels assigned to each class. There are five primary classifications in the KDD 99 dataset such as Normal, DoS, User to Root, User to Root, Remote to User, Probing. Training uses 70% of dataset testing uses 15% and validation uses 15%.The KDD 99 dataset is listed in the table 2.

Table 2: Feature from KDD 99 Dataset

KDD 99Features	Num root
Protocol type	Su_attempted
Service	Wrong fragment
Flag	urgent
Src bytes	hot
Dst bytes	Num failed logins
Land	Logged in

3.3Pre-processing using Trust-based Distributed Set-Membership Fusion Filtering

In this step, TDSMFF [29] is utilized to data normalization. By including trust information across nodes, the TDSMFF technique improves distributed systems' durability, resulting in increased accuracy, resilience against malicious or unreliable nodes, overall efficiency in set-membership filtering operations. Iterative adversarial training aims to lessen negative effects of adversarial samples on learning process. It is given in equation (8),

$$\hat{l}_{m,s} = \hat{l}_{s|s-1} + P_{m,s}\,(h_{m,s} - P_{m,s}) \tag{8}$$

Here $\hat{l}_{m,s}$ signifies local estimation of $_{m,s}$ on sensor r , $P_{m,s}$ signifies filter parameters $\hat{l}_{s|s-1}$ denotes Vectors depend on user mobility, channel multi-path components, they are continuously recomputed with channel coherence time. It is given in equation (9)

$$P_{m,s} = \hat{L}_{s|s-1} Z_{m,s}^{E} \left(\frac{\hat{L}_s}{1-\rho_{m,s}} + \frac{S_{m,s}}{\rho_{m,s}} \right) \tag{9}$$

The nonlinear functions $\rho_{m,s}$ of data in Taylor series expansion formula are linearized. Z signifies metric of distance among m , s 2 input instances: adversarial version of input S , original input P .The node remove ellipsoidal center data, where loss function is definite sum of distance error square. In this stage, DSMFF is used to normalize data, remove noise, and improve quality of input data such that remain data is correct is given in equation (10),

$$I(d,\eta) = \sum_{j=1}^{N} \| l_j - \eta_s \|^2 \tag{10}$$

Where l_j denotes I sample, d,η signifies centroid linked to cluster, s signifies ellipsoidal shapes. The TDSMFF normalized input data. The pre-processed output is given to feature selection stage.

3.4 Gazelle Optimization Algorithm for features selection

The feature selection utilizing GOA [30] is discussed.The GOA offers several advantages for complex optimization tasks. Inspired by gazelles' natural behavior, it combines exploration and exploitation effectively, allowing it to escape local optima and converge toward global solutions. GOA demonstrates strong adaptability across diverse problem spaces and ensures fast convergence with minimal parameter tuning. Its lightweight structure supports computational efficiency, making it ideal for high-dimensional, nonlinear, or multi-objective optimization problems. GOA also shows robust performance in real-world engineering and data-driven applications. The stepwise procedures of GOA for feature selection are presented below.

Step 1: Initialization

The population generated stochastically among the given issue's upper bound (U_b) and lower bound (L_b) based on equation (11),

$$W = \begin{bmatrix} w_{1,1} & w_{1,2} & \cdots & w_{1,d-1} & w_{1,d} \\ w_{2,1} & w_{2,2} & \cdots & w_{2,d-2} & w_{2,d} \\ \cdot\cdot & \cdots & w_{a,b} & \cdots & \cdots \\ w_{m,1} & w_{m,2} & \cdots & w_{m,d-1} & w_{m,d} \end{bmatrix} \tag{11}$$

Where w represented the current candidate population, $w_{a,b}$ represented the positioning of b^{th} dimension of the a^{th} population, m denotes whole candidate population.

***Step 2*:** Random Generation

Input parameters are made at randomly. The optimal progressive value is chosen depend upon specific hyper parameter conditions.

Step 3: Fitness function

Initialized parameters are depending upon resolute current best position. It is shown in equation (12).

$$Fitness\ \ function = [selecting\ \ optimal\ \ \ features] \tag{12}$$

***Step 4*:** Brownian motion

A stochastic process where the standard Brownian motion appears at a point y and the step size is determined by Normal (Gaussian) probability distribution using zero $(\eta = 0)$ mean and unit variance $(\lambda 2 = 1)$ using equation (13),

$$g_b(y;\eta,\lambda) = \frac{1}{\sqrt{2\pi\lambda^2}} E\left(-\frac{(y-\eta)^2}{2\lambda^2}\right) = \frac{1}{2\pi} E\left(-\frac{y^2}{2}\right) \tag{13}$$

***Step 5*:** Levy flight

Itis a random walk that uses Levy distribution that shows power-law tai. Using the Levy distribution (power-law tail), levy flight is represented based on the following equation (14)

$$d_L(y;\alpha,\gamma)=\frac{1}{\pi}\int_0^{\infty}E(-\gamma p^{\alpha})\cos(py)\delta p \tag{14}$$

Where γ represented distribution index manages scale properties of motion, and δ represented unit of scale.In this case, y denotes scale unit, α signifies distribution index that controls motion. The algorithm provided by is used by GOA to produce stable Levy motion. The definitions of the variables y , α , and γ are as follows: y has normal distribution by mean 0, variance $\sigma 2$ y , α is set to 1.5.

Step 6: Exploitation Phase

During exploitation phase, gazelles are observed grazing calmly in absence of predators, alternatively, predators are actively pursuing the gazelles. This behavior is characterized by Brownian motion, encompassing both uniform and controlled phases that effectively cover nearby regions. The Exploitation phase can be mathematically depicted using the equation (15)

$$\vec{G}_{m+1}=\vec{G}_m+t.\vec{S}*.\vec{S}_B*.\left(E_m-\vec{S}_B*.\vec{G}_m\right) \tag{15}$$

Here $\vec{G}_{m+1}$ means the next iteration's solution, $\vec{G}_m$ means the current iteration's solution, t expresses gazelles grazing speed, $\vec{S}_B$ random number vectors of the Brownian motion, $\vec{S}$ uniform random numbers vector in [0,1].

Step 7: Explorationphase

The Exploration phase enhances the search capabilities in optimization problems. When a gazelle spots a predator, it instinctively runs, triggering the predator to give chase. Two runs are denoted through sudden direction change, this can be denoted as ϕ . The character of gazelle when it spots predator is mathematically expressed equation (16)

$$\vec{G}_{m+1} = \vec{G}_m + \beta.\mu\vec{S}^*.\vec{S}_L^*.\left(E_m - \vec{S}_L^*.\vec{G}_m\right) \tag{16}$$

Here β represents the top speed of the gazelle, $\vec{S}_L$ represents random numbers vector depended on Levy distributions. $\vec{G}_m$ denotes variable that controls predator's movement.

Step 8:Termination

In this step, GOA completes, best solution obtained through each process iterations returned as output. If all the processes are completed to select the 12 features are selected, it is shown in table 4. Then, selected features are fed to classification phase.

3.5Attack detection using Physics-Informed Neural Networks

In this section PINN [31] is used to classifying the attacks normal, denial attack, remote to local attack, probe attack. Neural networks with physical knowledge can handle issues that are characterised by sparse data or noisy experiment observations. Deploying deep learning and optimization in lightweight WSN nodes is achieved through a hierarchical architecture. Figure 2 shows the architecture diagram of PINN.

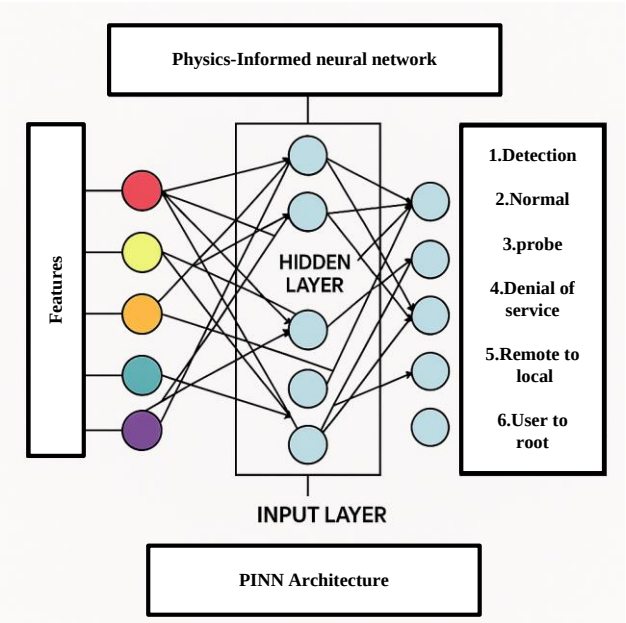

Figure 2: Architecture diagram of PINN

Sensor nodes handle simple sensing, while cluster heads perform complex tasks like GOA-based feature selection and PINN-based attack detection. PINNs are also known as neural networks for supervised learning issues because they may operate on known data while respecting any given physical law represented by general nonlinear partial differential equations (17).

$$\begin{aligned} E(v(x);\gamma) &= k(x) \qquad x\ in\ \ \Omega \\ D(v(x)) &= g(x) \qquad x\ in\ \ \Omega \end{aligned} \tag{17}$$

Here, E denotes the domain function; Ω is its boundary; v stands for the unknown solution; γ is the physics-related parameter, k for the function defining the problem's data, and E for the nonlinear differential operator. Here, $x:[x1,.....,x(d-1);k$ denotes space-time coordinate vector. Lastly, it is conceivable to designate D representing boundary conditions relevant to problem and g denotes boundary function. The maximum pooling method was applied equation (18)

$$\hat{v}_\theta(x) \approx v(x) \tag{18}$$

Here, $v(x)$ is produced through the computational prediction of neural network, which is parameterized by set of parameters and a neural network approximation realised with θ is indicated by $\hat{v}_\theta$.In this situation, the neural network (NN) has to learn how to approximate the differential equations in (19).

$$\theta^* = \arg\min_\theta (\omega_D L_D(\theta) + \omega_D L_D(\theta) + \omega_b L_{data}(\theta)) \tag{19}$$

Here, $\arg\min_\theta$ denotes the activation functions, L_D represents the hidden layers, ω_D is the softmax function. PINNs can be considered supervised learning methodologies for inverse problems or when some physical properties are derived from potentially noisy data.A general L -layer deep neural network can be expressed as the composition of L functions; θ^*

indicates the set of parameters for the i^{th} layer and L_D are state variables. A following equation (20) is used to classify the attacks.

$$v_\theta(x) = k_L \circ k_{L-1} ..... \circ k_1(z) \tag{20}$$

Where the layer composition denoted by $\circ$, k_L is to be understood as $k_L \circ k_{L-1} ..... \circ k_1(z)$ and each is specified on two inner product spaces. Finally PINN detects the attacks likes'normal, remote to local attack, user to root attack, probe attack, denial attack. Owing to its pertinence, convenience, AI-dependent optimization method is considering in PINN classifier. Here, TTAO is used to optimize PINN. Here, TTAO is used for tuning weight, bias parameter of PINN.

3.6 Optimization utilizing Triangulation Topology Aggregation Optimizer

The weights parameter D and L of TCRMGCN is enhanced utilizing TriangulationTopology Aggregation Optimizer (TTAO) [32]. In the proposed TTAO method four agents use similar triangles as fundamental evolutionary units to produce similar triangles of different sizes. Initially, TTAO creates equal dispersing populace to enhance parameter of PINN. The important key is enhanced utilizing TTAO procedure linked flowchart is presented in Figure 2.

***Step 1*:**Initialization

The population size and variable dimension are two factors that are being examined there. Each vertex in triangle topological unit signifies search agent in search agent hierarchy. Created for each agent is given in equation (21),

$$G_{j,1} = S_0 \times \left(\vec{VA} - \vec{LA}\right) + \vec{LA} \tag{21}$$

Where, j denotes positive integer value, $M_{j,1}$ denotes initial search individual in j^{th} triangular topological unit, $\vec{VA}$ denotes upper bound, $\vec{LA}$ implies lower bound.

***Step 2*:** Random generation

Input parameters made at randomly. Best fitness values are selected based upon clear hyper parameter situation.

***Step 3*:** Fitness Function

To generate random solution, initialized values are used. It is assessed for optimizing weight parameter $E \, and \, \theta$ of detection of cyber-attacks on autonomous vehicles utilizing parameter optimization value. It is shown in equation (22),

$$Fitness \; Function = optimize \; (D \, and \; L) \tag{22}$$

Where, D is used to increasing the accuracy D and L is used to decreasing the false positive rate.

Step 4: Generic Aggregation D

Information is obtained from respectable individuals in various triangular units, new, practical solutions are produced. The improved two-vertex interaction produces newly created individual is shown in equation (23),

$$\vec{Y}_{j,new1}^{\,s+1} = p_4 * \vec{Y}_{j,best}^{\,s} + \; E \; \left(1 - s_4\right) * \vec{Y}_{s\,and,best}^{\,s} \tag{23}$$

Where, $[0,1]$ denotes random number p_4 is s^{th} iteration, $\vec{Y}_{j,best}^{\,s}$ and $\vec{Y}_{s\,and,best}^{\,s}$ signifies best individual for unit, arbitrarily selected unit j, $\vec{Y}_{j,new1}^{\,s+1}$ signifies optimum or suboptimal search agent.

Step 5: Local Aggregation L

At this time, triangular topological units aggregate internally. After comprehending previous step, triangular topology was briefly created by 2 group vertices with high fitness values and people with either updated ideal or low fitness, respectively.

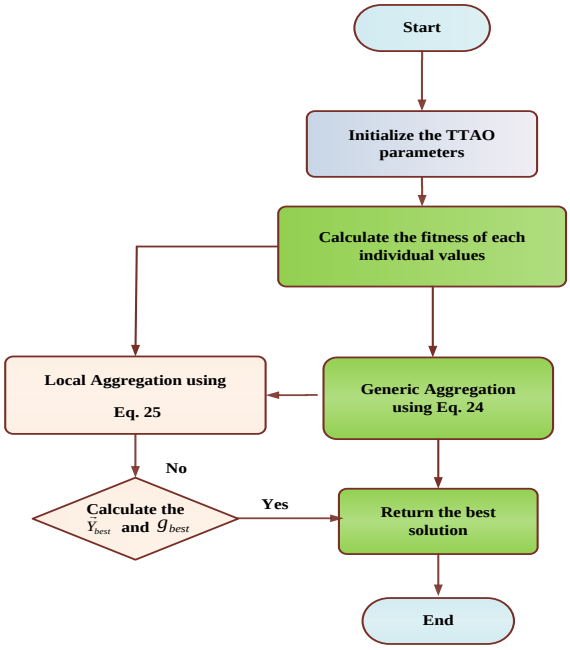

Figure3: Flowchart of TTAO for enhancing PINN

In a certain location, each group is re-examined using each topological triangle unit is given in equation (24), Figure3

$$\vec{Y}_{j,new2}^{s+1} = \vec{Y}_{j,best}^{s} + \alpha * \left(\vec{Y}_{j,best}^{s+1} - \vec{Y}_{j,tbest}^{s+1}\right) \tag{24}$$

Where, $\vec{Y}_{j,new2}^{s+1}$ denotes optimum or suboptimal search agent, $\vec{Y}_{j,best}^{s}$ signifies arbitrarily chosen unit, α denotes decreasing value is used to change the aggregate scope size. A triangle network topology's improved routing pathways can lower latency and enhance network performance in general.

Step 6:Termination

The weight parameter E *and* θ from PINN are optimized using support of TTAO process will repeat step 3 iteratively fulfil halting criteria $G = G + 1$ is satisfied. The ERR-EFIGNN method effectively detects the attacks with higher accuracy, lower false positive rate.

4. Result with discussion

The stimulation results of ERR-EFIGNN are discussed. The simulation is executed in i3-6100U CPU @ 2.30 GHz with 4 GB of RAM on MATLAB R2016a utilizing KDD'99

dataset. The performance metrics includes accuracy, recall, computational time, precision, Data uploading, retrieval phases, false-positive rate, Localization error analysis beacon nodes, lifetime of network, residual energy are examined. Obtained results of ERR-EFIGNN technique are analyzed with existing likes Artificial Neural Network depend intrusion detection in WSN (ANN-ID-WSN), Deep Neural Network intrusion detection scheme to forecast intrusion detection in WSN (DNN-FID-WSN), and An intelligent network ID technique based on RDL-depend feature fusion ensemble meta-classifier (RDL-WSN-DNN) techniques.Simulation setup for network method is given in table 5.

4.1 Performance Measures

Performance metrics are used to evaluate proposed technique's efficiency, metrics such as accuracy, precision, recall, Localization error analysis beacon nodes, computational time, Data uploading and retrieval phases, lifetime of network, false-positive rate, residual energy.

4.1.1 Accuracy

The percentage of correct predictions, total recommendations classifier made are computed by this evaluation statistic. It is given in equation (25)

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{25}$$

Here, TN denotes true negative, TP represents true positive, FP signifies false negative, FN denotes false negative.

4.1.2 Precision

It is a measure of obtained data's degree of accuracy. It is proportion of "true positives" to each "positive instances," where "true positives" denotes exactly returned outcomes. It is shown in equation (26),

$$\Pr ecision = \frac{TP}{TP + FP} \tag{26}$$

4.1.3 False positive rate

The number of wrongly labelled positive cases as negative is called as false positive rate. The probability that model mistakenly classify negative event as positive is measured.

$$FPR = \frac{FP}{FP + TN} \tag{27}$$

4.1.4 Residual energy

The amount of energy remaining an after a exact time. It is an important indicator for calculating longevity, efficiency of network. Higher residual energy shows that the node can run for an extended period of time, which is critical in situations where nodes are impossible to replace or recharge.

$$EC = ET - EL \tag{28}$$

Where**,** ET is the total energy consumed by node, EC denotes energy consumed to current time, EL represents the life time energy.

4.1.5 Lifetime of the network

A network's lifetime refers to the amount of time it remains operational and capable of performing its intended functions. In the context of WSNs and other similar networks, it frequently refers to the time it takes for the first node or a critical number of nodes to run out of energy and no longer is able to perform network activities.

$$alive(N) = total(N) - Dead(N) \tag{29}$$

4.2 Performance analysis

Fig 4-7 portrays experimental results of PINN-LAD-WSN technique. The PINN-LAD-WSNtechnique is compared with existing ANN-ID-WSN, DNN-FID-WSN, INS-WSN-DNNmethod.

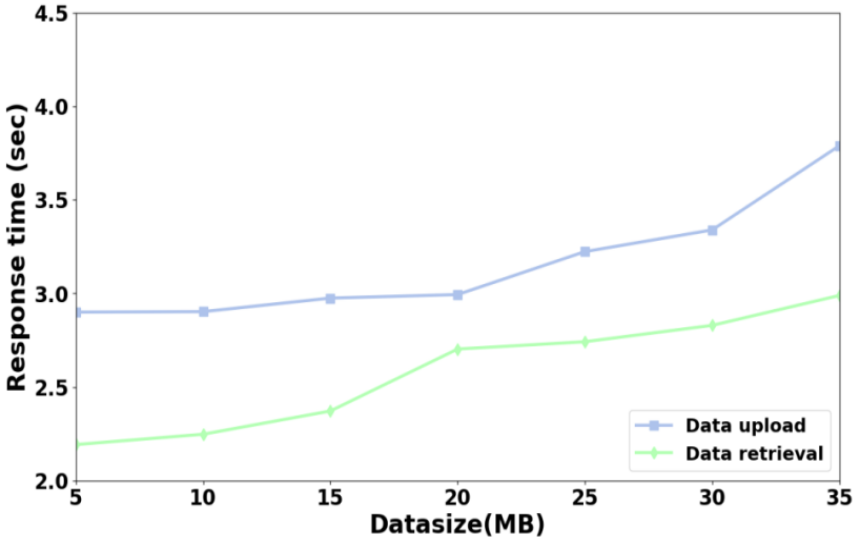

Figure 4: Performance Analysis of Data uploading and retrieval phases

Figure 4 shows data uploading and retrieval phase's analysis.The graph which shows data sizes ranging from 5 MB to 35 MB shows the relationship between data size and reaction time for both uploading and retrieving data. The uploading data response time increases gradually, from slightly less than 3 seconds for 5 MB to roughly 4.5 seconds for 35 MB. As data size increases, this trend points to a nonlinear increase in response time. This suggests that, in general, uploading data takes longer than retrieving data and grows faster with larger data quantities.

Table 3: Performance Analysis of Accuracy

Techniques	**Accuracy (%)**				
	Normal	**Denial attack**	**Probe attack**	**Remote to local attack**	**User to root attack**
INS-WSN-DNN	90.26	84.27	81.24	82.32	84.16
ANN-ID-WSN	70.36	67.44	56.37	60.44	73.25
DNN-FID-WSN	67.37	73.45	65.56	62.33	70.24
PINN-LAD-	95.34	93.56	97.39	95.77	96.38

WSN(Proposed)

Table 3 Performance analysis ofAccuracy.The number of cases with exact predictions out of all the instances was used to calculate the accuracy. The precision was indicated by the positive prediction value. The number of positive samples compared to those predicted to be positive was used to calculate the accuracy. Here, PINN-LAD-WSN method attains8.55%, 7.43% and 6.62% higher accuracy for normal; 8.55%, 7.43%,6.62% higher accuracy for denial attack; 26.35%, 31.23%, 30.62% greater accuracy for probe attack; 7.55%, 8.36% and 28.32% higher accuracy for remote to local attack;7.55%, 8.36% and 7.32% greater accuracy for user to root attack are analysed with existing method such as ANN-ID-WSN, DNN-FID-WSN, INS-WSN-DNN.

Figure 5shows localization error analysis. The graph shows how adding more beacon nodes affects the percentage of localisation errors in two distinct circumstances Data upload and Data retrieval. This suggests that increasing beacon nodes can enhance accuracy in the data upload situation by lowering the localisation error. This shows that more beacon nodes are beneficial for data retrieval scenarios as fewer localisation errors are consistently achieved across the spectrum.

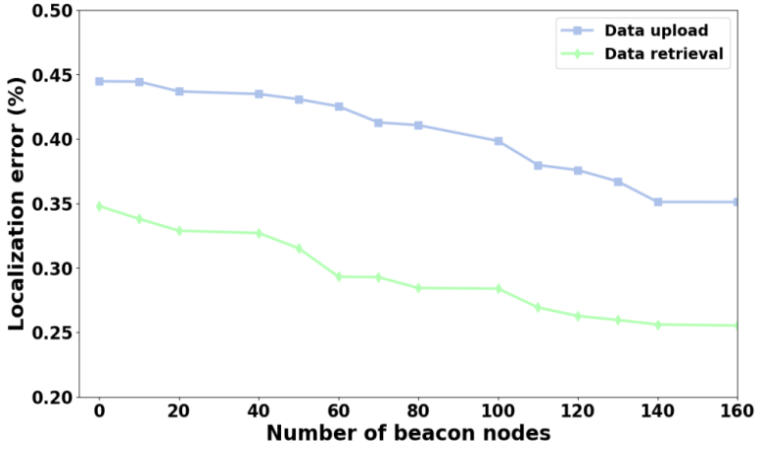

Figure 5: Performance Analysis of Localization error

Table 4: False positive rate analysis

Techniques	False positive rate (%)				
	Normal	**Denial attack**	**Probe attack**	**Remote to local attack**	**User to root attack**
PINN-LAD-WSN(proposed)	98.26	95.45	97.57	93.70	95.38
ANN-ID-WSN	68.27	72.19	74.27	80.28	76.10
DNN-FID-WSN	67.37	80.27	84.26	73.54	80.38
INS-WSN-DNN	78.38	69.20	78.28	65.38	71.20

Table 4 shows Performance Analysis of false positive rate.It determines the percentage of non-attack cases that are mistakenly categorised as attacks. A larger false positive rate suggests that there is a greater chance of mistaking routine actions for harmful activity, which could result in pointless alerts or the waste of resources in the reaction.Here, PINN-LAD-WSN method attains8.40%, 7.49% and 6.15% higher false positive rate for normal: 6.15%, 6.53% and 5.41% higher false positive rate for denial attack; 7.39%, 8.63% and 6.56% higher false positive rate for probe attack; 8.53%, 7.72% and 6.43% higher false positive rate for remote to local attack; 7.55%, 6.43% and 6.12% higher false positive rate for user to root attack are analysed with existing methods such as ANN-ID-WSN, DNN-FID-WSN, INS-WSN-DNN.

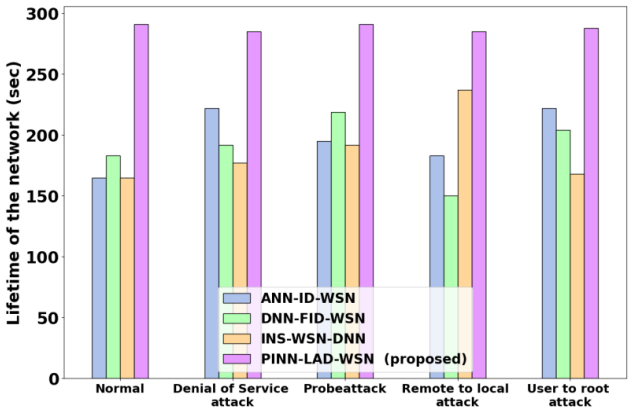

Figure 6: Life time of network analysis

Fig 6 shows life time of network analysis.The amount of time that a network can function normally before major nodes start to malfunction as a result of running out of energy is referred to as the network lifetime. Here, PINN-LAD-WSN method attains7.40%, 6.49% and 5.15% higher life time of the network for normal: 7.15%, 8.53% and 9.41% higher life time of the network for denial attack; 6.39%, 7.63% and 8.56% higher life time of the network for probe attack; 7.53%, 7.72% and 7.43% higher life time of the network for remote to local attack; 6.55%, 6.43% and 7.12% higher life time of the network for user to root attack are analysed with existing method such as ANN-ID-WSN, DNN-FID-WSN and INS-WSN-DNN.

Fig 7 portrays residual energy analysis. The energy or capacity that sensor nodes have left over after completing operations like detecting, processing, and communication is referred to as residual energy. For the network to be reliable and long-lasting, nodes must be able to operate for longer periods of time before needing to be recharged or replaced. This is shown by more residual energy. Here, PINN-LAD-WSN method attains7.40%, 7.49% and 6.15% lower residual energy for normal: 8.15%, 7.53% and 5.41% lower residual energy for denial attack; 23.39%, 18.63% and 26.56% lower residual energy for probe attack; 8.53%, 7.72% and 7.43% lower residual energy for remote to local attack; 7.55%, 6.43% and 5.12% lower

residual energy for user to root attack are analysed with existing method such as ANN-ID-WSN, DNN-FID-WSN, INS-WSN-DNN.

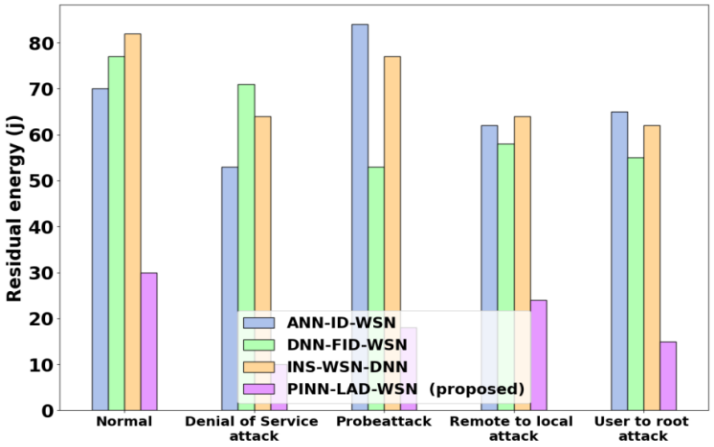

Figure 7: Residual energy analysis

Table 5: Performance Analysis of Precision

	Precision (%)				
Techniques	Normal	Denial attack	Probe attack	Remote to local attack	User to root attack
ANN-ID-WSN	87.27	78.30	77.55	88.28	75.16
DNN-FID-WSN	77.22	87.56	86.25	75.27	86.25
INS-WSN-DNN	87.66	87.45	77.26	68.59	78.25
PINN-LAD-WSN(proposed)	98.66	97.45	98.26	97.59	98.25

Table 5 Performance analysis of precision. Each bar shows the precision score obtained by a given model or method for classifying ragas. Determine which model or method has the highest precision for a certain classification challenge using the graph. Here, PINN-LAD-WSN method attains6.40%, 7.49% and 5.15% greater accuracy for normal, 5.15%, 6.53%,

7.41% higher precision for denial attack; 6.39%, 5.63%, 6.56% greaterprecision for probe attack; 7.53%, 7.72% and 8.43% higher precision for remote to local attack; 7.55%, 8.43% and 6.12% higher precision for user to root attack are analysed with existing methods such as ANN-ID-WSN, DNN-FID-WSN, INS-WSN-DNN.

4.3 Computational complexity

The time complexity during fitness assessment and maximum iterations, $Maxgen$, number of objectives, f population size, $Popsize$ is $P(Maxgen \times f \times popsize)$. The amount of time needed to initialize population is $P(popsize \times f)$. The TTAO necessitates $P(f \times (s + popsize))$ time for archive updates in non dominated solution, parameter σ signifies best search agents. Overall time complexity is $P(Maxgen \times f \times (popsize + s) \times L)$, The complexity of space through population development in memory necessitates $P(popsize \times f)$time. Until process reaches maximum iterations, fitness calculation, archive update repeat. The TTAO and N input is $P(N^3)$. The PINN-LAD-WSN Optimized with TTAO is $O(N^3 \times Maxgen \times f \times popsize)$ Figure 8 portrays computational complexity analysis.

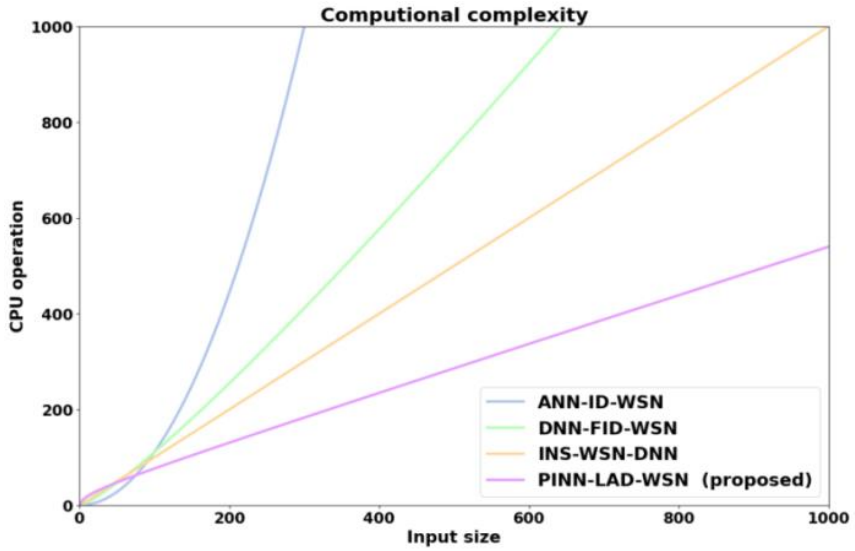

Figure 8: Computational Complexity analysis

Figure 8 portrays computational complexity analysis. The PINN-LAD-WSN techniques increase memory utilization and CPU operation time linearly. The time complexity of PINN-LAD-WSN technique portrays lower than existing method such as ANN-ID-WSN, DNN-FID-WSN, INS-WSN-DNN.

4.4 Discussion

The MLPANN method attains a higher detection accuracy of 99.62% when utilizing benchmark dataset for WSN-DS. The suggested method has the best average detection for a number of suspicious nodes, as confirmed by its efficacy in identifying and localizing different attack classes. Since it successfully identifies and locates many attack kinds, this method is unique. The proposed PINN-FFEM-IDS is a revolutionary approach that can measure security, performance for optimal region coverage. It is developed for WSNs with hierarchical architecture homogeneous, heterogeneous sensor nodes. The dataset are utilized to evaluate proposed system accuracy in detecting, localizing different types of attacks. Malicious nodes beacons and sensors were used in a tiered manner to simulate target field. To improve accuracy of malicious node identification and localization in WSNs a number of strategies are recommended. More attack types and strategies are added in this proposed model which builds on this work.

5. Conclusion

In this work, a novel attack detection and security enhancement framework, PINN-FFEM-IDS, is proposed to address multi-class intrusion threats in Wireless Sensor Networks (WSNs). By integrating Physics-Informed Neural Networks (PINNs) with TDSMFF and Gazelle Optimization Algorithm (GOA), the framework ensures robust data normalization and optimal feature selection critical for accurate threat classification. Further, the inclusion of the Triangulation Topology Aggregation Optimizer (TTAO) for hyperparameter tuning of the PINN significantly enhances detection accuracy and reduces false positives. Experimental

validation using the KDD Cup 1999 dataset confirms that PINN-FFEM-IDS model outperforms existing models such as ANN-ID-WSN, DNN-FID-WSN, and INS-WSN-DNN across multiple attack categories. The proposed method achieved up to 26.35% higher accuracy for probe attacks, 8.55% higher for denial attacks, and substantial improvements in residual energy and network lifetime, demonstrating its effectiveness in dynamic, resource-constrained WSN environments. Future enhancements will focus on developing a lightweight adaptive PINN variant with interpretable layers, integrating cross-layer optimization strategies, and deploying the framework in real-time IoT-WSN testbeds for resilient cyber-threat mitigation and autonomous anomaly localization.

Compliance with Ethical Standards

Disclosure of potential conflicts of interest

Authors declare that they have no conflict of interest.

Ethical Approval and Consent to participate: This article does not contain any studies with human participants performed by any of the authors.

Human and Animal Ethics: Not Applicable

Consent for publication: Not Applicable

Availability of supporting data: Data sharing does not apply to this article as no new data has been created or analyzed in this study.

Funding: This research did not receive any specific grant from funding agencies in the public,

commercial, or not-for-profit sectors.

Materials and Methods: Not applicable

Results and Discussions: Not applicable

Declarations: Not applicable

Conflicts of interest/Competing interests: Not applicable

Acknowledgements: Not applicable

Authors' contributions

Dr.B.Meenakshi -(Corresponding Author): Conceptualization, Methodology, Writing-Original draft preparation.

Dr.D. Karunkuzhali – Supervision

Reference

[1] Halbouni, A., Gunawan, T.S., Habaebi, M.H., Halbouni, M., Kartiwi, M. Ahmad, R., (2022). CNN-LSTM: hybrid deep neural network for network intrusion detection system. *IEEE Access*, 10, pp.99837-99849.

[2] Ravi, V., Chaganti, R. Alazab, M., (2022). Recurrent deep learning-based feature fusion ensemble meta-classifier approach for intelligent network intrusion detection system. *Computers Electrical Engineering*, *102*, p.108156.

[3] Narasimhan, H., Vinayakumar, R. Mohammad, N., (2021). Unsupervised deep learning approach for in-vehicle intrusion detection system. *IEEE Consumer Electronics Magazine*.

[4] Hussain, K., Xia, Y., Onaizah, A.N., Manzoor, T. Jalil, K., (2022). Hybrid of WOA-ABC proposed CNN for intrusion detection system in wireless sensor networks. *Optik*, *271*, p.170145.

[5] Zhiqiang, L., Mohiuddin, G., Jiangbin, Z., Asim, M. Sifei, W., (2022). Intrusion detection in wireless sensor network using enhanced empirical based component analysis. *Future Generation Computer Systems*, *135*, pp.181-193.

[6] Gavel, S., Raghuvanshi, A.S. Tiwari, S., (2021). A novel density estimation based intrusion detection technique with Pearson's divergence for wireless sensor networks. *ISA transactions*, *111*, pp.180-191.

[7] Simon, J., Kapileswar, N., Polasi, P.K. Elaveini, M.A., (2022). Hybrid intrusion detection system for wireless IoT networks using deep learning algorithm. *Computers Electrical Engineering*, *102*, p.108190.

[8] Abdallah, E.E. Otoom, A.F., (2022). Intrusion Detection Systems using supervised machine learning techniques: a survey. *Procedia Computer Science*, *201*, pp.205-212.

[9] Ramana, K., Revathi, A., Gayathri, A., Jhaveri, R.H., Narayana, C.L. Kumar, B.N., (2022). WOGRU-IDS—An intelligent intrusion detection system for IoT assisted Wireless Sensor Networks. *Computer Communications*, *196*, pp.195-206.

[10] Narasimha Prasad, S., SenthamilSelvan, K. Lakshmi Dhevi, B., (2022). Intrusion detection system in wireless sensor networks fair resource allocation using geometric deep learning techniques. *Wireless Personal Communications*, pp.1-12.

[11] Choudhary, D. Pahuja, R., (2022). Deep learning approach for encryption techniques in vehicular networks. *Wireless Personal Communications*, *125*(1), pp.1-27.

[12] Deshp e, S., Gujarathi, J., Ch re, P. Nerkar, P., (2021). A comparative analysis of machine deep learning algorithms for intrusion detection in wsn. *Security Issues Privacy Threats in Smart Ubiquitous Computing*, pp.173-193.

[13] Dina, A.S. Manivannan, D., (2021). Intrusion detection based on machine learning techniques in computer networks. *Internet of Things*, *16*, p.100462.

[14] Roy, S., Li, J., Choi, B.J. Bai, Y., (2022). A lightweight supervised intrusion detection mechanism for IoT networks. *Future Generation Computer Systems*, *127*, pp.276-285.

[15] Saheed, Y.K., Abiodun, A.I., Misra, S., Holone, M.K. Colomo-Palacios, R., (2022). A machine learning-based intrusion detection for detecting internet of things network attacks. *Alex ria Engineering Journal*, 61(12), pp.9395-9409.

[16] Maheswari, M. Karthika, R.A., (2021). A novel QoS based secure unequal clustering protocol with intrusion detection system in wireless sensor networks. *Wireless Personal Communications*, *118*, pp.1535-1557.

[17] Singh, A., Nagar, J., Sharma, S. Kotiyal, V., (2021). A Gaussian process regression approach to predict the k-barrier coverage probability for intrusion detection in wireless sensor networks. *Expert Systems with Applications*, *172*, p.114603.

[18] Lai, Y., Tong, L., Liu, J., Wang, Y., Tang, T., Zhao, Z. Qin, H., (2022). Identifying malicious nodes in wireless sensor networks based on correlation detection. *computers & security*, 113, p.102540

[19] Otair, M., Ibrahim, O.T., Abualigah, L., Altalhi, M. Sumari, P., (2022). An enhanced grey wolf optimizer based particle swarm optimizer for intrusion detection system in wireless sensor networks. *Wireless Networks*, *28*(2), pp.721-744.

[20] Hazman, C., Guezzaz, A., Benkirane, S. Azrour, M., (2023). Toward an intrusion detection model for IoT-based smart environments. *Multimedia Tools Applications*, pp.1-22.

[21] Singh, A., Amutha, J., Nagar, J. Sharma, S., (2023). 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*, p.118588.

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

[23] Ravi, V., Chaganti, R. Alazab, M., (2022). Recurrent deep learning-based feature fusion ensemble meta-classifier approach for intelligent network intrusion detection system. *Computers Electrical Engineering*, *102*, p.108156.

[24] Khedr, A.M., Raj, P.P. Rani, S.S., (2024). Time Synchronized Multivariate Regressive Convolution Deep Neural Network Model for Sinkhole Attack Detection in WSN. *Wireless Personal Communications*, *134*(1), pp.361-382.

[25] Subbiah, S., Anbananthen, K.S.M., Thangaraj, S., Kannan, S. Chelliah, D., (2022). Intrusion detection technique in wireless sensor network using grid search r om forest with Boruta feature selection algorithm. *Journal of Communications Networks*, *24*(2), pp.264-273

[26] Darvishi, H., Ciuonzo, D. Rossi, P.S., (2023) Deep Recurrent Graph Convolutional Architecture for Sensor Fault Detection, Isolation Accommodation in Digital Twins. *IEEE Sensors Journal*.

[27] Darvishi, H., Ciuonzo, D. Rossi, P.S., (2022). A machine-learning architecture for sensor fault detection, isolation, accommodation in digital twins. *IEEE Sensors Journal*, *23*(3), pp.2522-2538.

[28] https://www.kaggle.com/datasets/galaxyh/kdd-cup-1999-data

[29] Wu, H., Zhu, H., Li, X. Amuri, M.J.V., (2023). Trust-based distributed set-membership filtering for target tracking under network attacks. *IEEE Access*.

[30] Ekinci, S. Izci, D., (2023). Enhancing IIR system identification: Harnessing the synergy of gazelle optimization simulated annealing algorithms. *e-Prime-Advances in Electrical Engineering, Electronics Energy*, *5*, p.100225.

[31] Jagtap, A.D., Mao, Z., Adams, N. Karniadakis, G.E., (2022). Physics-informed neural networks for inverse problems in supersonic flows. *Journal of Computational Physics*, *466*, p.111402.

[32] Zhao, S., Zhang, T., Cai, L. Yang, R., (2024). Triangulation topology aggregation optimizer: A novel mathematics-based meta-heuristic algorithm for continuous

optimization engineering applications. *Expert Systems with Applications*, *238*, p.121744.