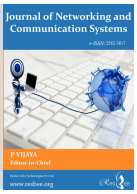
Vol.8 Issue 2 April 2025

Journal of Networking and Communication Systems

Received 3 March, Revised 12 March, Accepted 11 April



Adaptive Apiary Organizational-based Optimization with Deep Learning for Attack Detection in WSN

Arun Agarwal

Department of ECE
ITER, Siksha 'O' Anusandhan, Deemed to be University
Khandagiri, Bhubaneswar-751030, Odisha, India.
arunagrawal@soa.ac.in

Abstract: Wireless Sensor Networks (WSNs) are extremely susceptible to a variety of attacks due to their distributed architecture and resource limitations. The complexity of some intrusions, dynamic network behavior, and limited processing power make it challenging to detect these attacks efficiently and accurately. To address this critical issue, we propose a novel and robust intrusion detection framework tailored specifically for WSNs. To solve this, an effectual approach called Adaptive-Apiary Organizational Algorithm Deep Stacked Autoencoder (Ada-AOOA_DSA) is designed for attack detection in WSN in this article. This framework is distinguished by its hybrid learning and optimization design, ensuring adaptability to various attack vectors and noise conditions. The WSN is simulated first to emulate real-world communication and attack scenarios. In the attack detection model, input data is acquired from a particular dataset. Thereafter, the data normalization is carried out using median normalization to scale features uniformly and minimize the influence of outliers. Next, features are selected employing the correlation coefficient, ensuring the most suitable and non-redundant features are retained for assessment. Subsequently, the attack is detected employing a Deep Stacked Autoencoder (DSA), which is tuned employing the proposed Ada-AOOA algorithm. The Ada-AOOA is a newly established optimization method that integrates an adaptive concept with the Apiary Organizational Optimization Algorithm (AOOA). By combining the deep learning capabilities of DSA with the search efficiency of Ada-AOOA, the proposed method effectively captures complex attack patterns in WSNs. Furthermore, the proposed Ada-AOOA_DSA is examined considering numerous measures, including accuracy, True Positive Rate (TPR), and True Negative Rate (TNR), and the values acquired are 93.876%, 95.866%, and 92.654%, respectively. These results demonstrate that the Ada-AOOA_DSA achieves a high level of precision and generalization, outperforming several existing techniques in the literature.

Keywords: Attack Detection, Wireless Sensor Network, Security, Deep Learning, Intrusion Detection

Nomenclature

Abbreviations	Description
WSN	Wireless Sensor Network
LSTM	Long Short-Term Memory
AAOO	Adaptive Apiary Organizational based Optimization
DL	Deep Learning
ML	Machine Learning
TP	True Positive
TN	True Negative
FP	False Positive
FN	False Negative
PDR	Packet Delivery Ratio
FPR	False Positive Rate
TPR	True Positive Rate
DoS	Denial of Service
IDS	Intrusion Detection System
ANN	Artificial Neural Network
SNR	Signal-to-Noise Ratio

1. Introduction

WSNs have the potential to meet the requirements of several vital real-time applications and devise a new generation of distributed schemes. Further, wireless sensor node technology serves as a reliable communication platform for the majority of Internet of Things (IoT) devices. WSNs represent the essential and significant elements of the IoT [12] [1]. A WSN uses radio transceivers to spatially deploy small, low-

power sensor devices that monitor and gather data across diverse environments. WSNs can adapt to harsh environments, unlike wired networks. The recent development in WSNs is often wireless multimedia sensor networks. It collects scalar measures from the sensors utilized, which can obtain and process streaming media. This data encompasses streams of audio, video, and images gathered from Sensor Nodes (SNs). WSNs have been applied in several categories of fields, like home automation, remote monitoring, and environmental monitoring [13] [3]. They are valued for their simplicity, affordability, and adaptability in critical applications. WSNs meet real-world application requirements and are simple, affordable, and easy to utilize in a variety of critical areas. Throughout this paper, the term "sensor nodes" is consistently used to maintain clarity and uniformity when referring to the devices deployed in WSNs. Nevertheless, WSNs are extremely susceptible to several kinds of security attacks, especially Denial of Service (DoS) attacks, due to their drawbacks and computational capacity. The two main drawbacks are energy efficiency and security. The primary security attacks on WSNs are DoS attacks, node duplication, and node damage [1]. IDS systems monitor network traffic and node behavior, searching for any unusual or suspicious behavior that might indicate a security breach. IDS makes it possible to immediately detect and notify operators of possible attacks, allowing for prompt actions to reduce risks, protect private information, and assure network integrity and dependability [3].

Machine learning (ML) is a branch of Artificial Intelligence (AI), which is utilized in cybersecurity applications, including zero-day attack detection and prediction schemes. The four categories of ML approaches are unsupervised, reinforcement, supervised, and semi-supervised. ML is designed to be employed in reliable situations, as cyberattacks may lead to unstable conditions. Deep Learning (DL) can be considered a set of ML algorithms that undergo numerous phases and are trained on various databases. To preserve shared and stored data and information, it is essential to detect attacks in WSNs. More researchers have focused on employing ML's core and subcategories in cybersecurity to detect rejection attacks, malware, spam, and biometric identification [2]. However, training ML models effectively can be difficult due to insufficient labeled data for certain attack types, which leads to poor generalization. It may be difficult to efficiently train ML methods for some kinds of attacks due to a lack of labeled data. Poor generalization outcomes from particular attack patterns having insufficient instances. The efficacy of DL in big data domains can be applied to counteract cyber threats since attack mutations are similar to minor variations in image pixels. By forming high-level invariant representations of the training data, DL can learn the true face of cyber data on even minor changes, revealing its ability to adapt to slight variations in network data. DL's capacity to abstract meaningful features from raw data makes it particularly well-suited to WSN environments, where attacks may manifest in subtle and complex patterns. Recent findings on traffic classification and IDS suggest that DL may have a new application in detecting cybersecurity attacks, even though its application has primarily been limited to big data domains [14] [15] [16] [11].

The key intention of this work is to establish an effective technique termed Ada-AOOA_DSA for attack detection in WSN. Primarily, the WSN is simulated, and the attack detection process is carried out. In this process, the input data is obtained from the specified database, and it is passed for data normalization. Here, data is normalized by exploiting median normalization. Thereafter, the features are selected using the correlation coefficient. Furthermore, Ada-AOOA_DSA is employed for attack detection, where the DSA is trained by the proposed Ada-AOOA. Here, the proposed Ada-AOOA is the combination of the Adaptive concept and AOOA. The main objective of the developed technique is to minimize the false detection of threats as well as to increase the attack detection performance.

The primary contribution of this article is given as follows,

- ***Devised Ada-AOOA_DSA for attack detection in WSN:*** The Ada-AOOA_DSA is devised for attack detection in WSN in this work. In this case, the DSA model is employed for detecting the attack, and the proposed Ada-AOOA, developed by fusing the adaptive concept and AOOA, is exploited to train the DSA for accurate detection.

The residual sections of this research are as follows: Section 2 demonstrates the review of conventional research, Section 3 deliberates the system model, and a detailed process of the newly devised Ada-AOOA_DSA technique is explicated in Section 4. Next, Section 5 focuses on experimental outcomes, and the conclusion of this work is presented in Section 6.

2. Motivation

WSNs are widely exploited in crucial applications, such as healthcare, military surveillance, and environmental monitoring, because of their capacity to sense, process, and send data from distributed environments. Nevertheless, WSNs are highly vulnerable to a range of security attacks, like flooding, blackhole, spoofing, and greyhole attacks, due to their limited resources and open communication nature. In such dynamic and resource-constrained environments, conventional techniques frequently fail to maintain accuracy and efficacy, leading to high false alarm rates and delayed detection. This article

employs an effectual approach for WSN attack detection termed Ada-AOOA_DSA. Existing techniques either compromise on detection accuracy or lack the adaptability required to handle diverse and evolving threat landscapes in WSNs. Therefore, a more adaptive and intelligent detection strategy is warranted to address these security limitations.

2.1 Literature Survey

Elsadig, M.A., [1] established a Decision Tree (DT) for detecting attacks in WSN. Here, this approach attained superior classification accuracy with an acceptable overhead. Nonetheless, this technique failed to contemplate suitable oversampling and under sampling methods to establish a balanced version of the WSN-DS database. Sathishkumar, P., *et al*. [2] devised Fuzzy Logic- Long Short-Term Memory (FL-LSTM) for DoS attack detection in WSN. Here, this technique enhanced network performance while reducing network delay and false positive rate. This technique did not test the network in a real-time test bed and did not use intelligent agents to communicate in a distributed environment to enhance performance. Behiry, M.H. and Aly, M., [3] introduced Deep Learning-based Feed-Forward Neural Network-K-Means Clustering with Information Gain (DLFFNN-KMC-IG) for cyber-attack detection in WSN. In this case, this approach attained high accuracy and reliability while efficiently handling the data imbalance issue. Moreover, this method improved the model's ability to generalize and recognize minority classes. However, this approach failed to contemplate the dynamic behavior of evolving attack patterns, which may minimize its efficacy in continuously altering WSN environments. Gebremariam, G.G., *et al.* [4] presented a Multilayer Perceptron Artificial Neural Network (MLPANN) for the detection of multiple attacks in WSN. This scheme offered a minimal localization error and a close approximation of the unknown node location. In addition, this model proved efficient in detecting and safely localizing malicious attacks for WSNs that are hierarchically distributed and scalable. However, this model did not consider several attack classes and techniques for increasing the detection accuracy of the technique. Further, this model did not utilize various public databases as benchmarks for improved performance. While these methods offer promising results, each exhibits limitations such as poor scalability, inadequate feature selection, or a lack of adaptability to real-time and complex network behaviors. Consequently, a unified solution that integrates optimization, adaptive learning, and effective generalization is necessary for dependable WSN security.

2.2 Major Challenges

The major issues faced by the conventional attack detection approaches in WSN are exemplified below.

- In [1], a DT approach was devised for detecting attacks in WSNs. This technique was efficient, reliable, and secure with minimal computational complexity. However, this method struggled with minimizing the complication of managing heterogeneous data sources and improving the robustness of attack detection schemes.
- The FL-LSTM model was developed for DoS attack detection in WSN. Here, this system enhanced the training efficiency with minimal computational parameters. Nevertheless, it did not improve the scalability of the detection model, limiting its ability to process huge volumes of network data effectively.
- An effective model named the DLFFNN-KMC-IG model was established in [3] for cyber-attack detection in WSNs. This approach improved the model's ability to detect attacks and minimized computational cost. Though this method did not assist in highlighting significant features while reducing irrelevant noise, it resulted in better generalization and more precise detection.
- The MLPANN model was developed in [4] for the detection of multiple attacks in WSN. This model improved computational resource utilization by ensuring that only the most significant dataset attributes were employed during training. However, it failed to minimize the probability of further propagation of attacks and ensure data integrity.
- Attack detection in WSNs faces difficulties, including scalability, limited resources, dynamic topology, and the requirement for real-time detection. Consequently, it is essential to establish effective techniques that minimize computational complexity and enhance accuracy.
- Thus, there is a pressing need to develop a detection model that addresses these limitations while ensuring accuracy, low overhead, and adaptability. The proposed Ada-AOOA_DSA is designed specifically to overcome these major obstacles by integrating deep learning with adaptive optimization.

3. System Model

A WSN amalgamated with an IDS to protect against malicious activity is signified in the system model [5]. Several sensors are placed throughout the surroundings to monitor physical parameters, including

pressure, temperature, and motion. A centralized IDS receives data collected from these SNs and continuously investigates and assesses the incoming data for indications of abnormal behavior or probable intrusions. Moreover, a gateway connects the IDS to the Internet, facilitating remote reporting and monitoring. Nonetheless, the presence of potential attackers highlights the risk of external threats established by this connection. As a result, the system assures a comprehensive intrusion-aware WSN technique by ensuring both real-time data collection and robust security monitoring. Fig. 1 represents the system model of IDS.

To address detection challenges, the proposed Ada-AOOA_DSA framework integrates an Adaptive Apiary Organizational Optimization Algorithm (Ada-AOOA) with a Deep Stacked Autoencoder (DSA)-based intrusion detection system. Ada-AOOA enhances optimization performance by combining adaptive parameter control with the biologically inspired behavior of Apiary Organizational Optimization (AOOA). This hybrid strategy improves feature learning by adaptively tuning the weights of the DSA model during training.

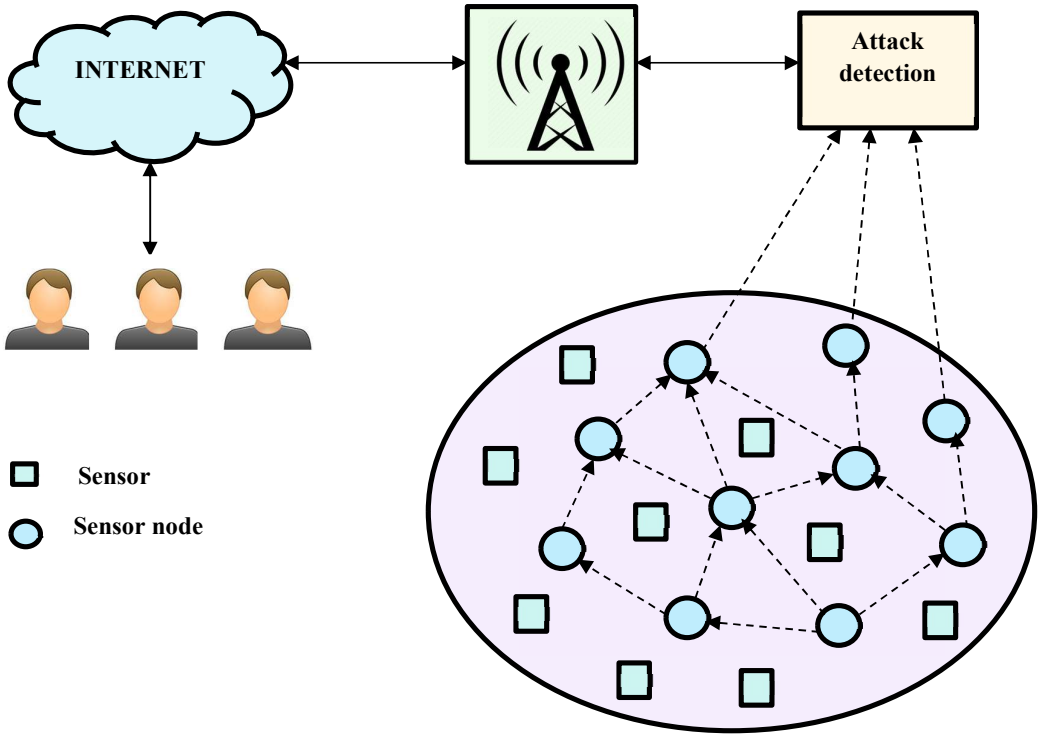


Fig. 1. *System model of intrusion detection*

4. Proposed Adaptive-Apiary Organizational Algorithm Deep Stacked Autoencoder for Attack Detection in WSN

Attack detection in WSNs is vital to safeguard against attacks, including Sybil, blackhole, and DoS attacks, which utilize the network's open communication and limited resources. In this research, an effective method called Ada-AOOA_DSA is established for attack detection in WSN. Here, the WSN is simulated initially to emulate real-world communication and attack scenarios. In the attack detection model, input data is accumulated from the given dataset [9]. Then, the data normalization is performed utilizing median normalization [6] to scale features uniformly and reduce the influence of outliers. Subsequently, features are selected exploiting the correlation coefficient [7]. This feature selection step ensures that only the most relevant and non-redundant input variables are retained, enhancing model interpretability and computational efficiency. Thereafter, the attack is detected employing DSA [8], which is trained using the proposed Ada-AOOA algorithm. The Deep Stacked Autoencoder (DSA) is responsible for unsupervised hierarchical feature learning, while the Long Short-Term Memory (LSTM) classifier integrated at the final layer enables sequential pattern detection, critical in identifying evolving network threats. The Ada-AOOA is a newly devised optimization technique that integrates an adaptive concept with the AOOA [10]. The adaptive component dynamically adjusts algorithmic parameters during training to prevent local minima entrapment and enhance convergence speed. This ensures that the model can generalize well under

varying WSN conditions and attack types. Fig. 2 illustrates the complete workflow from data preprocessing to feature optimization and final classification, emphasizing the interaction between the optimization algorithm and the deep learning architecture.

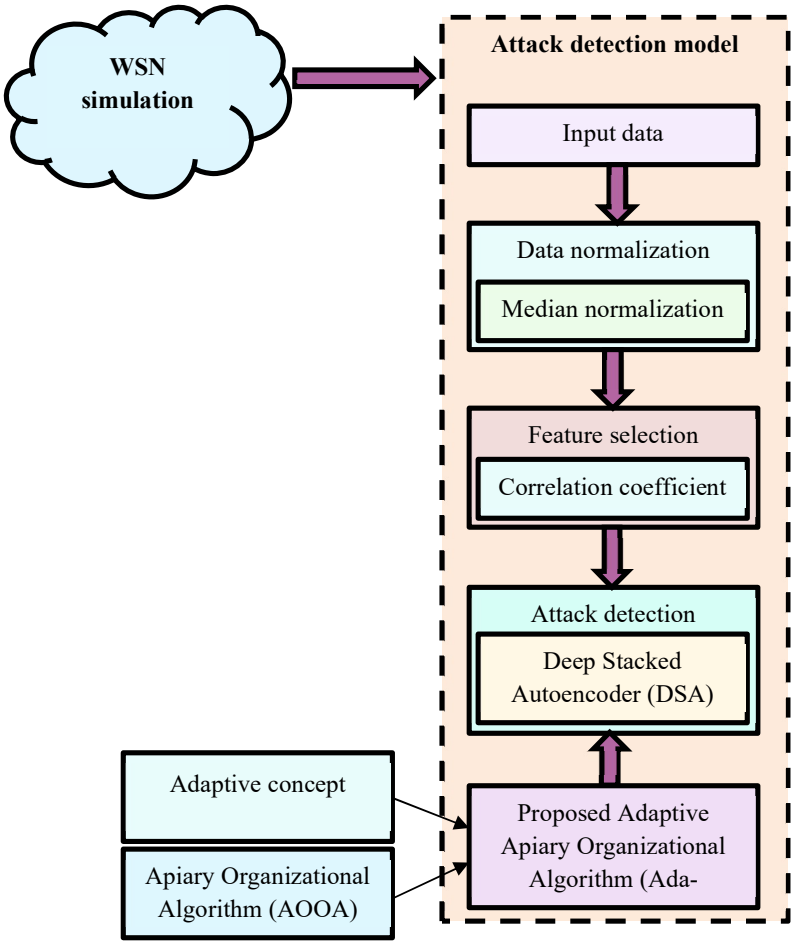


Fig. 2. *Block diagram of proposed Ada-AOOA_DSA for attack detection in WSN*

4.1 Data Acquisition

Originally, the input data is acquired from the WSN-DS dataset [9] for detecting attacks in WSN. Further, the dataset E is stated as follows,

$$E = \{E_1, E_2, ..., E_b, ..., E_k\} \tag{1}$$

wherein k signifies the number of data records available in the dataset, the b^{th} data used to detect attacks is specified as E_b, and the database contemplated to detect attacks is typified as E. This dataset includes labeled instances representing both normal and malicious traffic, making it suitable for training and validating supervised as well as unsupervised learning models.

4.2 Data Normalization

Data normalization is the procedure of eliminating redundant and duplicate data to arrange the input data into a standardized data form for precisely detecting attacks. Moreover, normalization enhances the model's overall capacity for generalization, boosts convergence during optimization, and improves training stability. The median normalization [6] approach is employed in this case to normalize input data E_b into a standardized data format. The normalized dataset u_{norm} is passed to the next phase to ensure uniformity across features with varying scales and units.

4.2.1 Median Normalization

Median normalization [6] is a data preprocessing approach where the median of the database is exploited to normalize values. This technique enhances the performance and stability of ML algorithms by centering attributes in a way that supports faster convergence and better generalization. The median of all the values of a feature is exploited in this approach to normalize every input value. By employing the subsequent equation, the normalized value u_{norm} of value u of the feature δ can be measured.

$$u_{norm} = \frac{u}{median(\delta)} \tag{2}$$

Here, the normalized outcome is designated as u_{norm}. The normalization ensures that extreme values or skewed distributions do not dominate the learning process, especially in sensitive attack detection tasks.

4.3 Feature Selection

Finding and selecting the most significant features to use in model training from a database is called feature selection. Feature selection enhances model performance by minimizing dimensionality and eliminating redundant or unnecessary data. The correlation coefficient [7] is employed in this research to effectively select the features. The normalized value u_{norm} is considered an input here.

4.3.1 Correlation Coefficient

A statistical metric that calculates the direction and strength of a linear relationship among two variables is called the correlation coefficient [7], and it normally ranges from -1 to +1. A strong negative correlation is signified by a value near -1, a strong positive correlation by a value near +1, and no linear relationship is specified by a value near 0. It is often utilized to find and eradicate redundant features in data analysis. When utilizing the correlation coefficient for feature selection, features are selected based on their statistical relationship with the target variable; specifically, attributes with high absolute correlation values are regarded as informative. In addition, to minimize redundancy and multicollinearity, one feature from any pair of highly correlated features is generally eliminated. The Pearson correlation coefficient $w_{B\varepsilon}$ signifies the strength and direction of the linear relationship between two variables. Moreover, the expression for the Pearson correlation coefficient is specified beneath:

$$w_{B\varepsilon} = \frac{\sum\left(B-\overline{B}\right)\left(\varepsilon-\overline{\varepsilon}\right)}{\left(\sum_1^{\alpha}\left(B_g-\overline{B}\right)^2\right)\left(\sum_1^{\alpha}\left(\varepsilon_g-\overline{\varepsilon}\right)^2\right)} \tag{3}$$

wherein B_g denotes the g^{th} data point of variable B', ε_g signifies g^{th} the data point of variable ε', the mean of the overall values of variable B' is typified by $\overline{B}$, and the mean of the overall values of variable ε' is typified by $\overline{\varepsilon}$. The outcome attained from the feature selection is designated as χ_d. This process yields the feature-selected output set, which is passed as input to the detection model.

4.4 Attack Detection

WSNs are susceptible to many security risks, such as sinkhole attacks, node compromise, and data tampering, which are often brought on by open communication channels and limited resources. For this reason, attack detection is vital. Effective detection methods are required to ensure the network's availability, confidentiality, and integrity. Adaptive monitoring and rapid detection of malicious activity are made possible by the use of a DSA [8] model for attack detection in this work. Further, the DSA model is trained using the proposed Ada-AOOA, which is developed by the assimilation of the Adaptive concept and AOOA [10]. Here, the feature selection output χ_d is fed as input to the DSA technique. The integration of DSA with Ada-AOOA ensures both deep feature learning and optimal model tuning, contributing to a more accurate and resilient detection system.

4.4.1 Architecture of DSA

The DSA technique [8] is a type of Deep Neural Network (DNN) that consists of numerous autoencoder layers, each of which is tuned to exploit the outcome of the preceding one. The autoencoders indicate the relationship between independent and dependent attributes and efficiently minimize the size of the data. The DSA is contemplated as an unsupervised learning approach, and it generally exploits a backpropagation technique to acquire the outcome value. Autoencoders are generally categorized into two primary types, decoders and encoders. Here, the encoder is exploited to minimize the size of the data by carrying out the encoding procedure, and the decoder reconstructs the actual data from the minimized

representation by the decoding procedure. As a result, anomalies from the data with high reconstruction error are precisely detected employing the DSA.

The DSA encoder is composed of a mapping function, input, and hidden layer; the hidden layer's outcome is specified beneath.

$$h(\chi_d) = f(\mu\chi_d + I) \tag{4}$$

Here, the encoding weight matrix is signified by μ, the activation function is specified by $f(.)$, and the input and bias are typified by χ_d and I.

At the same time, the decoder exhibits the outcome, mapping function, and hidden layer. The decoder employs a mapping function to transform the hidden layer output into the input layer. Hence, the outcome that is generated as a result of the mapping function and the reconstructed data is specified below,

$$\hat{\chi}_d(F) = \hbar\left(\mu^* F + I^*\right) \tag{5}$$

Here, reconstructed input data is typified by $\hat{\chi}_d$, and $\hbar(.)$ indicates decoder activation function, I^* indicates decoded bias vector, and decoded weight matrix represented as μ^*. In addition, the autoencoder's reconstruction effect is validated by exploiting Mean Square Error (MSE), which is represented below,

$$MSE = \frac{1}{2}\left\|\chi_d - \hat{\chi}_d\right\|^2 \tag{6}$$

High reconstruction errors are indicative of data anomalies, which correlate with potential intrusions. The DSA model is tuned in two phases, like unsupervised layer-by-layer pre-training and supervised reverse fine-tuning. The stages assist in enhancing the model's learning accuracy and rate. Over-training problems occur because the DSA model takes longer to learn the data attributes from specific training samples. As a result, DSA includes the weight decay coefficient and performs dropout during training.

Dropout operations generate a sub-network of the original network by randomly discarding neurons in the hidden layer with the possibility of m_η. The discarded matrix $\varsigma = [\varsigma_1, \varsigma_2, \varsigma_3, ..., \varsigma_\varpi]$ checks with a Bernoulli distribution. Consequently, the resultant function acquired during the probability distribution is represented below,

$$\beta(\kappa, m_\eta) = \begin{cases} m_\eta, & \kappa = 1 \\ 1 - m_\eta, & \kappa = 0 \end{cases} \tag{7}$$

wherein the probable outcome is typified by κ. At the initial neural network, the mapping function is updated, and the dropout operation is later carried out in hidden layers, which is articulated as follows,

$$\varsigma_\gamma(\chi_d) = \varsigma_\gamma f\left(\sum_{N=1}^{H} \mu\chi_d + I\right) \tag{8}$$

$$\varsigma_\gamma(\chi_d) = \begin{cases} f\left(\sum_{N=1}^{H} \mu\chi_d + I\right), & \varsigma_\gamma = 1 \\ 0, & \varsigma_\gamma = 0 \end{cases} \tag{9}$$

Here, ς_γ indicates discarded matrix; overall components are signified as γ. The structure of the DSA framework is portrayed in Fig. 3, and the acquired outcome J_x is attained while subjecting the feature-selected output χ_d to of DSA technique. The final predicted outcome $\hat{y}$ is compared with ground truth labels for performance evaluation in later stages.

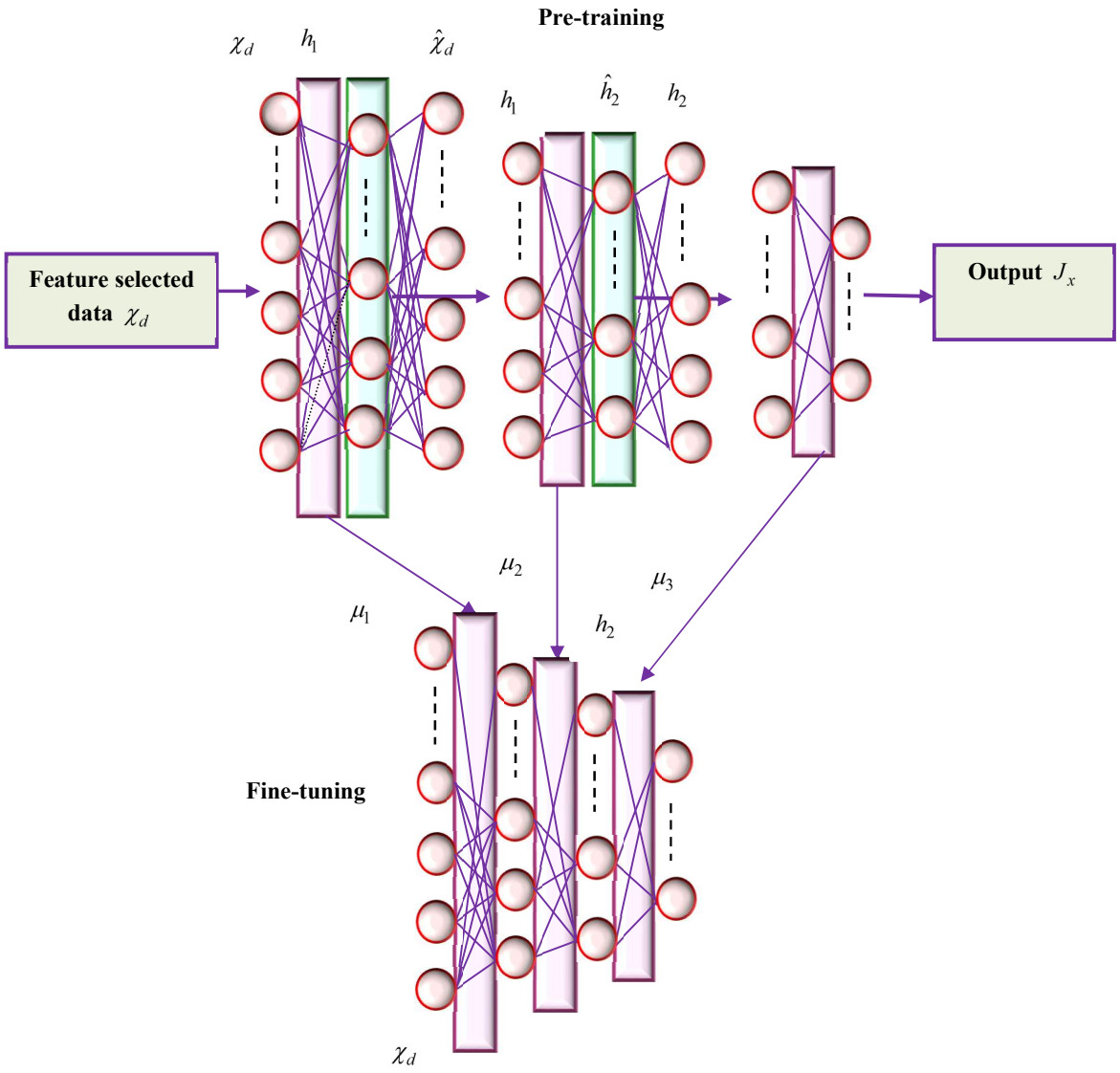


Fig. 3. *Structure of the DSA model*

4.4.2 Training of DSA utilizing the proposed Adaptive-Apiary Organizational Optimization Algorithm

The supremacy of DSA is enhanced by changing its hyperparameters, optimally by employing the Ada-AOOA method. In this case, Ada-AOOA is established by assimilating the Adaptive concept and AOOA [10]. A novel metaheuristic optimization algorithm called AOOA is inspired by the organizational behavior of honeybees within an apiary. The algorithm finds the most effective solutions to optimization issues by simulating how honeybees cooperate and coordinate within their hive, performing activities, including communication, foraging, and decision-making. Bees in an apiary demonstrate a clear hierarchy and division of labor. While scout bees investigate potential new foraging positions, worker bees are responsible for gathering nectar. Bees employ the "waggle dance" to exchange information about the finest places to find nectar. In complex optimization issues, AOOA can avoid local minima and find more optimal solutions by effectually balancing exploration and exploitation. Furthermore, the AOOA minimized the effort needed for parameter training and setting. The term "adaptive" also defines a system's or algorithm's capacity to dynamically modify its structure, parameters, or behavior in response to modifications in the data, environment, or internal performance. To enhance performance and robustness, this concept is often applied in control and optimization systems. By including the adaptive concept in AOOA, it significantly enhances the efficiency, flexibility, and robustness of the algorithm, making it suitable for dynamic and real-world environments. The algorithmic phases of Ada-AOOA are elaborated below,

Step i) Initial population

This stage simulates the queen's role by mathematically initializing the bee colony and signifying hive members. Every apiary contains an arbitrarily produced population of individuals that is represented by L, where the number of hives is specified by G, and every hive encompasses T bees. The simplest hive configuration contains ten bees, like one queen, one drone, and eight worker bees. Expression (10) designates the relationship among L, G and T.

$$L = G \times T \tag{10}$$

wherein, $1 \le G \le S$, $S \in Z^{+}$ and $10 \le T \le 100$.

Step ii) Fitness function

The fitness equation is exploited to determine the optimum honeybee's position utilizing MSE, which is computed as follows,

$$D_{fitness} = \frac{1}{Q}\sum_{x=1}^{Q}\left(J_x^{*} - J_x\right)^2 \tag{11}$$

In the above expression, the overall training sample count is designated by Q, the targeted outcome of DSA is signified by J_x^{*}, and the obtained outcome of DSA is specified by J_x.

Step iii) Drones exchange

In this phase, drone behavior is simulated by arbitrarily selecting two hives, y and T then selecting drones R_1 R_2 from every hive, followed by conducting a swap operation among them.

Step iv) Queen fertilization and bees breeding

This stage simulates queen fertilization, where every hive's queen is fertilized by top-performing drones to generate ζ new bees. If the feature difference is within half the drone's features, offspring inherit mostly from the queen; otherwise, features are split evenly. The fertilization procedure is specified in Equation (12).

$$K_c\left(W+1\right) = q_c\left(W\right) + \vartheta \cdot \left(n_c\left(W\right) - q_c\left(W\right)\right),\ if\left(\frac{n_c\left(W\right) - q_c\left(W\right)}{q_c\left(W\right)}\right) < 0.5 \tag{12}$$

Here, iteration is indicated as W the position of the new bee at $\left(W+1\right)^{th}$ iteration is signified as $K_c\left(W+1\right)$, ϑ is regarded as an adaptive parameter, the drone of the c^{th} hive is represented by n_c, and the queen of the c^{th} hive is represented by q_c. The expression of the adaptive parameter ϑ is computed as below,

$$\vartheta = \vartheta_{\min} + \left(\vartheta_{\max} - \vartheta_{\min}\right) \times \left(1 - e^{-vW}\right) \tag{13}$$

wherein, the minimum value is signified by $\vartheta_{\min}$, the decay constant is represented by v, maximum value is typified as $\vartheta_{\max}$.

Step v) Worker lifecycle

This stage models worker behavior, where every worker's age determines the possibility of replacing an existing bee. The worker's lifecycle, ranging from 1 to 60 days, is mathematically designated by its age. Equation (14) designates that in every period, a certain number of translocations are carried out on the selected worker to form a new bee.

$$NW_c = A_c + \vartheta \cdot \left(\frac{A_c^{\max\_P} - A_c^{P}}{A_c^{\max\_P}}\right) \times A_c \tag{14}$$

Here, the new worker of the c^{th} hive is denoted as NW_c, A_c designates the worker of the c^{th} hive, the maximal age of the worker is indicated by $A^{\max\_P}$.

Step vi) Queen Investiture

This stage simulates queen replacement; if a new bee's fitness exceeds the fitness of the queen by a threshold ϕ, it becomes the new queen, replacing the old one. Moreover, the fitness is then computed employing equation (11).

Step vii) Fading out.

This stage simulates drone fading behavior by introducing a control parameter Y, which regulates the number of bees that are eradicated.

Step viii) Swarming

This stage simulates the queen's swarming behavior, where hive separation is controlled by a user-defined control parameter U_{ratio} according to the specific problem.

Step ix) Termination

The Ada-AOOA model employs the newly acquired values to proceed to the next iteration after the position has been updated. In addition, the iterative process is performed repeatedly until the best possible solution is found.

5. Results and Discussion

This section validates the efficacy of Ada-AOOA_DSA in detecting attacks in WSN by contrasting its outcomes with those of classical detection schemes. In addition, the discussions concerning the outcomes are presented below,

5.1 Experimental Setup

The Ada-AOOA_DSA introduced to detect attacks is implemented by exploiting Python 3.9.11 with the WSN-DS dataset [9].

5.2 Dataset Description

WSN-DS [9] is a benchmark dataset created specifically for evaluating attack detection in WSNs. This database contains labeled data that signifies both malicious and normal activities within a simulated WSN environment. The WSN-DS database involves 374661 records, each signifying a network instance labeled as either normal or one of four kinds of DoS attacks. Moreover, the database involves numerous kinds of attacks, like scheduling attacks, flooding, greyholes, and blackholes, making it suitable for testing both signature and anomaly-based IDS techniques. WSN-DS is devised to facilitate the development of effective and precise detection algorithms by offering a structured format that reflects realistic and diverse network behaviors.

5.3 Evaluation Measures

The effectualness of the Ada-AOOA_DSA model is evaluated through the utilization of evaluation measures, namely TPR, TNR, and accuracy, as elaborated below.

a) Accuracy: Accuracy is a measure employed to assess the ratio of correctly detected instances over the overall amount of evaluated instances and is measured as follows;

$$Accuracy = \frac{j^{tp} + j^{tn}}{j^{tp} + j^{tn} + j^{fp} + j^{fn}} \tag{15}$$

wherein, the number of attack instances precisely identified as attacks is signified as j^{tp} the number of normal instances accurately identified as normal, is specified by j^{tn} the amount of normal instances incorrectly detected as attacks are represented as j^{fp}, and the count of attack instances incorrectly detected as j^{fn}.

b) TPR: TPR measures the proportion of actual positive instances that are precisely detected by the Ada-AOOA_DSA, evaluating its sensitivity to malicious activities, and is measured as,

$$TPR = \frac{j^{tp}}{j^{tp} + j^{fn}} \tag{16}$$

c) TNR: TNR quantifies the ratio of actual negative instances that are accurately identified as such, reflecting the system's ability to avoid false alarms. The TNR formula is specified beneath,

$$TNR = \frac{j^{tn}}{j^{tn} + j^{fp}} \tag{17}$$

5.4 Comparative Methods

The efficiency of the established Ada-AOOA_DSA model for attack detection is investigated by correlating it with numerous traditional approaches, namely DT [1], FL-LSTM [2], DLFFNN-KMC-IG [3], and MLPANN [4].

5.5 Comparative Analysis

The experiments were conducted by changing the K Value and learning set to examine the supremacy of Ada-AOOA_DSA, and the details of the experimental examination are outlined beneath.

5.5.1 Analysis Based on Learning Set

The examination of Ada-AOOA_DSA for attack detection by changing the percentage of the learning set is depicted in Fig. 4. In Fig. 4a), the assessment of Ada-AOOA_DSA with existing methods employing accuracy is designated. In this case, the Ada-AOOA_DSA surpasses traditional approaches with an accuracy of 92.765% for a 90% learning set, and the accuracy computed by conventional schemes, like DT is 86.987%, FL-LSTM is 87.909%, DLFFNN-KMC-IG is 89.879%, and MLPANN is 90.876%. The experimental outcomes demonstrated that the Ada-AOOA_DSA gained a maximal performance of 5.778% concerning accuracy than the traditional DT technique. Fig. 4b) signifies the evaluation of Ada-AOOA_DSA through TPR. By assuming a learning set of 90%, the Ada-AOOA_DSA acquired a TPR of 94.868%, while the classical methods, including DT, FL-LSTM, DLFFNN-KMC-IG, and MLPANN, obtained a TPR of 89.876%, 90.766%, 91.766%, and 92.644%. The Ada-AOOA_DSA achieved a maximal performance of 4.102%, than the FL-LSTM detection model contemplated for comparison. Additionally, the investigation of Ada-AOOA_DSA concerning TNR is illustrated in Fig. 4c). The TNR of 91.876% is quantified for the learning set of 90% by Ada-AOOA_DSA, while the prevailing approaches acquired a TNR of 86.868% by DT, 87.757% by FL-LSTM, 88.766% by DLFFNN-KMC-IG, and 89.566% by MLPANN. The experimental consequences show that Ada-AOOA_DSA gained a superior performance by 3.11% over DLFFNN-KMC-IG.

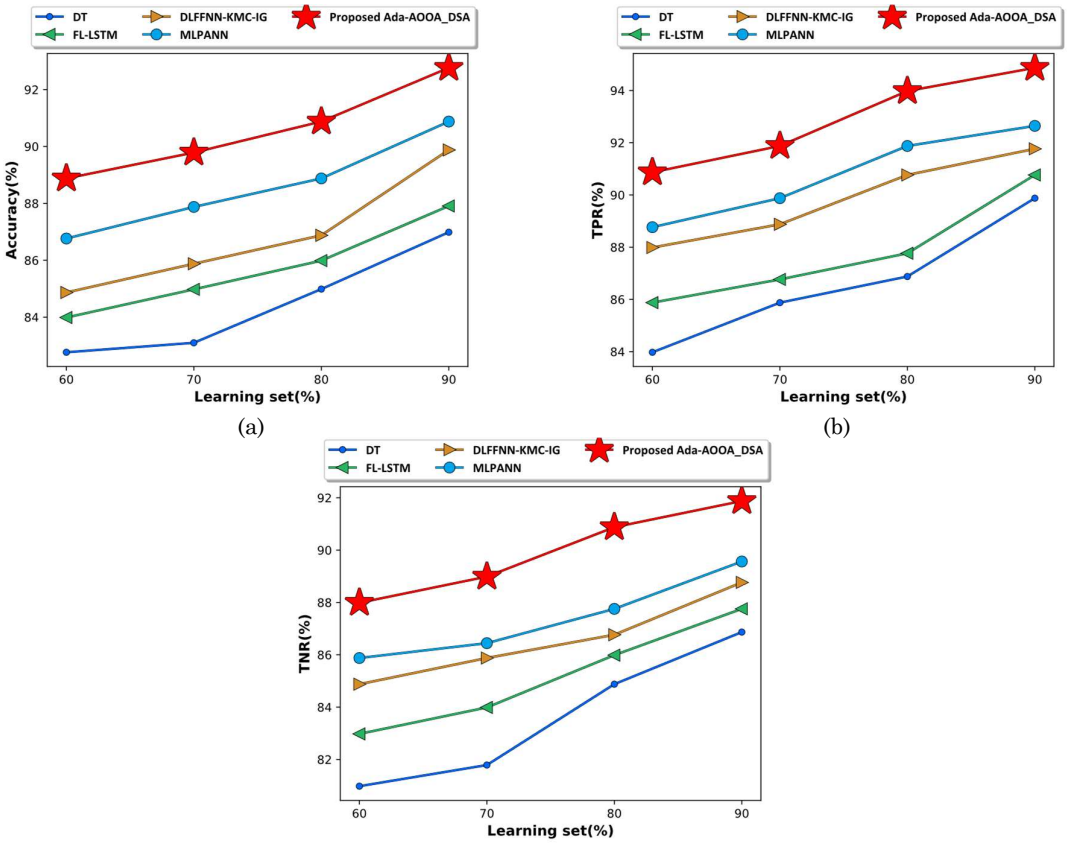


Fig. 4. *Valuation of Ada-AOOA_DSA employing a) Accuracy, b) TPR, and c) TNR regarding the learning set*

5.5.2 Analysis Based on K Value

Fig. 5 displays the quantitative examination of the devised Ada-AOOA_DSA model, performed by varying the K Value. The comparative investigation of Ada-AOOA_DSA exploited for detecting attacks regarding accuracy is represented in Fig. 5a). The Ada-AOOA_DSA acquired an accuracy of 93.876%, and the classical approaches quantified an accuracy of 87.978% by DT, 88.766% by FL-LSTM, 89.877% by DLFFNN-KMC-IG, and 91.655% by MLPANN for a K Value of 8. The experimental results proved that the Ada-AOOA_DSA recorded an improved performance of 5.889% than DT. The TPR recorded by several detection schemes with varying K-Value is designated in Fig. 5b). The Ada-AOOA_DSA gained a maximal TPR of 95.866% for a K Value of 8, than the TPR quantified by conventional techniques, such as DT at 89.868%, FL-LSTM at 90.899%, DLFFNN-KMC-IG at 91.977%, and MLPANN at 95.866%. The experimental results highlight the remarkable performance of the Ada-AOOA_DSA method, which

attained a TPR 4.967% higher than that of the baseline FL-LSTM technique. Further, the evaluation of Ada-AOOA_DSA concerning TNR is exhibited in Fig. 5c). The Ada-AOOA_DSA gained a TNR of 92.654%, while classical techniques, including DT, FL-LSTM, DLFFNN-KMC-IG, and MLPANN, measured a TNR of 86.977%, 87.877%, 88.766%, and 90.868% for K Value of 8. The devised Ada-AOOA_DSA approach recorded superior performance, exhibiting a 1.786% enhancement over the traditional MLPANN model.

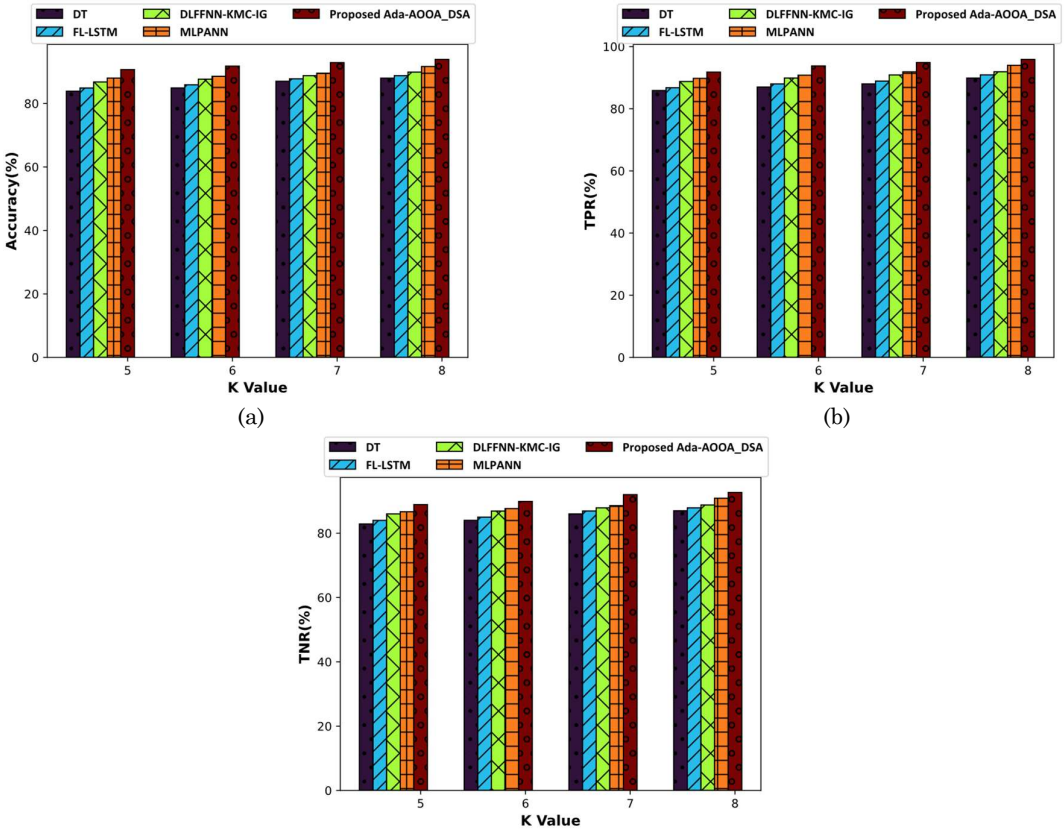


Fig. 5. *Valuation of Ada-AOOA_DSA utilizing a) Accuracy, b) TPR, and c) TNR concerning K value*

5.6 Comparative Discussion

The efficacy of Ada-AOOA_DSA in attack detection is examined through comparative assessment with classical approaches, and the outcomes for both Ada-AOOA_DSA and the traditional models are presented in Table 1. The examination is carried out by considering the learning set of 90%, and the K Value of 8 under numerous performance metrics. The Ada-AOOA_DSA technique developed for attack detection showed a high effectiveness in detecting attacks with a TPR of 95.866%, an accuracy of 93.876%, and a TNR of 92.654% by contemplating K Value as 8. Conversely, the baseline techniques recorded an accuracy of 87.878% by DT, 88.766% by FL-LSTM, 89.877% by DLFFNN-KMC-IG, and 91.655% by MLPANN. Moreover, the classical models, such as DT, FL-LSTM, DLFFNN-KMC-IG, and MLPANN, quantified TPR of 89.868%, 90.899%, 91.898%, and 93.977% and TNR of 86.977%, 87.877%, 88.766%, and 90.868%. Furthermore, DSA minimizes overfitting and has high generalizability, which is crucial for modern security systems facing constantly evolving threats. In addition, the adaptive concept assures enhanced generalization and faster convergence during training, while AOOA balances the exploration and exploitation effectively, thereby preventing local minima and enhancing the convergence of the training procedure. By combining the adaptive concept and AOOA, the model's ability to precisely detect attacks across diverse and evolving data environments is significantly improved.

Table 1. *Comparative discussion of Ada-AOOA_DSA*

Based on	Metrics	Methods				
		DT	FL-LSTM	DLFFNN-KMC-IG	MLPANN	Proposed Ada-AOOA_DSA
Learning set as 90%	Accuracy (%)	86.987	87.909	89.879	90.876	92.765
	TPR (%)	89.876	90.766	91.766	92.644	94.868
	TNR (%)	86.868	87.757	88.766	89.566	91.876
K Value as 8	Accuracy (%)	87.978	88.766	89.877	91.655	**93.876**
	TPR (%)	89.868	90.899	91.898	93.977	**95.866**
	TNR (%)	86.977	87.877	88.766	90.868	**92.654**

6. Conclusion

WSNs are highly vulnerable to numerous cyberattacks due to their resource constraints and open communication nature. Designing an effective attack detection system is crucial to ensure security and reliable network operation. This work proposes a detection technique named Ada-AOOA_DSA in this research for attack detection in WSN. Originally, the WSN is simulated, and the attack detection process is performed. In this process, the input data is gained from the specified database, and it is forwarded to data normalization. In this case, the data is normalized utilizing median normalization. After this, the features are selected employing the correlation coefficient. In addition, Ada-AOOA_DSA is exploited for attack detection, where the DSA is tuned by the proposed Ada-AOOA. Furthermore, the proposed Ada-AOOA is the combination of the Adaptive concept and AOOA. Moreover, the proposed Ada-AOOA_DSA is scrutinized because of multiple parameters, such as accuracy, TPR, and TNR, and the values acquired are 93.876%, 95.866%, and 92.654%. The results demonstrate that the Ada-AOOA_DSA method outperforms several traditional models in terms of both detection accuracy and efficiency. This performance is attributed to the integration of the adaptive mechanism with the AOOA, which allows the model to dynamically adjust to the evolving nature of the attack patterns in WSNs. Future work aims to contemplate developing hybrid DL networks to boost the performance of the proposed method. Moreover, future work will concentrate on designing lightweight and energy-efficient detection models appropriate for resource-constrained nodes. In addition, further research will explore optimizing the model to enhance real-time attack detection, which is critical in dynamic WSN environments.

Compliance With Ethical Standards

Conflicts of interest: Authors declared that they have no conflict of interest.

Human participants: The conducted research follows ethical standards and the authors ensured that they have not conducted any studies with human participants or animals.

References

[1] Elsadig, M.A., "Detection of denial-of-service attack in wireless sensor networks: A lightweight machine learning approach", IEEE Access, vol. 11, pp.83537-83552, 2023.

[2] Behiry, M.H. and Aly, M., "Cyberattack detection in wireless sensor networks using a hybrid feature reduction technique with AI and machine learning methods", Journal of Big Data, vol. 11, no. 1, pp.16, 2024.

[3] Sathishkumar, P., Gnanabaskaran, A., Saradha, M. and Gopinath, R., "DoS attack detection using fuzzy temporal deep long Short-Term memory algorithm in wireless sensor network", Ain Shams Engineering Journal, vol. 15, no. 12, pp.103052, 2024.

[4] Gebremariam, G.G., Panda, J. and Indu, S., "Localization and detection of multiple attacks in wireless sensor networks using artificial neural network", Wireless Communications and Mobile Computing, vol. 1, pp.2744706, 2023.

[5] Nguyen, T.M., Vo, H.H.P. and Yoo, M., "Enhancing intrusion detection in wireless sensor networks using a GSWO-CatBoost approach", Sensors, vol. 24, no. 11, pp.3339, 2024.

[6] Bhanja, S. and Das, A., "Impact of data normalization on deep neural network for time series forecasting", arXiv preprint arXiv:1812.05519, 2018.

[7] Chen, P., Li, F. and Wu, C., "Research on intrusion detection method based on Pearson correlation coefficient feature selection algorithm", In Journal of Physics: Conference Series, vol. 1757, no. 1, pp. 012054, IOP Publishing, 2021.

[8] Yu, Y., Li, J., Li, J., Xia, Y., Ding, Z. and Samali, B., "Automated damage diagnosis of concrete jack arch beam using optimized deep stacked autoencoders and multi-sensor fusion", Developments in the Built Environment, vol. 14, pp.100128, 2023.

[9] The WSN-DS dataset is acquired from "https://www.kaggle.com/datasets/bassamkasasbeh1/wsnds", accessed on May 2025.
[10] Al-Sharqi, M.A., Al-Obaidi, A.T.S. and Al-mamory, S.O., "Apiary Organizational-Based Optimization Algorithm: A New Nature-Inspired Metaheuristic Algorithm", International Journal of Intelligent Engineering & Systems, vol. 17, no. 3, 2024.
[11] Diro, A.A. and Chilamkurti, N., "Distributed attack detection scheme using deep learning approach for Internet of Things", Future Generation Computer Systems, vol. 82, pp.761-768, 2018.
[12] Gebremariam, G.G., Panda, J. and Indu, S., "Blockchain-Based Secure Localization against Malicious Nodes in IoT-Based Wireless Sensor Networks Using Federated Learning", Wireless Communications and mobile computing, vol. 1, pp.8068038, 2023.
[13] Jayarajan, P., Kanagachidambaresan, G.R., Sundararajan, T.V.P., Sakthipandi, K., Maheswar, R. and Karthikeyan, A., "An energy-aware buffer management (EABM) routing protocol for WSN", The Journal of Supercomputing, vol. 76, no. 6, pp.4543-4555, 2020.
[14] Javaid, A., Niyaz, Q., Sun, W. and Alam, M., "A deep learning approach for network intrusion detection system", In Proceedings of the 9th EAI International Conference on Bio-inspired Information and Communications Technologies, formerly BIONETICS, pp. 21-26, May 2016.
[15] Kang, M.J. and Kang, J.W., "Intrusion detection system using deep neural network for in-vehicle network security", PloS one, vol. 11, no. 6, pp.e0155781, 2016.
[16] Li, Y., Ma, R. and Jiao, R., "A hybrid malicious code detection method based on deep learning", International Journal of Security and its Applications, vol. 9, no. 5, pp.205-216, 2015.