REPUBLIC OF TÜRKİYE
ALTINBAŞ UNIVERSITY
Institute of Graduate Studies
Electrical And Computer Engineering

DESIGN OF ADVANCED ANOMALY DETECTION SYSTEM BASED ON HYBRID MACHINE LEARNING TECHNIQUE WITH OPTIMIZED FEATURE SELECTION IN WIRELESS SENSOR NETWORK

Taha Fakhri Abd-Alhamza ALMSHHED

Master's Thesis

Supervisor

Assoc. Prof. Dr. Sefer KURNAZ

İstanbul, 2025

DESIGN OF ADVANCED ANOMALY DETECTION SYSTEM BASED ON HYBRID MACHINE LEARNING TECHNIQUE WITH OPTIMIZED FEATURE SELECTION IN WIRELESS SENSOR NETWORK

Taha Fakhri Abd-Alhamza ALMSHHED

Electrical and Computer Engineering

Master's Thesis

ALTINBAŞ UNIVERSITY

2025

The thesis titled DESIGN OF ADVANCED ANOMALY DETECTION SYSTEM BASED ON HYBRID MACHINE LEARNING TECHNIQUE WITH OPTIMIZED FEATURE SELECTION IN WIRELESS SENSOR NETWORK Prepared by TAHA FAKHRI ABD-ALHAMZA ALMSHHED and submitted on 30/01/2025 has been **accepted unanimously** for the degree of Master of Science in Information Technology.

_____

Assoc. Prof. Dr. Sefer KURNAZ

Supervisor

Thesis Defense Committee Members:

Assoc. Prof. Dr. Sefer KURNAZ	Department of Computer Engineering, Altınbaş University	_____
Asst. Prof. Dr. Abdullahi Abdu IBRAHIM	Department of Computer Engineering, Altınbaş University	_____
Asst. Prof. Dr. Serdar KARGIN	Department of Biomedical Engineering, İstanbul Arel University	_____

I hereby declare that this thesis meets all format and submission requirements of a master's Thesis.

I hereby declare that all information/data presented in this graduation project has been obtained in full accordance with academic rules and ethical conduct. I also declare all unoriginal materials and conclusions have been cited in the text and all references mentioned in the Reference List have been cited in the text, and vice versa as required by the abovementioned rules and conduct.

Taha Fakhri Abd-Alhamza ALMSHHED

Signature

DEDICATION

First of all, I would like to thank ALLAH for His many blessings. Praise be to ALLAH the Almighty who has given me the strength of mind, good health, strength, guiding knowledge and skills to complete this study. With gratitude and love, I dedicate this thesis to my dear father. His constant love, wisdom and unwavering support have shaped me into the person I am today. To my beloved mother, your strength and love have always been a source of comfort. To my supportive brothers and my martyred brother (Sadeq), may ALLAH have mercy on him, thank you for standing by me. To my dear children, you are my inspiration to reach new heights. And to my wonderful wife, her patience, understanding and encouragement have been my strength throughout this journey. This work is a testament to the love, sacrifice and support of my family. Thank you for being my constant source of motivation and making this journey meaningful. I dedicate this achievement to Asst. Prof. Dr. Hameed Mutlag Farhan and conclude my words to each and every one of you, my love and gratitude.

ABSTRACT

DESIGN OF ADVANCED ANOMALY DETECTION SYSTEM BASED ON HYBRID MACHINE LEARNING TECHNIQUE WITH OPTIMIZED FEATURE SELECTION IN WIRELESS SENSOR NETWORK

ALMSHHED, Taha Fakhri Abd-Alhamza

M.Sc., Electrical and Computer Engineering, Altınbaş University,

Supervisor: Assoc. Prof. Dr. Sefer KURNAZ

Date: 01/2025

Pages: 77

At present, the Wireless Sensor Network (WSN) plays a pivotal role in the wireless communication system that works based on a large number of sensor nodes. The development of the WSN has become more popular and the nature of versatility resulted in more security concerns and making it hard for the investigation to prevent the anomaly in it. One of the essential and challenging tasks in WSN is the security concern. Detecting the anomaly present in the network becomes the major challenge to ensure the security of WSN. In general, WSNs are affected by a different type of threats that tends the nodes to get damaged and form the wrong determination. Therefore, it is necessary to identify anomalous to minimize the false alarm. Moreover, the quality of the data gathered by the sensor nodes is mainly affected by the anomalies that are produced because of different reasons like reading errors, malicious attacks, failures, and unusual events. Hence it is significant to process the anomaly detection to ensure the quality of the sensor data before it is used to make decisions. In WSN, anomaly detection is the significant process to determine the anomaly or unusual event. However, timely anomaly identification is more complex to function to execute reliably in real-time. For the secure and reliable operation in the WSN, effective anomaly detection is more necessary. However, the standard anomaly detection techniques often fail to adequately secure the privacy of the data and identify the complex, particular, and unique breaches in the WSN. Also, the present anomaly detection models only process under the stationary environment and need to keep all the training data in the node. To address these limitations, a novel Hybrid Machine Learning Technique (HMLT) is

introduced to effectively detect the presence of anomalies in WSN. The advanced hybrid technique is designed to enhance the detection performance and safeguard privacy. Initially, the required data from the WSN is collected from the available data resource. Further, the significant feature from the raw data is selected using the optimal feature selection process. Here the Secretary Bird Optimization Algorithm (SBOA) is used to achieve the optimal feature selection. Finally, the HMLT is implemented to perform the detection task, in which the hybrid classifier is the combination of the Deep Belief Network (DBN) along with the Bayesian Learning (BL). The model is specifically developed to identify the occurrence of anomalies in WSN using the HMLT for a given dataset. Extensive comparative analysis is performed to analyze the detection capability of the designed approach along with the conventional model. The resulting outcome defines that the proposed approach performs greater in detecting the anomaly than other standard models.

Keywords: Anomaly Detection, WSN, Machine Learning, SBOA, Deep Belief Network.

TABLE OF CONTENTS

Pages

LIST OF TABLES

Pages

LIST OF FIGURES

Pages

ABBREVIATIONS

BL	:	Bayesian Learning
BL	:	Bayesian Learning
DBN	:	Deep Belief Network
DBN	:	Deep Belief Network
HMLT	:	Hybrid Machine Learning Technique
LSTM	:	Long Short-Term Memory
ML	:	Machine Learning
RNN	:	Recurrent Neural Networks
SBOA	:	Secretary Bird Optimization Algorithm
SVM	:	Support Vector Machine
WSN	:	Wireless Sensor Network

1. INTRODUCTION

In the present decades, WSNs evolved quickly and become more popular in the research field of network applications. In general, the WSN can easily deployed and it requires minimum cost to enable the network. Therefore, this network is used in multiple sectors, which is based on the smart sensor devices in our day-to-day lives. Some of the applications like smart homes, vehicle communication, and remote monitoring [9]. There are a greater number of independent sensor nodes composed to form the WSN, which is investigated through different research to gather significant information and collectively transfer the information to the base station with the help of corresponding sink nodes. WSN works based on the data collection and transmits the gathered data to the sink nodes [10]. For all the collected data, the station is the responsible spot, which helps the network to transmit the information and make further analysis. There is a huge number of sensor nodes deployed in the WSN network to gather different kinds of information like humidity, pressure, light variation in multiple environments, sound, and temperature. Some of the applications of WSN are biodiversity mapping, environmental monitoring, earthquake, intensive care unit, mechanical stress recognition, patient monitoring, and observing wildlife. In general, sensor nodes are deployed in unattended areas, therefore analyzing each sensor node is not possible [11]. Further, data security is important to reflect the accurate and true world state of WSN applications. However, the raw measures gathered by the sensor nodes, mainly from the large-scale WSN generally have a complexity like incompleteness and inaccuracy. This improper sensor measurement is formed because of the sensing environment or sensor device itself. The sensor device resource constraints regarding the energy, bandwidth, storage, and processing may cause failure in the node and hence report the anomaly reading [12]. Other reasons that correspond to the environment include the difficulties and harshness of the deployment area that resulted in the undefined data. Additionally, malicious attacks like sinkholes, selective forwarding, wormhole attacks, black hole attacks, and denial of service also offer to produce such low-quality and inaccurate data. Other than the physical interruptions like the sensor device movement or the destructions by the animals or humans may affect the information gathering process and tend to anomalous measurements.

Environmental information collected and delivered by the WSN in real-time and the efficient feature tends the people to live easily [13]. But at the same time, it also has the challenges of less processing, security, capability, and data trustworthiness. These complexities tend to

corrupt or hack at any time. Once the network has been attacked, there is a huge amount of loss presented. Therefore, the detection of such anomalies in WSN becomes significantly necessary [14]. Incomplete or inaccurate data measurement generally causes anomalies. An anomaly is determined by the observation that seems to be inconsistent with the rest of the dataset. The procedure to find the deviation in the data pattern from the corresponding behavior is known as the anomaly. Many types of research analyzed the anomaly detection issue from various perspectives like data security, pattern recognition, and data mining [15]. Anomaly is also termed as the deviation or fault recognition. For each network, the anomaly can be varied. One of the general and possible attacks is the Denial of Service (DoS) because it can be implemented easily. Anomaly attacks generate huge traffic in the network and tend to network congestion and the user suffers from the network traffic to transfer the information. While the anomaly takes place, the general operation ability of the host is minimized as the result of wrong memory allocation. This may cause the depletion in the network bandwidth and even affect the system process of the network like the routers and firewalls [16]. Based on the detection effectiveness and the utilizing efficiency the WSN characterized the anomaly detection with the limited network source. Detection accuracy generally represents the effectiveness of the identification process and it includes the false alarms and detection rate. Also, the efficiency of detection indicated the memory utilization and energy consumption.

The present network environment is more difficult, diverse network attacks and multisector attacks based on the different combinational protocols for anomaly attacks, becoming more general [17]. These are the complexities present in the detection of anomalies in the WSN. Machine learning is the most used anomaly detection, which proves the reliable result in many investigations. The advancement of the machine learning model for managing complex data is more popular in the present days and it is the most widely utilized approach in detecting the anomaly with high efficiency and simplicity [18]. In the earlier research, the Random Forest (RF) and Conditional Variational Autoencoder (CVAE) are the widely used anomaly detection in the network, which helps to determine the similarity among the input features and further the RF used to categorize the anomalies [19]. Compared with the earlier handmade signature-based approaches, machine learning plays an efficient role in detecting the anomaly with a higher False Positive Rate (FPR). This resulted in determining the data and detecting the real-time incursions are complex for the machine learning-based

anomaly detection system. In machine learning, the learning process for the system needs highly dimensional training data to get the corresponding constraints, which makes it more complex and time-consuming than the competing techniques [20]. For the identification of the anomaly, there are different types of techniques used which are statistical-based, classification-based, artificial intelligence-based, and clustering-based models. Most generally utilized machine learning techniques are one class principal component, Bayesian network, Support Vector Machine (SVM), and self-organizing map which are utilized to minimize the false alarm rate. These approaches are used to determine the anomalies and offer effective conclusions in specific network settings [21]. Mostly the practice of successful custom anomaly detection includes different types of complexities. Depending on the system's accuracy, capability, and usability, the underlying implementation concerns may divide into many kinds of issues. To reduce the sensing of energy consumption, machine learning is used to predict the future context. This model shows the accurate forecasting by the presented nodes and it is aware of the sensor reading in the vicinity [22]. Also, the adaptive sampling models based on the neural network are initiated to forecast the major parameter that includes the network load and sample period.

Machine learning can manage the pattern and relationship from the data which makes it ideal for identifying the anomalies in WSN. However, the implementation of machine learning methods directly on resource-constrained sensor nodes offered more complexities because of the limitations in energy constraints, power, and memory [23]. Standard anomaly detection techniques are not effectively suitable for the resource and dynamic limited nature of the WSN environment. Most of the existing anomaly identification models are generally tailored for univariate time series or batch data processing. Subsequently, the techniques are not suitable for real-time applications [24]. The general design of the offline detection does not effectively address the complexities posed the real-time anomaly detection. Because of the limited labeled anomaly data, the task of the anomaly becomes more difficult. Further, there is a lack of sufficient resource-aware anomaly identification approach that is suitable for the WSN. The earlier models have difficulty in addressing the necessity of effective and accurate detection with the reduction of communication overhead [25]. Therefore, for efficient anomaly detection in WSN, it is significant to solve the shortcomings of the previous research and to meet the present requirements.

1.1 PROBLEM STATEMENT

In the present days, WSN become the major priority for the wireless communication system, which is processed based on the large number of sensor nodes. The sensor node present in the WSN helps to communicate with the nearby node to develop the network. These sensor nodes are generally utilized for tracking and monitoring purposes. Due to the open and distributed nature of the WSN, they are unprotected from security threats like malicious and anomaly attacks. To ensure the security and reliability of WSNs, it is essential to have anomaly detection. There are different statistical and rule-based standard techniques in the earlier research for detecting anomaly detection. However, the existing techniques have many drawbacks that cause the network to perform poorly in detecting the anomaly in WSN. Some of the complexities in the traditional anomaly detection model are explained as follows.

a. Existing techniques require manual feature engineering to analyze the data pattern from the changing environment, which offers more struggle to adapt the information and has a lack of scalabilities. To solve this complexity the optimization-based feature selection is implemented to take out the potential information from the data pattern.
b. Some of the standard techniques from the literature works are not effective for the resource-limited and dynamic surrounding of WSN. Further, the biased result occurred due to the imbalanced data, which tends to poor functionality in detecting the anomalies. Therefore, this work implements an advanced hybrid anomaly detection model to address the changing difficulty in WSN.
c. The existing approaches are limited in terms of practical determination because of the absence of prior knowledge in terms of the correlation structure of the data. Therefore, an alternative model based on the machine learning technique is introduced in this work to effectively train the given data to achieve anomaly detection.
d. For the variable and complex network environment, it is difficult for the existing machine learning model to evaluate the feature learning. It is necessary to analyze the feature effectively to detect the anomaly with maximum accuracy. Hence this article utilizes the optimal feature selection to extract the high-level feature from the network data.
e. In the earlier methodology, the time required to identify the anomaly in the training data was high. This also leads to high memory consumption in the detecting process.

Therefore, to enhance anomaly detection in WSN, an advanced and hybrid model is implemented to uncover the potential benefits.

1.2 RESEARCH MOTIVATION

The list of complexities is needed for the motivation in developing anomaly detection in the WSN that is explained below.

a. Since the data can be damaged and corrupted for many reasons, providing quality and reliable data is a significant motivation to develop an effective anomaly detection model in the WSN.
b. Event detection is the main reason for the necessity of constructing the anomaly detection approach. Because WSN utilizes multiple sensors to monitor various phenomena. The use of anomaly detection early stage tends to make effective decisions based on the disaster.
c. In WSN, the malicious sensor nodes make a deal with some adversaries, which is another motivation for implementing the anomaly detector. Because this malicious sensor has the power to control other nodes and initiate attacks that can drain the network resources.
d. The measurements that occurred from the data fault become inconsistence by the characteristic phenomenon. Detecting this type of error is significant in improving the data quality because it causes complexity in the data transmission process.
e. Because of the unattended characteristic of the sensor node, the intruders earn access and hijack the nodes, which can exhaust the limited source of the network and provide corrupted data. To address this issue, the anomalies related to malicious attacks need to be detected for network security.

1.3 RESEARCH OBJECTIVES

The major research objectives of the designed anomaly detection model are described below.

a. To gather the required data regarding the WSN to test and train the designed machine learning model for the accurate detection of anomalies present in the network.
b. To create an efficient and precise model for detecting the anomalies in the network, which helps in identifying unusual patterns for the secure operation in WSN.

c. To enhance the detection accuracy effective feature selection is initiated to determine the significant feature from the WSN data based on the heuristic algorithm.
d. To design a hybrid machine learning-based anomaly detection system in WSN to determine the issues related to computational resource constraints and data privacy.
e. To investigate the potential of the system to provide an effective, reliable, and privacy-preserving solution for anomaly detection in WSN.

1.4 RESEARCH CONTRIBUTION

The major contribution of the work is to develop a secure and efficient WSN by implementing an innovative anomaly detection approach. The significant contribution list of the research work is detailed below.

a. To implement the effective method for the detection of anomalous data in WSN using the machine learning approach based on online prediction with limited memory consumption and reduced false alarm rates. The designed technique is more robust and able to determine the feature based on the probabilistic behavior, which helps the application to perform better with high security.
b. To achieve the optimal feature selection by using the SBOA model for retaining the significant feature from the given data, which makes the detection process much easier. In the developed model, the relevant features are selected and optimization is carried out by the metaheuristic algorithm to attain the optimal feature selection.
c. To design the HMLT model for detecting the anomaly in the WSN based on the optimal feature. This model is constructed by combining both the DBN model and BL for accurate detection. The detection process is performed based on the probabilistic behavior of the DBN network to obtain features. By analysing the DBN feature the BL model determines the anomaly and provides the detection result.
d. To validate the detection performance of the designed hybrid model for evaluating the abnormal behavior in the data by conducting a comparative analysis with existing models. The achieved result demonstrates the robustness of the proposed anomaly detection model.

2. LITERATURE RIVEW

2.1 RELATED WORK

In 2020, Gethzi*et al.* [1] have introduced a new model for anomaly detection in WSN using the Online Locally Weighted Projection Regression (OLWPR). The regression models were generally nonparametric and the present forecasting was functioned by the local function that utilized the data subset. This reduces the computation complexity, which was mainly required in WSN. By using the Principal Component Analysis (PCA) the dimensionality reduction occurs in the LWPR to manage the redundant and irrelevant data in the input. After the process of prediction, the determination of the dynamic threshold was modeled to evaluate the prediction deviation from the actual sensed value.

In 2024, Bertalanic*et al.* [2] have initiated the advanced anomaly identification model by implementing the time-series data. The predictive model mainly focused on solving the network disruption at the physical layer of the network. The developed approach performed state-of-the-art in time series data and achieved higher computational efficiency. In addition, the developed technique outperformed the conventional approaches with high leading points with significantly low computational complexities. The developed model attained a mean response latency and the result determined that the model offered high interpretability insights by analyzing the gradient changes in the network structure.

In 2023, Matar *et al.* [3] have suggested a methodology that mainly focused on energy-efficient anomaly detection by using the compression calculation data for the time series data of multivariate and further minimizing the operating time without compromising the measurement resolution. The developed technique effectively minimizes the energy consumption. To sense the sensor individually in the time series model, the developed approach sequentially learns the information based on the multiple sensors concurrently for the effective interaction among them. In addition, the initiated deep sequential learning technique reduced the necessity of the labeled data and directly applied it to real-world scenarios in the large data stream. The result of the real-world WSN determined that the implemented model was both robust and adequate in practice.

In 2022, Yao *et al.* [4] have recommended a model based on the Deep Convolution Neural Network (DCNN) and PCA for WSN anomaly detection. The developed approach was based

on the vulnerability of the WSN to attack the minimum storage space of the device. While compared with the traditional techniques the proposed approach has the more effective and lightweight capability of feature extraction, which potentially identified the network anomaly with less storage capacity. To enhancement of the developed model was determined by using the different metrics with the Receiver Operating Curve (ROC) to validate the classification result. From the research comparison, the implemented technique outperformed other standard models.

In 2024, Kannadhasan *et al.* [5] have presented the deep learning model for detecting the anomaly present in the WSN by using the data communication technique. The major steps involved in the suggested model were implementing the sensor network, cluster head selection, connectivity, detecting the attack, and the data broker. It was analyzed that the designed approach for anomaly detection performed better than the other neural networks and the deep learning model. From the comparative analysis, the result revealed the superior performance achieved by the presented model. Further, the wide-band single-patch microstrip antenna was included in this investigation. There were two parallel slots in the microstrip antenna patch to improve the bandwidth. The slot length gets optimized to attain the broad bandwidth. The displayed result proved that the developed approach achieved a higher performance in terms of detecting the anomaly.

In 2024, Muhammad *et al.* [6] have designed the novel Stacked Convolutional Neural Network and Bidirectional Long Short Term Memory (SCNN-Bi-LSTM) technique for anomaly detection in the WSN. To improve the detection performance, the Federated Learning (FL) was leveraged with the safeguard of privacy. The designed approach was unique to train the model without showing private information and hence improve the security concerns. The model effectively determines the sophisticated and early unknown pattern. The approach was specially developed to identify and classify the multiple attacks using the standard dataset. Compared to the standard model, the proposed technique is determined with a high superiority in the detection rate and identifies the unknown attack. The developed approach attained notable classification with great precision and accuracy by reducing the false positives and negatives. The proposed framework not only evaluated the identification of the complex cyber threat but also determined the effectiveness of the employed model for anomaly detection.

In 2022, Mittal *et al.* [7] have analyzed two energy-efficient strategies to achieve better performance in anomaly detection using the proposed neural network and the optimization architecture. He presented parameters that were considered to calculate the functionality of the energy-efficient throughput. Once the proposed model was implemented, the results were analyzed to validate the performance of the detection model. The simulation result showed that the proposed model outperformed other standard algorithms. From the classification outcome, the developed SVM achieved a better outcome in detecting the anomaly in the network.

In 2024, Gayathri *et al.* [8] have developed two optimization procedures for detecting the anomaly by using the FL along with the cloud-integrated energy efficiency technique. FL and the ensemble approach based on cloud integration help to improve data privacy and detection accuracy. Energy efficiency techniques and online learning were used to aggregate the cloud-based model to conserve energy on resource-constrained sensor nodes. Based on this combination an efficient and comprehensive architecture was developed for detecting the anomaly in the WSN. The experimental outcome defined that the cloud integration attained the highest detection accuracy, which was suitable for the real-time application. The integration of cloud computing in the framework makes more advancement in the system model of the WSN application. The effective outcome attained from the presented model was suitable for the large-scale WSN, which was used for industrial application.

Table 2.1: Characteristics and Complexities in the Existing Anomaly Detection Model in the WSN Network.

Author [citation]	**Methodology**	**Features**	**Challenges**
Gethzi*et al.* [1]	OLWPR	• It is the kind of learning model that helps to generate a nonlinear model to manage the data. • It also works very fast for the second-order learning approaches.	• It has poor performance while working with high-dimensional data.
Bertalanic*et al.* [2]	Graph Neural Network	• It helps to solve the physical layer disruption in the network. • It can observe the gradient changes and offer effective interpretability about the network structure.	• It has a high computation requirement for large time series data. • In decision-making, it has a lack of transparency, which makes it hard to analyze the procedure.
Matar *et al.* [3]	Deep sequential learning	• It reduces the necessity of the labeled data, which implies it can handle real-world scenarios with high efficiency.	• It is time-consuming and impractical to label the large stream of data
Yao *et al.* [4]	DCNN	• The architecture is lightweight and has high feature extraction capability. • It only requires limited storage capacity	• Training requires a long time to process. • For the large set of labelled data high computation requirement is necessary

Table 2.1: Characteristics and Complexities in the Existing Anomaly Detection Model in the WSN Network "Table Continued".

Kannadhasan *et al.* [5]	LSTM	• It enhances the stability to consistently function in multiclass and binary classification. • It has an acceptable network structure to run the real-time application.	• It performs badly while managing a huge amount of data for a large network framework.
Muhammad *et al.* [6]	SCNN-Bi-LSTM	• It improves the safeguarding of privacy and anomaly detection performance. • It determines superior detection for the unknown and the complex attack. • It can learn the temporal and local dependencies.	• It is a slower model and needs more training time. • It requires cross-domain knowledge to manage the data information
Mittal *et al.* [7]	LMNN	• It improves the training time of the network. • It is more effective in processing the nonlinear system.	• It can easily converge to the local minimum than the global minimum.
Gayathri *et al.* [8]	EFL	• It has high detection accuracy. • It can handle large datasets, which is suitable for huge data applications.	• It requires more computation and resources. • It has less interpretability.

2.2 WIRELESS SENSOR NETWORK

The architecture of the WSN [41] is generally based on the huge number of sensor nodes which are constructed by using four main components. The components are a data processing unit, data transmission unit, sensing unit, and power unit. The small storage media utilized by the processing unit in the processing task. Between one node and another, communication can be attained using the transceiver unit, or else it is used in the base station.

Similarly, the sensing unit has two subunits termed sensor and analog. The data from the field are collected using the sensor node, and the analog converts the signal into digital form and is used in the processing unit. In the sensor framework, there are more additional units present in it. The units are incorporated in the construction that depends on the energy generator application that transfers the sensor with an additional energy source. The sensor node mobility got support from the mobilizer and the present position is determined by the position-finding system of the sensor nodes. There are three major layers present in the WSN structure which are

a. Physical layer helps to combine the sensor nodes to the base station and also ensures the physical communication between them.
b. Data link layer determines the reliable connection between the base station and sensor nodes. It helps to handle the data transmission in the network.
c. Application layer helps the nodes to communicate with the base station with the corresponding data. It supports different kinds of applications for transmitting and receiving data.

Based on the various layers present in the WSN its structure gets varied from the physical layer to the network layer [42]. For the source encoding multiple protocols are utilized in the physical layer. In general, the design is selected between the delta modulation or the pulse code modulation and it is processed for the signal and coding propagation. Several choices are presented in the Medium Access Control (MAC) for maintaining the structure. Also, there are two major protocols in the MAC layer contention-free medium access and contention-based medium access.

According to the structure of the network, the routing protocols are classified on the network layer into location-based, hierarchical-based, and fit-based. All nodes are equally treated in the flat-based structure and offer similar functionality. According to the responsibilities, the hierarchical framework has different roles played by each node to fulfill the function. Additional responsibilities are given by the cluster head selection and the resource over the common nodes. The most suitable routing is determined using the node position in the location-based structure to achieve the target. The diagram for WSN is defined in Figure 2.1.

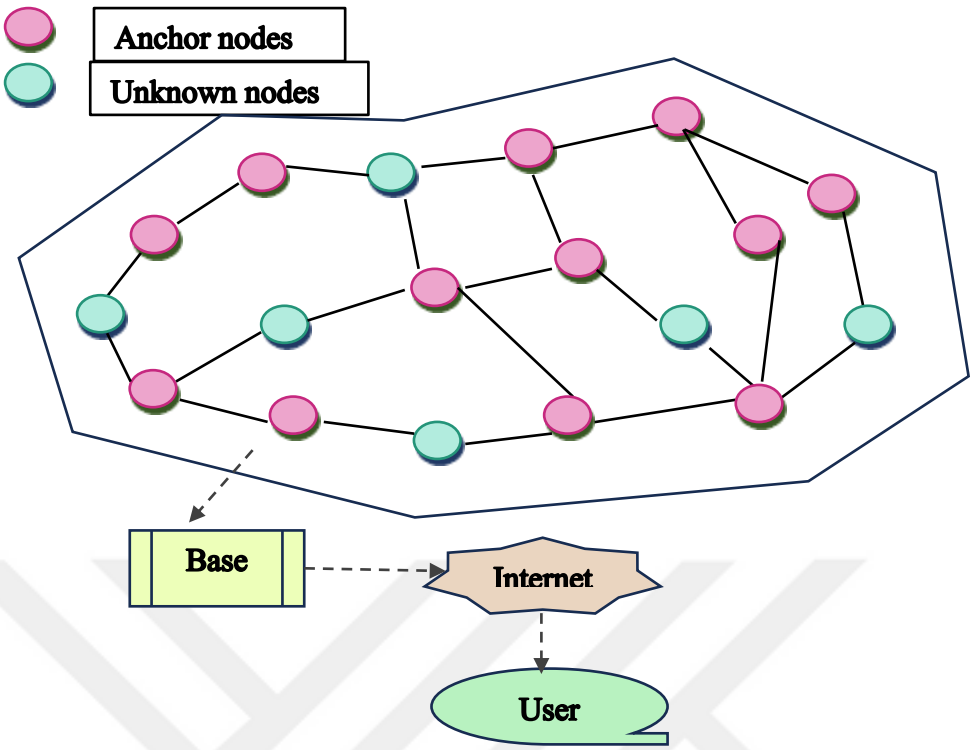


Figure 2.1: Characteristics and Complexities in The Existing Anomaly Detection Model in the WSN Network

2.3 APPLICATION USE OF WSN

There are different types of sensors are combined to form the WSN network. Some of the sensor nodes are visual, magnetic, thermal, and infrared. They are mainly designed for different applications according to the task [43]. These nodes help to monitor several conditions that include humidity, pressure, object direction speed, noise level, temperature light, and size of the object. Due to the unique feature of the WSN, it is widely used in more applications including real-time and lifetime applications which are defined in the following.

a. Environmental monitoring: It is used for different requirements that include the calculation of parameters for the wind direction along with the speed. For environmental monitoring, different sensors are used like humidity, wind speed, air pollution, and temperature, in which the sensors are deployed in the harsh environment to determine and calculate the factors of the environment.
b. Industrial monitoring: The sensor nodes are used to monitor the equipment state, and the sensors installed are pressure, temperature, and vibration. These sensors are very useful for industrial applications [44]. These sensors are further used to control, process, and

monitor the data information. The collected information is forwarded to the system management by the sensors. It also plays a significant role in determining the business process.

c. Healthcare monitoring: In the medical field, patients are monitored by using the small sensor nodes in a vital state. The different positions of the patient's body are induced with sensors to monitor the heart rate, mineral pressure, and enzymes. Advanced medical sensors are utilized in the healthcare domain to monitor the patient continuously using wearable hardware. The real-time monitoring of the patient even at their home is also possible.
d. Smart cities: Multiple types of sensors are used in smart cities like pedestrian sensors, parking sensors, and dustbin sensors, to make the cities more comfortable for the people. For the citizen's optimal life, various parameters installation is necessary in large cities [45]. There is a wide range of applications offered by the WSN to achieve real-time data to the corresponding authority for the optimal function of the city. WSN helps to monitor the traffic which helps to propose the intelligent parking system.
e. Forest fire detection: To prevent fires in the forest, different sensors are used. Here huge number of sensors are deployed in the targeted area to forecast and prevent forest fires. In human life, the significance of the earth and the value of forests play a major role. Also, continuous monitoring is required for the surveillance of the forest. Usually, the WSN is deployed in the aforesaid region or managing the safety.
f. Military application: WSN can perform various operations in the military field because of its technological advancement. The main categories that utilize the WSN are intruder identification, combat monitoring, and battlefield surveillance. Smart dust is the sensor node that is constructed in a small size, which can accomplish spying activities.

2.4 PROBLEMS CAUSED BY WSN

Some of the major complexities that are caused in the WSN, which affect the functionality of the network are defined as follows.

a. Communication fault-tolerant: In a harsh environment or uncontrolled surroundings, the deployment of the sensor nodes tends to become unreliable or produce faulty measurements because of environmental issues.

b. Minimum latency: The process in which the architecture deals with the sudden requirement that needs to be identified quickly by the operator [46]. Hence the system has to identify and make notifications for the event immediately as soon as possible.
c. Limited energy and power: In general, WSN is constructed with battery power sensors, which generally have limited energy resources. This tends to complexity in the network function for the long time operation.
d. Scalability: After auditioning the hardware, the performance of the system gets enhanced proportionally to the capacity that is added and tends to be the scalable system. In the sensing region, the number of sensor nodes deployed may be in the order of a greater number of nodes.
e. Media transmission: In general, the communication nodes are connected to the wireless medium in the network, which contains the multi-hop sensors. The standard issues related to the wireless channel like high error rate and fading may also affect the sensor network operation.
f. Coverage issue: In WSN one of the common issues is the coverage issue that shows the service quality, which is offered by the corresponding sensor network. In definition of the coverage is explained in multiple points of view because of the variety of the sensor network and the huge range of the applications.
g. Geographic routing: Geographic position information is the base structure to define the routing principle of geographic routing. It is generally defined by the wireless network that is based on the information idea of the source that offered the message to the geographic location of the destination other than the usage of the network address.
h. Sensor holes: There is the region of the sensor network in the routing hole, where each node is not presented or the available nodes cannot able to participate in the actual routing of the information because of multiple possible reasons [47]. It is generally challenging to determine the task since the typical wireless sensor network consists of low-capability lightweight nodes that are unaware of their geographic location.
i. Topology coverage: The issue of coverage defines how well the region is monitored or tracked by the sensors. In sensor networks, the connectivity and the coverage complexity have received notable attention in the investigation community in the present years. These issues are determined as the decision problem, whose goal is to evaluate, whether every

point in the service region of the sensor network is folded by the least k sensors, where k is given as the parameters.

2.5 CHALLENGES IN THE EXISTENCE OF ANOMALIES

Several types of complexities are present in anomaly detection in the WSN network. It is important to analyze a better detection model with high effectiveness and less energy cost. Similarly, the main goal is to offer highly efficient resources and detection effectiveness utilization at a similar time in the design of the anomaly detection solution [48]. There are several methods were developed in the earlier studies with the help of traditional network systems. Moreover, the context of the WSN and the nature of the sensor data make these solutions unsuitable for WSN applications. During the design of the corresponding anomaly detection solution, the challenges that need to be considered for the WSN are defined below.

a. Storage and computational resource limitations: In some cases, cheap sensors are used to create the WSN that are more resource-constrained regarding processing and memory. The utilization of the storage resource and the computation is significant for the anomaly detection process in real-time data processing.
b. Overhead in communication: Based on the centralized approach, some of the standard anomaly detection is created, in which the data are gathered from the sensors and sent whole data to process the cluster head and the base station. However, several order magnitudes are required for the data transmission which require more cost than the cost of the data processing. Additionally, the structure of the distributed online anomaly identification model also needs communication between the sensor nodes [49]. This resulted in the amount of communication overhead affecting the energy consumption incurred by the distribution process.
c. Dynamic change in network topology: In some WSN applications, the mobility nodes fail in communication, which tends to the network topology change. The channels are affected negatively by the normal reference model by the anomaly detector.
d. Heterogeneity network: There are multiple types of nodes required for the WSN application to conduct multiple jobs with different nodes. Furthermore, the present sensor nodes may be structured with different sensors for calculating multiple environment phenomena at a similar time. Another reason for the appearance of the heterogeneity is when in sensor collects too much distribution data making the anomaly. This is learned

based on the multiple types of distribution that are not workable to cope with such kind of heterogeneity.

e. Dynamic streaming data: The sensing data have the nature of dynamic streaming, which is more complex for the network structure. In common there is no prior knowledge that is required to build the general distribution of transferring data. Ata specific point in time, the knowledge becomes available and it is insufficient for the future because of the dynamic streaming that tends to natural distribution over time.
f. Network scalability: Over time some WSN applications become expanded in such a way that the nodes may tend to add to the network. As an outcome, the earlier normal reference technique constructed for the network required to be updated [50]. The expansion poses resulted in a high false alarm rate that is more challenging for anomaly detection. Other than the huge set of data produced, because of the network size expansion is also difficult for real-time detection.
g. High dimension data: There is the chance for maximizing the network size, and then the gathered data dimensionality also gets maximized. The maximization in the dimension of data incurs a larger computational cost that drains the energy and the sensor's memory. Most of the anomaly identification procedures are based on the measurement of data that higher the data dimension and become the source for the efficiency aspect of the anomaly detection.

2.6 DIFFERENT TYPES OF ANOMALIES

In the WSN there are different types of anomalies are present, which need to be detected effectively for the better performance of the network and to achieve effective rest for the corresponding task [51]. Some of the major types of anomalies in the WSN are explained below.

a. Node Anomaly: During the power problem in the WSN or the node fails, this kind of anomaly is discovered. Also, the several component power fluctuations or the solar panel failure resulted in the anomaly. The issues in the software and hardware in WSN also cause node anomalies.
b. Network Anomaly: The connection issue in the signal or the unexpected fluctuation in the signal strength are reason for the network anomaly [52]. This anomaly tends to

episodic connectivity or the complete loss of connectivity and becomes more issues in the network signals.

c. Data Anomaly: From the disordered data communication, there is the presence of intrusion and it is known to be the data anomaly. For the perfect decision making the data quality is necessary, which can be worsened by the data anomaly.

2.7 IMPORTANCE TO DETECT THE ANOMALIES

In WSN detecting the anomaly is a critical task, since it helps to identify the abnormal behavior and unnecessary events in the data. Some of the significant to determine the anomaly in WSN are detailed below.

2.7.1 Data Dimension Reduction

In common, the sensor data are classified by their dimension into univariate and multivariate data based on regional characteristics [53]. There are different sensors are there to originate the sample in the multivariate data for the specific or the different nodes. Notably, it is known that the sharing of the multivariate data improves the energy consumption in the sensor due to the overhead radio communication that is included in every variable. Hence the data sharing among the central location and the sensor nodes like the cluster head and the base station is the major reason for the immediate energy consumption in the sensors. Based on the sharing of one bit of data takes the power required to proceed with the greater number of bits present in the sensor. For the multivariate and large-scale data, additional energy is needed for the processing. This resulted in the dimensionality reduction in the multivariate is a significant task for minimizing the energy consumption to improve the lifetime of the sensor network.

2.7.2 Operation Mode

For WSN, early anomaly identification has not been noticed for the data anomaly in the online detection. Other than this identification functions after the time windows that correspond to the process of the WSN application. Moreover, the identification of the offline takes minimum energy and it needs additional memory for saving the data batches for the corresponding time window. Because of the delay in the detection timing the data integrity is affected. Hence to ensure data integrity and reduce the delay time, online identification is

preferable. Additionally regarding the computation, the utilization of the online identification mode is also known to be the cost of detection [54]. It is considered that the candidate method for online anomaly detection is lightweight to manage with the limitations in the resource. The efficiency of the anomaly identification solution is not only affected by the data dimension but also limited by computation complexity.

2.7.3 Model Structure

There are three types of network structures called centralized, distributed, and loca for detecting the anomaly. In the node scope, anomaly detection is initiated in the local structure with no collaboration among the network nodes. The data are sent to the central location in the centralized structure in which the cluster head and the base station take place in the anomaly identification process. In the end, the collaboration adopted the distributed structure between the nodes for the identification procedure in which each node forwards the summary of the data representation by its local normal reference model for the global construction to the cluster head based on the reference model. Each node utilizes the global reference model in the cluster for the corresponding detection.

2.7.3.1 Dynamic and adaptable data changes

Because of the sensor data measurement dynamic streaming, the network indicated the behavior of the normal data that becomes rigid on time. Therefore is important to have the effective anomaly detection than the normal model [55]. Further, with the resource restriction demand, the adoption of WSN is determined for the sensors. Therefore the required model needs to be efficient and lightweight to meet the demand in the resource restriction of the sensor device.

2.7.3.2 Exploitation of the data correlation

Closed neighbourhood sensor data measurements are generalized by temporal, spatial, and high attribute data correlations. The efficiency of the identification needs to improve for the attribute feature correlation through the data dimension reduction. The readings gathered at the single period are the temporal correlation and are related to the reading of the earlier period. The reading of nodes is the spatial correlation that is geographically related to each other and expected to correlate.

2.7.4 General Techniques For Anomaly Detection

This phase explains the existing classification criteria for the anomaly detection technique in the WSN based on the state-of-the-art classification model. Multiple types of models presented in the earlier research are discussed here with the feasibility for harsh environments [56]. It determines the features of the optimal outlier identification model for the harsh environment. The general classification criteria found in the earlier period are presented briefly as follows.

2.7.4.1 Statistical-based approach

An underlying data distribution is required for this type of model to detect the anomaly. The statistical model gets estimated and assumed to capture the data distribution and analyze the data instance with reading to fit the model. The anomaly is declared by the data instance if the probability of the data being created by the model with the distance measures. This approach can be categorized as parametric or non-parametric. Availability of the knowledge is assumed by the parametric technique about the underlying data distribution like the generation of data known to be the distribution. From the available data, the distribution parameter gets estimated. This approach can either be a non-gaussian or Gaussian model. The data distribution availability is not assumed by the non-parametric approach. Between the new test instance, for the typical distance measures the statistical model is utilized and utilizes some kind of threshold on the distance to evaluate whether the anomaly is observed. Histogram, wavelet, and kernel density are the most widely used models.

2.7.4.2 Nearest neighbor-based approach

It. Is the generally used model to evaluate the data instance regarding the nearest neighbor in the data mining community in the earlier time. The distances are computed using the multiple well-defined distance notion between the two data instances [57]. The anomaly is declared by the data instance as it is located far from the neighbors. For the univariate data, Euclidean distance is the most popular, whereas the continuous attributes of multivariate are handled by the distance metrics. This model is focused on many investigations because of the complexity of the forthcoming sections.

2.7.4.3 Clustering-based approach

Clustering is the type of grouping of the same type of data instance with similar behavior based on the cluster format. It can either be distributed or centralized. In the distributed model, all the nodes can function in the clustering of the sensed data and then spend the corresponding parameter in all nodes of cluster data to the gateway node to minimize the communication overhead. In centralized clustering, each node shares the whole data with the central node or the gateway to function the data clustering. Some distance measures are utilized by the nodes from the nearest cluster to determine the anomalies.

2.7.4.4 Classification-based approaches

The classification model learned to utilize the data instance set during the training section and then categorize the data instance to one of the training classes based on the testing section. This model is either unsupervised or supervised [58]. The normal instance boundary is learned by the one-class technique during the training while some anomaly instances may exist and offer any new instance lying outside the boundaries as anomalies. The definition of boundaries is represented as a quarter-sphere or sphere. This type of model requires self-training based on the new arrival of the datasets. In the past anomaly identification methodologies in WSN, classification-based models were split into different networks that depended on the model that was utilized.

2.7.5 Machine Learning-based Model

In WSN, one of the essential and challenging tasks is security. The security of the network is ensured by detecting the anomaly in the network. Multiple machine learning techniques are used in the earlier approach to detect the anomaly effectively and are described as follows.

2.7.5.1 Random forest

RF [26] is a collaborating-based algorithm that works on the surroundings of the query for similarity. It is the kind of classifier generally based on the decision tree. For conquer, enhance, and divide the efficiency by using the conventional strategy. The major strategy behind the random forest is that a group of weak learners generates a powerful group. It

mainly works for the hypothesis disjunction. It is the kind of supervised approach that has a collection of trees. Every tree in the forest gives the corresponding classification. There are two stages are there to function in the random forest mechanism, which are prediction and classifier. For the large dataset, the method works effectively and also with the heterogeneous data. The missing values are accurately predicted using this model. The huge number of decision trees produced by the impact of the randomly selected subset of the training sample and with each tree isolated variables. Hence there is a lower sensitivity level in the classifier with other streamlines apprising because of the training sample quality and the decision tree robustness. Significant challenges are faced by the earlier classifiers because of the curse of dimensionality and the large correlated data. For classifying the hyperspectral data, RF classifiers are the robust method. In WSN, the random forest algorithm solved different kinds of problems like MAC protocol and coverage.

2.7.5.2 Support vector machine

SVM [27] is a statistical-based model, that has efficiency in managing high dimensional data and can split the classes with huge margins but it needs tuning of parameter setting. The model utilizes regression to resolve different types of classification issues. For the importance of each data and the plot, the number of features re considered as the general coordinate. The hyperplane divided the group and also considered the nearest borderline from the general finding. The decision function specified by the support vector and the samples are divided into multiple subsets in practice.

2.7.5.3 Decision tree

DT [28] is generally used to manage noisy data because it can handle missing values and can easily be interpreted. But still, it is prone to sensitive and overfitting to the split criteria selection. The corresponding data characteristic and the application requirement are the main choices of the model. With the continuous and categorical dependent variable, the model is performed. Initially, the data are split into two or more sets of a similar type. It is the supervised machine learning model for classifying the set of rules to improve readability. There are two types of nodes in the decision tree which are known as decision nodes and leaf nodes. The target or class is predicted using the decision tree by generating the training approach based on the inferred decision rule from the training data. One of the main features

of the decision tree is that it allows comprehensive analysis, and minimizes ambiguity in decision-making and transparency. Multiple problems are solved using the decision tree like data aggregation path selection and anomaly detection.

2.7.5.4 Artificial neural network

ANN [29] is the supervised learning model that depends on the human neuron model for data classification. There are huge numbers of neurons connected with the ANN model that handle the information and perform the accurate outcome. Layers are used to process the ANN model and each layer is integrated with the nodes. These nodes are generally associated with the active function. There are three layers in the ANN structure, which are the input layer, the output layer, and one or more hidden layers. The non-linear and the complex data are easily handled by the ANN classifier and there are no restrictions for the given data. ANN are utilized by multiple real-time WSN applications and have higher computation requirements. The efficiency of the process is improved by the ANN model to solve different types of issues that are present in the WSN including routing, congestion control, localization, data aggregation, and identifying the faulty sensors.

2.7.5.5 K-Nearest neighbour

KNN [30] is the most straightforward instance-based model mainly used for classification and regression. The input is considered to be the k-nearest training set from the feature space. Based on the distance among the specified training samples KNN generally classifies and tests the samples. Multiple distance functions are utilized by the KNN like Hamming distance, Manhattan distance, chebychev distance function, Euclidean distance, Canberra distance function, and Minkowski distance. The size of the input dataset defines the complexity of KNN to perform the optimal solution for the same scale of the data. The possible missing value from the feature space also minimizes the dimensionality. In WSN, fault detection, and anomaly detection methods are used in the KNN.

2.7.5.6 Gradient boosting classifier

GBC [31] is the ensemble-based learning approach utilized for determining the regression and classification. This model worked under a weak predictive approach like the decision tree. The general strategy of the model is to construct and evaluate the ensemble model by

optimizing the arbitrary loss function. By utilizing the earlier loss function the model is constructed by the negative gradient regarding the iteration manner. It is necessary to reduce the loss function in the machine earning model and significantly optimize it. The difference between the predicted target and output is represented by the loss function.

3. PROPOSED METHODOLOGY

3.1 DESCRIPTIVE ANALYSIS OF PROPOSED ANOMALY DETECTION IN WSN

WSN is the kind of network, that is low cost, multifunctional, tiny, and low energy sensors that are deeply induced to process controlling, object tracking, and monitoring the phenomenon. Various applications use the WSN including sales tracking in business applications, target monitoring in military applications, control and architectural management in industrial applications, and home automation in personal applications. There are hundreds and thousands of sensor nodes employed in the high-density WSN within the setting resulting in insufficient and inaccurate data in the malfunction nodes. These nodes are liable to some malevolent attacks like DoS, eavesdropping, and black holes. The anomaly generally affected the collected high-quality data, in which the anomaly formed due to multiple reasons like reading error, malicious attack, node failure, and unusual events. Therefore, anomaly detection is a significant procedure to evaluate the sensor data quality before it is used for decision-making. The unusual patterns present in the nodes are generally termed outliers, exceptions, peculiarities, and anomalies. The necessary anomaly detection in the data can offer important actionable information in a huge range of application domains. Under various conditions, multiple researchers have examined abnormal data like outlier detection, fraud detection, and anomaly detection. Some of the machine learning techniques used to minimize the false rate to an extent in the existing research are class principal component classifiers, Bayesian network, SVM, neural network, and Naïve Bayes. The examination result revealed that the existing model outperformed in the classification with greater accuracy. However, the earlier approaches cannot able to identify the new variant of the known attack and tend to get a high false alarm rate for the unknown attack. Further, the time requirement is high in identifying attacks and the accuracy is generally based on the collected features. Therefore, it is necessary to develop an effective and accurate anomaly detection model in WSN. Figure 3.1 defines the proposed machine learning model procedure for detecting anomalies in WSN.

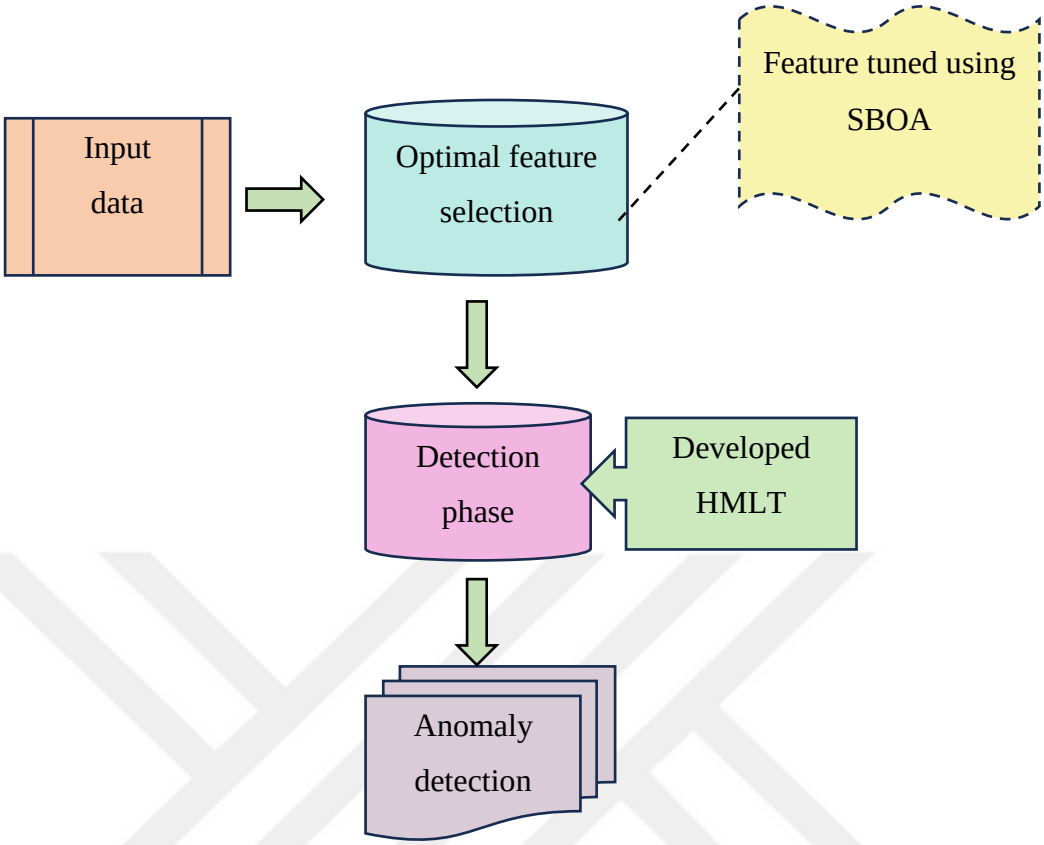


Figure 3.1: Illustration for Implemented Anomaly Detection Model Using Machine Learning.

The initiated methodology utilizes the effective machine learning model for detecting the anomaly in WSN. The system model involves steps like data gathering, feature selection, and anomaly detection. At first, the required data from the WSN network are collected from the available data resource called WSN-DS. The collected data includes different attacks that occurred in the WSN, which helps to train the developed model. From the given data using all the features to train the detection model is more time-consuming and generates trouble in detection. Moreover, DBN focuses mainly on feature extraction rather than feature selection. In addition, for the large-scale features, understanding and determining the compressed data is complex. Therefore, feature selection is more efficient than taking out the relevant feature. Hence the SBOA approach is utilized to select the optimal setting for the feature selection task. Therefore, raw data are subjected to an optimal feature selection process. This stage is significant to achieve the best result from the detection model by utilizing the minimum data, which ensures the simplicity and explainability of the model. Here the feature selection is carried out by implementing the SBOA approach based on

optimizing the selected feature. The main aim of the feature selection is to determine the best set of features from the given dataset that models the obtained issue to attain the detection model with robustness and better performance. It also minimizes the difficulty of the model and helps to solve the general complexities in the machine learning technique. The selected optimal features are subjected to the HMLT to build the anomaly detection model. The proposed HMLT is composed of two different machine-learning approaches called DBN and BL. The given optimal feature is initially moved through the DBN model.DBN has a stack of several RBM frameworks that generate the deep structure. It is a kind of probability generative model with a hidden and visible layer. The visible layer observes the given feature information based on the previous RBM. This RBM is constructed to boost the accuracy of the feature extraction by exchanging the learning features. Also, it follows the probability distribution principle to manage the learning cycle. It can manage a huge set of features based on the hidden unit to extract the underlying correlations. It achieves better results with a minimum of time-consuming. The obtained feature from the DBN is sent to the BL model for anomaly detection.BL is the probabilistic model, which has the advantage of quantifying the uncertainty. It performs more robust decision-making by analyzing the range of possible outcome and their related probabilities. The model is enabled by the integration of existing knowledge with new data to make the detection accuracy higher. The BL provides an effective detection outcome. The result obtained from the BL model defined the detection outcome of the anomaly present in the WSN. The functionality of the detection technique is evaluated by differentiating the model from other standard techniques. The comparative outcome showed that the developed model attains higher detection performance.

3.2 DATASET DETAILS

This research work uses a single dataset to test and train the designed anomaly detection model along with the existing approaches to validate the functionality of the initiated approach. The utilized data resource and its explanation are explained as follows.

The WSN-DS dataset for detecting the anomaly in the WSN is taken from the link "https://www.kaggle.com/datasets/bassamkasasbeh1/wsnds Access date: 2024-08-19". The dataset is mainly designed to achieve better identification and classification of different possible attacks in the network. The dataset included the DoS attack, scheduling attack, gray

hole, flooding, and blackhole. This dataset helps in determining the normal and abnormal behavior of the WSN.

From the obtained dataset the gathered data are indicated as Ws_a . Here the term $a = 1,2,3\ldots, A$, where A is the total collected data.

3.3 ILLUSTRATION OF HEURISTIC ALGORITHM: SBOA

The utilization of the SBOA [32] approach is to optimally select the feature from the given data. The SBOA is inspired by the natural behavior of the survival of the secretary bird. It helps to improve the feature selection by tuning the corresponding feature to attain the optimal solution.

a. Inspiration: The Secretary bird is an African bird, that has unique characteristics and mostly lives in the desert and grassland. It has individual hunting skills based on the sturdy and long legs that help to run and hunt the prey in the ground. After finding the prey, it spots it through its sharp eyes to make a plan. Further, it strikes the prey on the ground with the intention of killing. Exceptional intelligence is displayed by the secretary bird while hunting the snake. Also, it can predict the next move of the snake. This behavior inspired me to utilize the SBOA approach. The mathematical formulation of the SBOA is evaluated in the following.

b. Initialization: SBOA is the metaheuristic system, which is based on population. In the population of the optimization process, the secretary bird is known to be the member. The decision variable range is determined by using the secretary bird position in the search space. The candidate solution is represented by the position of the secretary bird in the SBOA approach. In the search space, the random initialization of the bird position is derived using Eq. (3.1)

$$W_{i,j} = k_j + q \times (t_j - k_j), i = 1,2,\ldots, M,\ j = 1,2,\ldots, Di \tag{3.1}$$

Here the random factor between the values $[0,1]$ is denoted as q . The lower and upper bounds are specified as k_j and t_j . The i^{th} bird position is indicated as W_i . In the algorithm, the optimization is initiated from the candidate solution of the population.

In the upper and lower bounds, the candidate solutions are generated randomly. Each iteration offered the optimal solution and it is evaluated using Eq. (3.2)

$$W = \begin{bmatrix} w_{1,1} & w_{1,2} & \cdots & w_{1,j} & \cdots & w_{1,Di} \\ w_{2,1} & w_{2,2} & \cdots & w_{2,j} & \cdots & w_{2,Di} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ w_{i,1} & w_{i,2} & \cdots & w_{i,j} & \cdots & w_{i,Di} \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ w_{M,1} & w_{M,2} & \cdots & w_{M,j} & \cdots & w_{M,Di} \end{bmatrix}_{M \times Di} \tag{3.2}$$

Here the group of secretary birds is indicated as W, and the j^{th} question of i^{th} secretary birds is specified as $W_{i,j}$. The number of members in the group is indicated as M and the variable dimension issues are specified as Di.

To optimize the issues, the candidate solution is specified by each secretary bird. The combined vector for obtaining the objective function is determined using Eq. (3.3)

$$E = \begin{bmatrix} E_1 \\ \vdots \\ E_i \\ \vdots \\ E_M \end{bmatrix} = \begin{bmatrix} E(W_1) \\ \vdots \\ E(W_i) \\ \vdots \\ E(W_M) \end{bmatrix}_{M \times 1} \tag{3.3}$$

Here the objective function vector is denoted as E, and the i^{th} bird objective function is indicated as E_i. The candidate solution quality is analyzed effectively by the value of the obtained objective function. This step provides the best candidate solution for many of the problems. In every iteration, the objective function value and the secretary bird position are updated. Two natural behaviors of the secretary bird are used to determine the SBOA member.

c. Exploration phase: The secretary bird hunting strategy is managed to perform the exploration phase. In this phase, the secretary bird initially proceeds with the prey-searching skill based on the sharp vision to spot the hidden snake. This bird has a long leg, which helps to sweep the ground and has the tendency to avoid getting the snake attacked. Multiple regions are explored by the individual in the solution space to enhance

the global optimum. The position updation of the secretary bird is formulated in Eq. (3.4) and (3.5)

$$While\ s < \frac{1}{3}S, w_{i,j}^{newo1} = w_{i,j} + (w_{ran\_1} - w_{ran\_2}) \times Q_2 \tag{3.4}$$

$$W_i = \begin{cases} W_i^{ne,O1}, & if\ E_i^{ne,O1} < E_i \\ W_i, & else \end{cases} \tag{3.5}$$

The present iteration is specified as s, the secretary bird new state is indicated as $W_j^{ne,O1}$. The objective function fitness value is indicated as $E_i^{ne,O1}$. After finding the prey, it started the hunting strategy. This model helps to solve the local optimum premature converging and tune the convergence of the algorithm to attain the best solution. Here the Random Brownian (RB) motion is initialized to the individual to manage the effective solution space and offers the local optimum that leads to the prey-consuming stage and it is expressed using Eq. (3.6) and (3.7)

$$RB - ran(1, Di) \tag{3.6}$$

$$W_i = \begin{cases} W_i^{ne,O1}, & if\ E_i^{ne,O1} < E_i \\ W_i, & else \end{cases} \tag{3.7}$$

The arrays that are generated randomly are indicated as $ran(1, Di)$. Further, the secretary bird utilizes the leg-kicking technique to hurt the prey in the target position. This kick is generally to kill the snake and to safeguard themselves from the snake. The capability of the optimization process in the global search is improved by the levy flight strategy. The search space exploration improved by simulating the secretary bird's flight ability. The position updation of the secretary bird in attacking the prey is derived using Eq. (3.8)

$$W_i = \begin{cases} W_i^{ne,O1}, & if\ E_i^{ne,O1} < E_i \\ W_i, & else \end{cases} \tag{3.8}$$

The weighted levy flight is utilized to improve the accuracy of the optimization and it is evaluated using Eq. (3.9)

$$RL = 0.5 \times Levy(Di) \tag{3.9}$$

Here the levy flight is specified as $Levy(Di)$ in the distributed function. It is demonstrated by using the Eq. (3.10)

$$Levy(Di) = r \times \frac{t \times \sigma}{|u|^{\frac{1}{\eta}}} \tag{3.10}$$

Here the fixed constant is indicated as r, η. Further, the term σ evaluated by using the Eq. (3.11)

$$\sigma = \left(\frac{\Gamma(1+\eta) \times \sin\left(\frac{\pi\eta}{2}\right)}{\Gamma\left(\frac{1+\eta}{2}\right) \times \eta \times 2\left(\frac{\eta-1}{2}\right)} \right)^{\frac{1}{\eta}} \tag{3.11}$$

Here gamma function is specified as Γ.

d. Exploitation phase: The secretary bird escape strategy is utilized here to achieve the exploitation phase. Multiple evasion strategies are utilized by the secretary bird to protect their food and themselves from the threat. In the corresponding camouflage environment, the predators are detected by the secretary bird. The exploitation phase is enhanced by adjusting the possible factors at various stages and it is expressed using Eq. (3.12) and (3.13)

$$w_{i,j}^{ne,O2} = \begin{cases} B_1 : w_{bes} + (2 \times RB - 1) \times (1 - \frac{t}{T})^2 \times y_{i,j} & if\ q\ and < q_i \\ B_2 : w_{i,j} + Q_2 \times (w_{ran} - J \times y_{i,j}) & else \end{cases} \tag{3.12}$$

$$W_i = \begin{cases} W_i^{ne,O2}, & if\ E_i^{ne,O2} < E_i \\ W_i, & else \end{cases} \tag{3.13}$$

Here the solution of the random candidate is indicated as w_{ran} of the present iteration.

The flow chart determination of the SBOA approach is defined in Figure 3.2. The pseudocode for SBOA is defined in Algorithm 1.

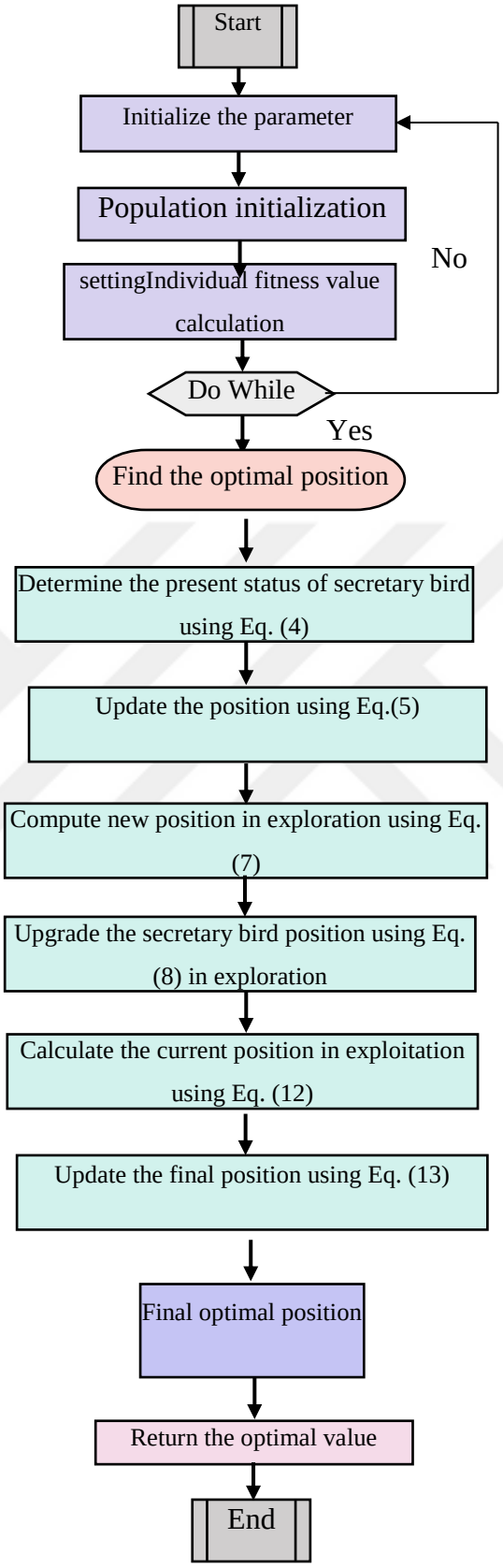


Figure 3.2: Flow Chart for SBOA Algorithm.

Algorithm 1: SBOA

Problem setting initialization for SBOA

Iteration updating in algorithm

Population initialization

While the iteration starts

Exploration

Evaluate the present status of the i^{th} Secretary bird using Eq. (4).

Update i^{th} Secretary Bird using Eq. (5)

Compute the new position of the i^{th} Secretary Bird using Eq. (7)

Upgrade the i^{th} Secretary Bird using Eq. (8).

else

Solve the new level of the i^{th} Secretary Bird using Eq. (9).

Reform the i^{th} Secretary Bird using Eq. (10)

Exploitation:

Calculate the current position of the i^{th} Secretary Bird using B_1 Eq. (11).

Else

Evaluate the present status of i^{th} Secretary Bird using B_2 Eq. (12).

Determine the i^{th} Secretary Bird using Eq. (13).

End while

Update the best candidate solution

Return the best optimal solution for SBOA.

3.4 SELECTION OF OPTIMAL FEATURES

One of the significant factors in designing the anomaly detection system based on the machine learning model is to develop a corresponding feature selection process [33]. The available data from the publicly available dataset, which is used to detect the anomaly makes the process complicated and delays the systematic investigation of the effect of the features. To avoid these issues, optimal feature selection is utilized in this work.

Optimal feature selection is the method used to remove unnecessary and redundant features from the given data to maximize the functionality in terms of accuracy. In general, the raw

data from the dataset are noisy and have more irrelevant features. For the high dimensional data, it is complex to analyze the corresponding feature that is required for detection. Hence the effective optimal feature selection is necessary to enhance the system process. The irrelevant feature in the data has the chance to mislead the learning process. This problem can be only addressed using the feature selection process. The feature selection process searching for the optimal feature subset is more complex. Hence, the SBOA approach is implemented in this work to select the optimal feature from the given data Ws_a. It reduces the computation time and improves the detection rate in the final anomaly detection. This process helps the detection model to perform with a minimal number of features. It simplifies the features, which is significant for the decision-making. It eliminates the unnecessary features to construct an efficient subset of features. The initiated SBOA algorithm optimizes the feature to get the effective resultant feature. The objective function is expressed using Eq. (3.14)

$$Obj = \arg \underset{\{Fe^s\}}{Max}[\mathrm{Re}\, Sc] \tag{3.14}$$

Here is the obtained optimal feature from the raw data is indicated as Fe^s. The term $\mathrm{Re}\, Sc$ specified the relief score respectively and it is defined in the following.

Relief score is mainly used in the feature selection that determines the feature score of each feature that is applied to choose the top-scoring feature. It is generally based on the evaluation of the feature value between the nearest instance pair. It helps to calculate how well the feature discriminates between the same and different class instances and it is derived using Eq. (3.15)

$$\mathrm{Re}\, Sc = w - (z_i - Sm_i) + (z_i - Dm_i) \tag{3.15}$$

Here the same and different class instances are specified by the term Sm_i and Dm_i. The feature vector is indicated by the term z_i. The resultant feature from the optimal feature selection is represented as Fe^s.

3.5 DEEP BELIEF NETWORK

DBN [34] is the type of machine learning approach that become more powerful because of the semi-supervised learning nature. The network has a multi-layer structure that initiates

the enhanced functionality in the detection model. The training set can learn and extract the specified characteristics and subject them to the sensor nodes. It can manage new training data within less time, and hence it is suitable for the WSN. There are several layers of Restricted Boltzmann Machine (RBM) are presented to generate the DBN. Initializing the biases and weight are the major ideas to pretrain the unlabeled data.

DBN has more hidden layers, which implies the specialty of the model. There are more descriptive features are present in the upper layer of the DBN network that helps to determine the solution for the detection system. It also has the capability of using the connection among the features to achieve effective performance with a minimum training set. Initially, the training of the RBM is done separately with the independent and unsupervised features in the training phase. After retaining the feature information the feature mapping is attained possibly into different feature spaces.

The updation of weight is performed in the RBM training along with the gradient descent based on Eq. (3.16)

$$v_{ij}(s+1) = v_{ij}(s) + \eta \frac{\partial \log(q(u))}{\partial v_{ij}} \tag{3.16}$$

Here j^{th} hidden cell and i^{th} visible cell weight are represented as $v_{i,j}$. The detection rate is specified as q. The visible vector probability is denoted as $q(u)$ and it is derived using Eq. (3.17)

$$q(u) = \frac{1}{Y} \sum_{g} d^{-D(u,g)} \tag{3.17}$$

For normalizing the partition function is utilized and it is termed as Y. Similarly, the energy function is indicated as $D(u, g)$ that is assigned to the network. Based on the G_j hidden layer and input w the joint distribution is observed, and it is modeled using Eq. (3.18)

$$q(w, G_1, \ldots, G_M) = \left(\prod_{j=0}^{M-2} Q(G_j \mid G_{j+1}) \right) . Q(G_{M-1}, G_M) \tag{3.18}$$

Here the visible unit conditional distribution is represented as w and $w = G_0, Q(G_{j-1} \mid G_j)$ in the j^{th} layer with the RBM hidden unit condition. The joint distribution between the

visible and hidden layers is denoted as $Q(G_{M-1} \mid G_M)$. The training vector initializes a new visible layer and the values are assigned based on the biases and weight. The structural diagram for the DBN method is defined in Figure 3.3.

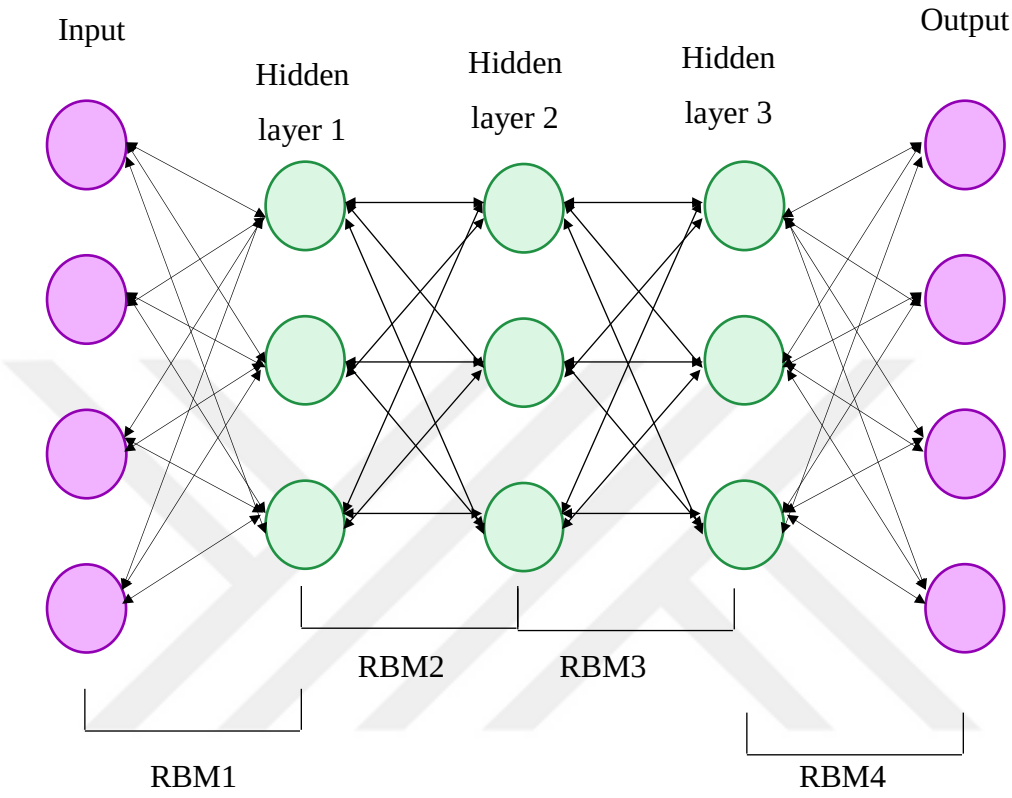


Figure 3.3: Architectural Illustration for DBN Model.

3.6 BAYESIAN LEARNING

BL [35] is the most efficient learning model in machine learning that has the specialty of accurate detection. It is well suitable for detecting the anomaly because it can manage high-dimensional information which human finds hard to interpret. It is the kind of graphical model based on the probabilistic nature that encodes the joint probability distribution between the variables of interest. With the set of directed edges and nodes, the BL directly forms the acyclic graph. It achieves convenient and fast calculation. It is more robust for the missing information and better related to the categorical information. In high dimensional space, the joint probability distribution is efficiently classified using conditional and unconditional encoding. Figure 5 defines the framework of the BL method.

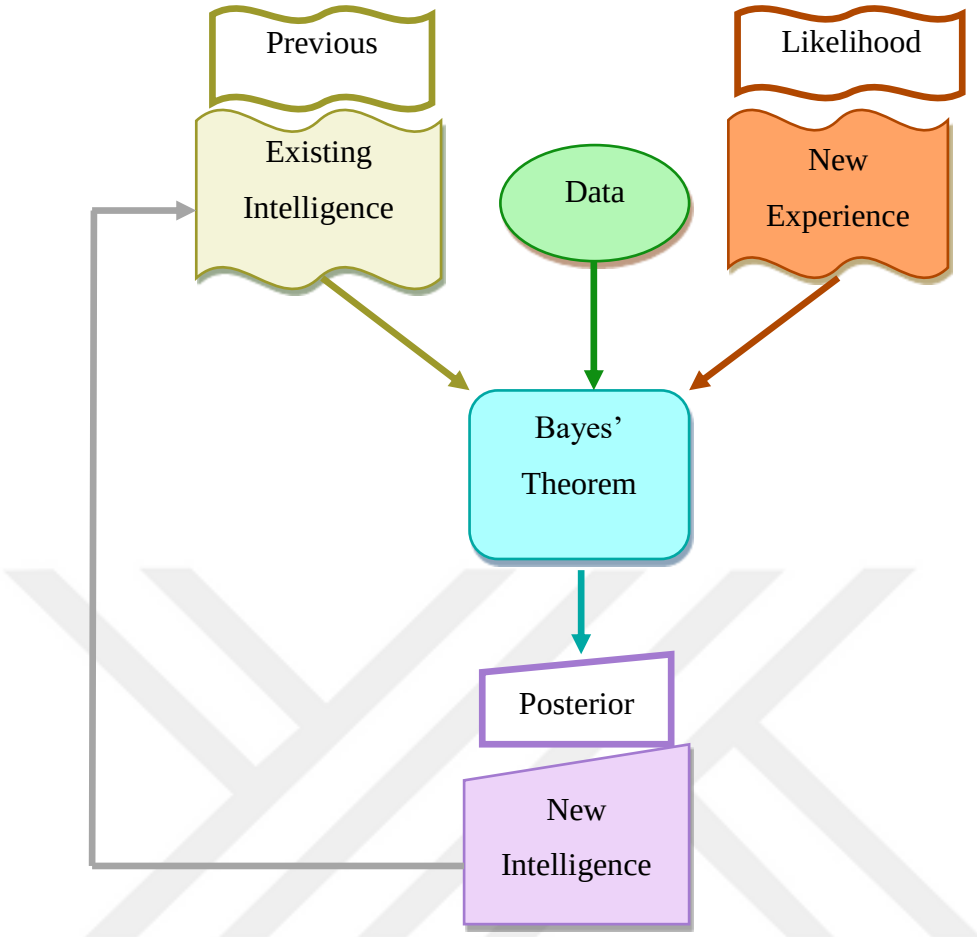


Figure 3.4: Process Flow Diagram for BL Model.

In BL, the given data are considered as the nodes in the network and can take any state in the state space. These nodes are given prior probability distribution over the state depending on the prior belief in the nodes. The distribution in the BL is derived using Eq. (3.19)

$$P(q \mid r) = \frac{P(r \mid q)P(q)}{P(r)} \tag{3.19}$$

Here the prior probability of the training data is indicated as $p(r)$, prior probability of the hypothesis node is specified as $p(q)$. The posterior probability of r given q represented the $P(r \mid q)$ respectively. It is essential to have the prior information, that allows the probability function to learn the function based on the probability distribution.

3.7 RECOMMENDED HYBRID CLASSIFIER FOR DETECTION

Anomaly detection is a significant task in WSN because it helps to determine the abnormal behavior and unusual events in the sensed data. The presence of an anomaly leads to potential security threats and failure in equipment, which needs to be solved immediately. However, the existing anomaly detection models are not efficient for WSN, because they need the predefined rules that are complex to construct the WSN system with high dimensional data. Therefore, this work developed the HMLT, which helps to improve the accuracy of anomaly detection.

The HMLT model is initiated to detect the anomaly in WSN based on the optimal feature selection. The developed model utilizes the machine learning approach because it can learn the sensor data and identify the patterns that are suggestive of normal and abnormal character without manual operation. Here the HMLT is constructed by integrating the standard DBN and BL to enhance the detection performance. The resultant optimal feature Fe^{s} is given as input to the HMLT approach. The given input is induced to the DBN model, which contains the stack of several RBM structures to construct the deep framework. Every RBM has both the hidden and visible layers. The given feature input is accepted by the visible layer from the past layer and the processed output is stored in the hidden layer. Here the initial layer learns the given feature directly and generates latent representation during the procedure. The feature is learned effectively by this layer-wise operation. Once the RBM is trained with the feature, the input is taken by the other stacked RBM in the training layer. The vector gets trained by the initialization of the new visible layer. The whole procedure is repeated until the corresponding feature is obtained. The resultant features from the DBN network are sent to the BL model for anomaly detection. From the feature, the BL learns the probable hypothesis from each set of hypotheses. Initially, it observes the given feature and builds the probabilistic model to determine the likelihood of the feature. The developed HMLT model for identifying anomalies in WSN is defined in Figure 3.5.

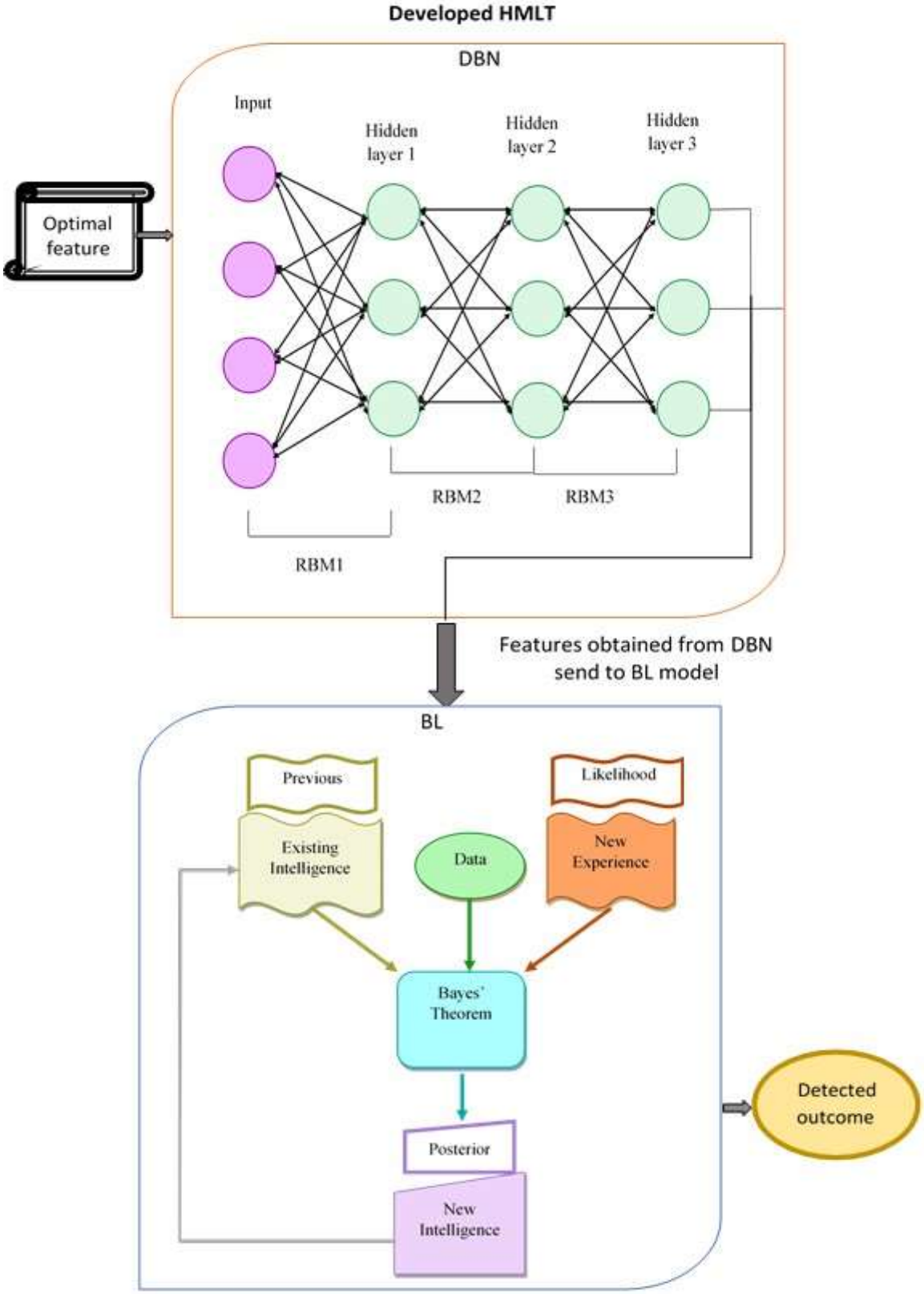


Figure 3.3: Structural Representation of HMLT Model for Detecting Anomaly in WSN.

The conditional probability described in this model is computed based on the prior knowledge. Here the DBN is utilized because it can deal with complex and high-dimensional data. Also, it works faster, when compared with other standard approaches. It provides better generalization and can learn the hierarchical representation from the feature. Similarly, BL offered a principled method to evaluate the uncertainty in detection. It offers inference without relying on huge samples. The result obtained from the BL defines effective anomaly detection.

4. RESULT AND DISCUSSION

This section determines the corresponding result and discussion of the suggested anomaly detection model in WSN. It involved the comparative result of the developed model along with the other existing techniques in graphical and table form.

4.1 SIMULATION SETUP

The suggested anomaly detection model in WSN was executed in the MATLAB 2020a platform, and the performance analysis was carried out to ensure the advancement of the developed approach. Here the population number was 10, chromosome length was 5, and a maximum of 50 iterations were utilized. Several comparative algorithms were utilized Black Widow Optimization (BWO)[36], Archimedes Optimization Algorithm (AOA) [37], Golden Eagle Optimizer (GEO) [38], Mud Ring Algorithm (MRA) [39], and Secretary Bird Optimization Algorithm (SBOA) [32] were adopted. Also, classifiers like LSTM [59], GRU [40], DBN [60], and BL [35] were employed.

4.2 PERFORMANCE MEASURES

Multiple metrics are utilized for determining the functionality of the suggested anomaly detection model and are explained below.

Accuracy is the general metric that is utilized for analyzing the performance of the detection model. This measures as the ratio of perfect prediction to the whole number of input samples and it is determined using Eq. (4.1)

$$Acy = \frac{Mx^{p} + Mx^{n}}{Mx^{p} + Mx^{n} + Ny^{p} + Ny^{n}} \tag{4.1}$$

Sensitivity to estimate, how better the technique can identify the positive instance. It demonstrates how likely you are to get an effective result while testing the sample. The technique that has the high sensitivity only has fewer false negatives and it is calculated using Eq. (4.2)

$$Sty = \frac{Mx^{p}}{Mx^{p} + Ny^{n}} \tag{4.2}$$

Specificity is considered to be the true negative rate. It evaluates the performance of the approach for detecting the negative classes. It is estimated by dividing the number of true negatives from the whole number of false positives and true negatives. The achievement of maximum specificity can perfectly determine the most negative results. It is demonstrated by using Eq. (4.3)

$$Spy = \frac{Mx^{p}}{Mx^{n} + Ny^{p}} \tag{4.3}$$

Precision is the metric to analyze the performance of the machine learning model. It is measured by dividing the number of true positives by the total number of positive predictions. The balance between completeness and accuracy is termed precision and it is evaluated using Eq. (4.4)

$$\Pr s = \frac{Mx^{p}}{Mx^{p} + Ny^{p}} \tag{4.4}$$

The False Positive Rate (FPR) is to calculate the models for how often it wrongly detects the correct result. It is the likelihood that a false alarm to be raised. It is measured using Eq. (4.5)

$$FPR = \frac{Ny^{p}}{Ny^{p} + Mx^{n}} \tag{4.5}$$

A False Negative Rate (FNR) is the likelihood that a true positive gets missed by the analysis. It is also considered to be the missing value. The number of false negatives is calculated using the RNR by using Eq. (4.6)

$$FNR = \frac{Ny^{n}}{Ny^{n} + Mx^{p}} \tag{4.6}$$

A Negative Predictive Value (NPV) is to determine whether the sample generates a negative prediction. It is explained by the proportion of the real negatives with the detected negatives. it is estimated using Eq. (4.7)

$$Npv = \frac{Mx^{n}}{Mx^{n} + Ny^{n}} \tag{4.7}$$

The False Discovery Rate (FDR) is the statistical metrics, that differentiate the quantity of expected false positives to precision. It is generally determined for investigating the whole and useful assessing of the model prediction and it is measured using Eq. (4.8)

$$FDR = \frac{Ny^{p}}{Ny^{p} + Mx^{p}} \tag{4.8}$$

The F1-score is the evaluation measure that can assess the forecasting ability of the technique by investigating the functionality of each class individually rather than knowing the accuracy functionality. It is formulated in Eq. (4.9)

$$F1S = 2 * \frac{Mx^{p} * Mx^{n}}{Mx^{p} + Mx^{n}} \tag{4.9}$$

Matthew's Correlation Coefficient (MCC) is the statistical metric used to calculate the amount of multiclass and binary classification. It helps to determine the error metrics based on Eq. (4.10)

$$MCC = \frac{Mx^{p} \times Mx^{n} - My^{p} \times Ny^{n}}{\sqrt{\left(Mx^{p} + Ny^{p}\right)\left(Mx^{p} + Ny^{n}\right)\left(Mx^{n} + Ny^{p}\right)\left(Mx^{n} + Ny^{n}\right)}} \tag{4.10}$$

False Omission Rate (FOR) offers the number of false negatives that happened in the form of a percentage of the negative result. It is the decision-making process, which has the conditional probability of condition that is offered for the negative decision and it is derived using Eq. (4.11)

$$FOR = \frac{Ny^{n}}{Ny^{n} + Mx^{n}} \tag{4.11}$$

Prevalence Threshold (PT) is calculated by using the measures of specificity and sensitivity. The obtained values are not dependent on the population of interest. it is computed using Eq. (4.12)

$$PT = \frac{\sqrt{Mx^{p} \times My^{p}} - Ny^{p}}{Mx^{p} - Ny^{p}} \tag{4.12}$$

The Critical Success Index (CSI) is efficiently integrating the sensitivity and positive predictive value. It helps to validate the performance of the model based on the correct event with the total number derived using Eq. (4.13)

$$CSI = \frac{Mx^{p}}{Mx^{p} + Ny^{n} + Ny^{p}} \tag{4.13}$$

Balanced Accuracy (BA) is the arithmetic measure of specificity and sensitivity, which is used to deal with imbalanced data. It is determined by the average of obtained recall on every class measure using Eq. (4.14)

$$BA = \frac{Mx^{p} + Mx^{n}}{2} \tag{4.14}$$

Fowlkes–Mallows index (FM) is the external performance measure that is utilized to demonstrate equality between the two phases. It is formulated using Eq. (4.15)

$$FM = \sqrt{\Pr s \times \mathrm{Re}} \tag{4.15}$$

Bookmaker (BM) is used to analyze measures like the event outcome probability and the corresponding outcome. Here the elements are balanced to change the odd one to profitable. It is estimated using Eq. (4.16)

$$BM = \mathrm{Re} + Spy - 1 \tag{4.16}$$

Markedness (MK) is the calculation of the negative and positive trustworthiness of the system model. It is measured by using the precision and NPV values. It demonstrates between the real negatives and real positives and it is defined using Eq. (4.17)

$$MK = \Pr s + NPV - 1 \tag{4.17}$$

The Positive Likelihood Ratio (LR+) is the tool used for the conditions as positive test results, in which the present result is odds. It is the probability of testing negative in which it is negative and it evaluated using Eq. (4.18)

$$LR+ = \frac{\mathrm{Re}}{FPR} \tag{4.18}$$

The Negative Likelihood Ratio (LR-) is the determination of the probability ratio for the sample with continuous value or higher than two results that are equal to the measures and resulted in a specific probability ratio shown in Eq. (4.19)

$$LR- = \frac{Ny^{p}}{Mx^{n}} \tag{4.19}$$

Diagnostic Odds Ratio (DOR) denoted the improved test that is simply inverting the result of the test in the wrong direction, which it determined using Eq. (4.20)

$$DOR = \frac{Mx^p / Ny^p}{Ny^n / Mx^n} \tag{4.20}$$

Prevalence is the proportion of the specific population that is generated to affect the condition at the corresponding time. It is evaluated by differentiating the number of found cases from the total number of cases and it is expressed in Eq. (4.21)

$$\Pr e = \frac{p}{p+n} \tag{4.21}$$

The true positive and true negative is specified as Mx^p and Mx^n. False positive and false negative is indicated as Ny^p and Ny^n respectively. Similarly, the term p and n denoted the positive and negative values. These metrics are used to determine the functionality of the developed model by analyzing the obtained result compared with the actual result.

4.3 COST FUNCTION ANALYSIS OF THE UTILIZED SBOA OPTIMIZATION

The cost function determination of the feature selection process in the anomaly detection model on the WSN helps to analyze how well the detection approach evaluates to precisely select the effective feature. For understanding the improvement of multiple machine learning algorithms, this convergence analysis is necessary. The cost function estimation of the implemented model in better feature selection is offered in Figure 7. The developed SBOA model converges faster, which makes the cost function lower than other optimization models. It also minimizes the training time that stabilizes the cost function. The SBOA model is used to tune the feature parameters in the feature selection process to achieve the optimal result in feature selection. The effectiveness of the feature tuning is represented in the graphical representation of the SBOA model. More training is required for the less convergence performance and it takes more time to adjust the feature setting. From the graph, the SBOA achieved higher convergence than 25% of BWO, 8.3% of AOA, 16.6% of GEO, and 16.3% of MRA for taking the number of iterations as 10. From the result, the SBOA exhibits smooth and fast convergence, which defines the positive side of the SBOA. While comparing the conventional algorithm the SBOA has a high potential with maximum convergence in the feature selection process.

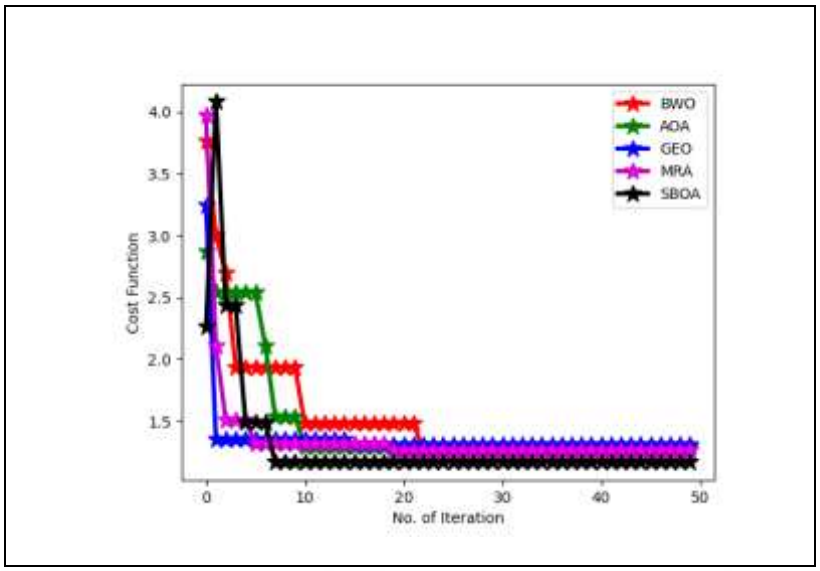


Figure 4.1: Coat Function Validation of the Utilized Algorithm SBOA Compared Over other Existing Algorithm.

4.4 ROC-BASED DETECTION PERFORMANCE ANALYSIS

ROC estimation of the implemented model is defined in Figure 8. In this research, the improvement of the developed HMLT approach for detecting the anomaly in the WSN is determined using the Receiver Operating Characteristic (ROC). The efficiency of the approach was evaluated by plotting the ROC curve, which discriminates the multiple categories of the final rest obtained from the HMLT. The investigation based on the ROC analysis defines the overall capacity of the model in the identification phase, which is also compared with other existing techniques to know the validation of the model. The visual representation of the false positive rate and the true positive rate are evaluated in this ROC determination to validate the ability of the model. Here different conventional approaches are utilized to validate the proposed HMLT to measure the detection capability of the technique. From the graph, the HMLT achieves a higher value than 16.6% of LSTM, 13.3% of GRU, 11.1% of DBN, and 5.5% of BL while taking the false positive rate as 0.2. The occurred higher value defines the overall functionality in terms of different metrics. The HMLT model achieves a significantly higher area under the ROC curve than other conventional models in detecting the anomaly in WSN.

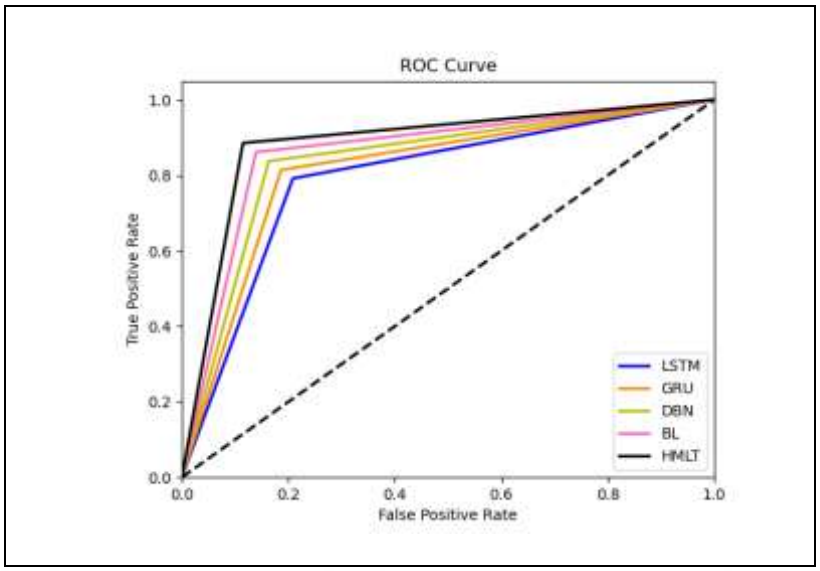


Figure 4.2: ROC-Based Classification Performance of The Developed Classifier Along with Standard Techniques.

4.5 PERFORMANCE ANALYSIS OF THE DESIGNED ANOMALY DETECTION FRAMEWORK BASED ON MULTIPLE ACTIVATION FUNCTIONS

The performance calculation of the proposed HMLT technique compared with other standard techniques regarding the several activation functions is expressed in Figure 9. The comparative analysis of the designed model functionality in anomaly detection compared with the other well-established model. Here the comparative models are taken from the existing studies based on significant activation functions for various metrics like accuracy, BA, BM, CSI, etc. The generated model improves the detection performance by using the feature selection process and the detecting methodology. Differentiating the technique performs specifically well by enhancing the detection rate than other available models. From the graphical analysis, the developed HMLT achieved higher accuracy than other models for 15.7% of LSTM, 12.6% of GRU, 9.4% of DBN, and 5.2% of BL by taking the linear activation function. The outcome showed that the developed HMLT strategy can streamline the procedure of the detection and identify the anomalies effectively. From the result, the developed technique can continuously detect the anomaly that is present in the WSN by using the advancement of the model. From the comparison result, it is noted that the HMLT approach achieved better accuracy in detection when compared with other standard techniques.

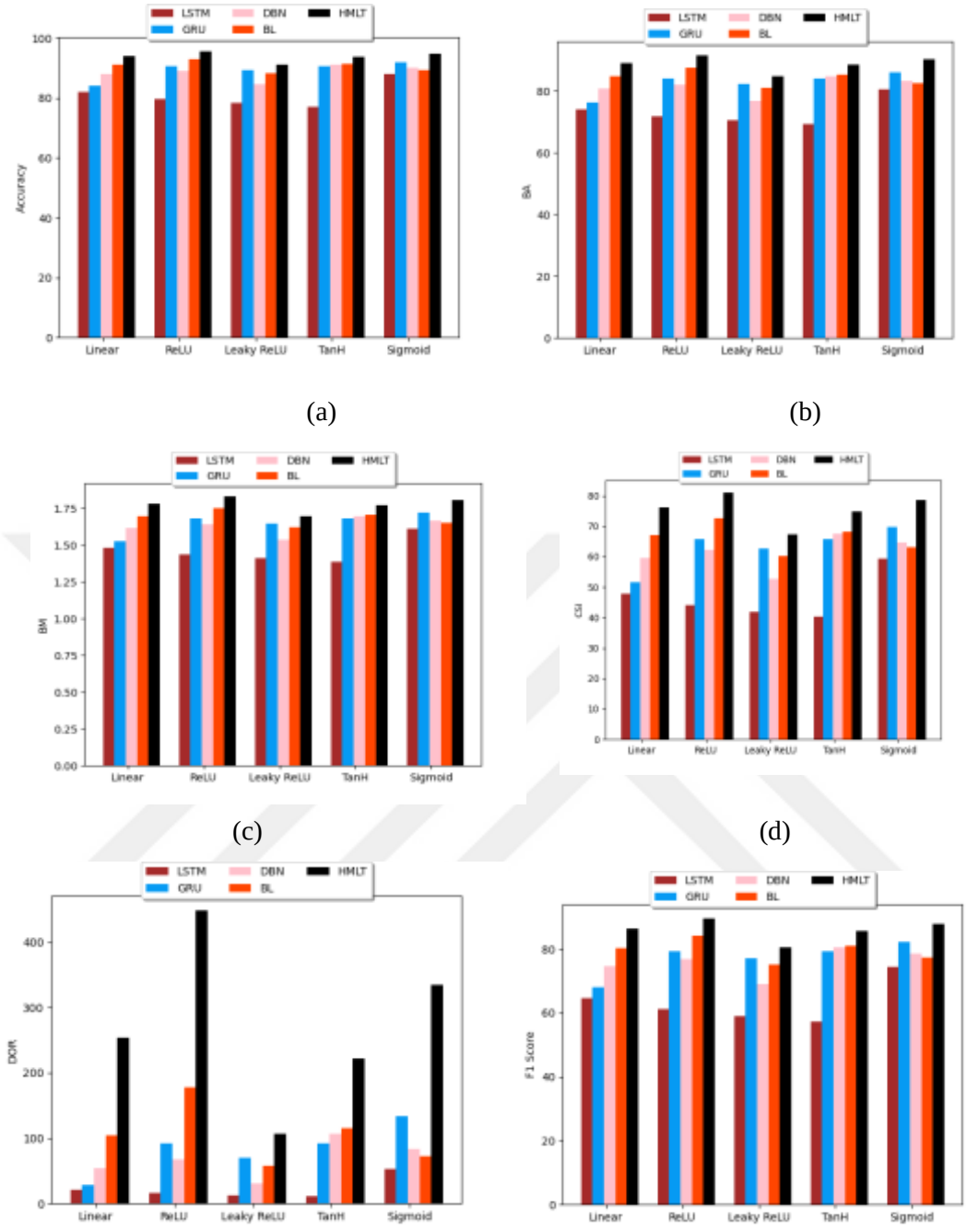


Figure 4.3: Performance Analysis of the Developed HMLT Model for Anomaly Detection in WSN Compared with Other Classifiers Based on Different Activation Functions in Terms of "(a) Accuracy, (b) BA, (c)BM, (d) CSI, (e) DOR, (f) F1-score".

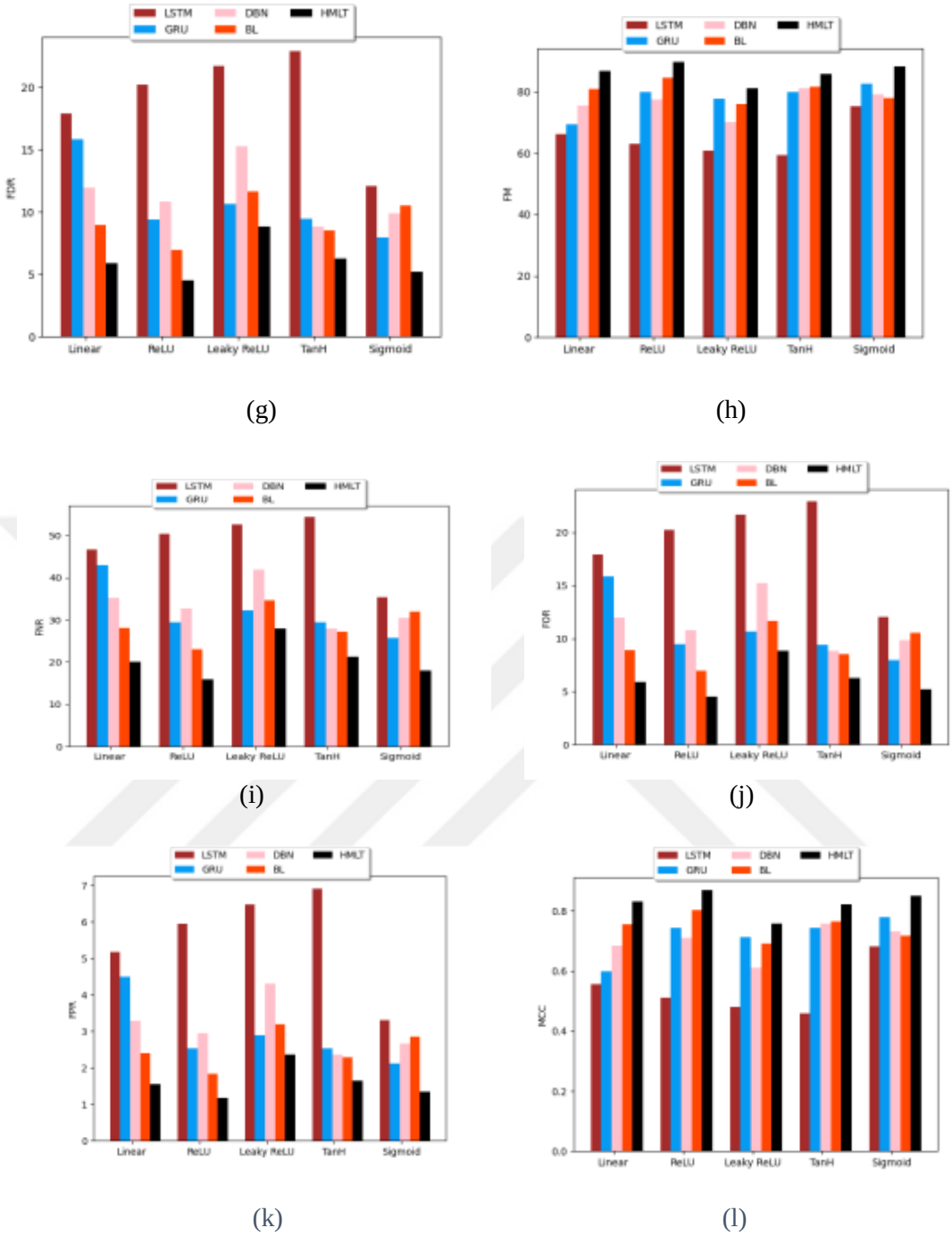
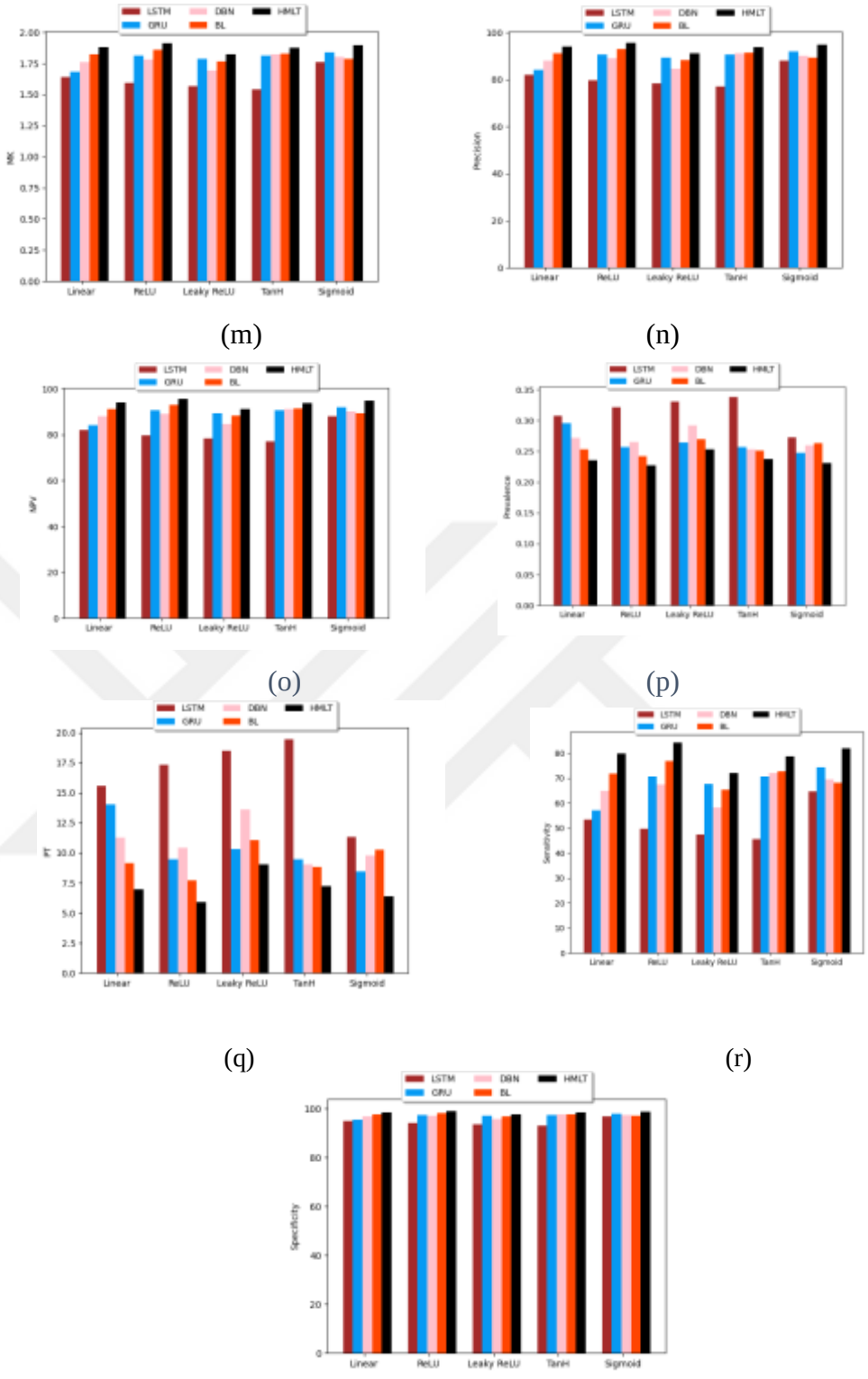


Figure 4.4: Performance Analysis of the Developed HMLT Model for Anomaly Detection in WSN Compared with Other Classifiers Based on Different Activation Functions in Terms of "(g) FDR, (h) FM, (i) FNR, (j) FOR, (k)FPR, (l) MCC".



(m) (n)

(o) (p)

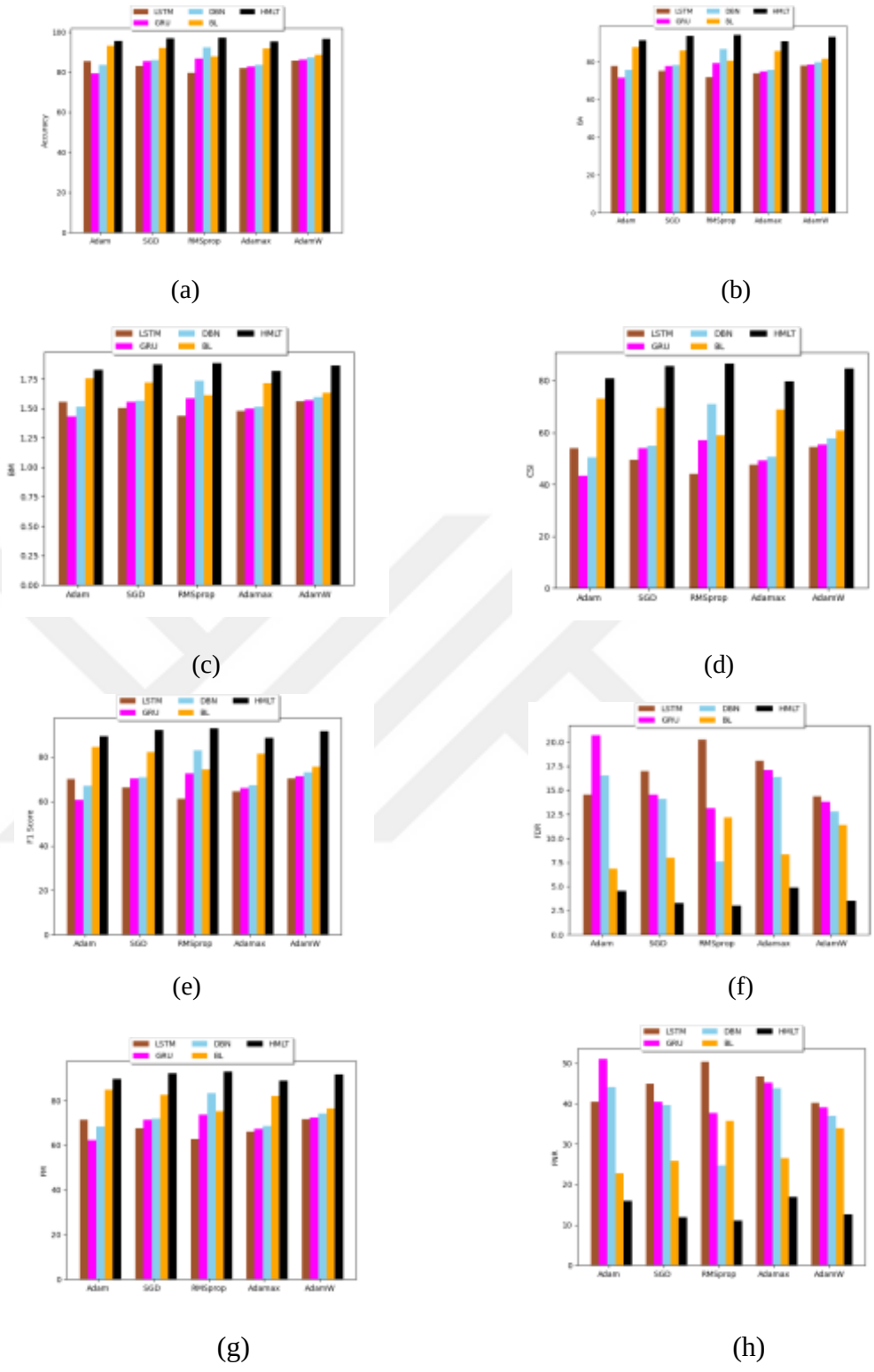
(q) (r)

(s)

Figure 4.5: Performance Analysis of the Developed HMLT Model for Anomaly Detection in WSN Compared with Other Classifiers Based on Different Activation Functions in Terms of "(m) MK, (n) NPV, (o) Precision, (p) Prevalence, (q) PT, (r) Sensitivity and (s) Specificity".

4.6 COMPARATIVE ANALYSIS OF THE SUGGESTED ANOMALY DETECTION SYSTEM BASED ON SEVERAL OPTIMIZERS

The comparative calculations in anomaly detection tasks are significant for enhancing the functionality and security of the WSN system. The Graphical definition of the developed anomaly identification model compared with other available techniques is defined in Figure 10. Multiple performance metrics like FDR, FNR, F1 score, MCC, precision, sensitivity, and PT are employed to determine the reliability of the developed approach. Different optimizers like Adamax, Adam, and RMSprop are used to determine comparative analysis. The effectiveness of the model is clarified by using this analysis regarding the different metrics. The designed HMLT attained higher accuracy than 10.5% of LSTM, 17.8% of GRU, 15.7% of DBN, and 5.2% of BL while taking the Adam optimizer. From the graphical determination, the HMLT achieved higher accuracy, which shows the efficiency of the method in detecting the anomaly and provides great results.



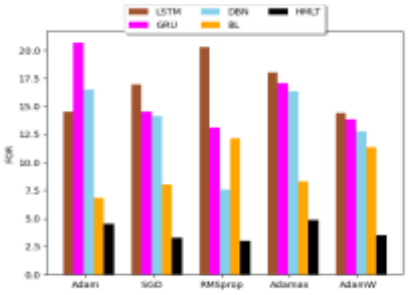
(a) (b)

(c) (d)

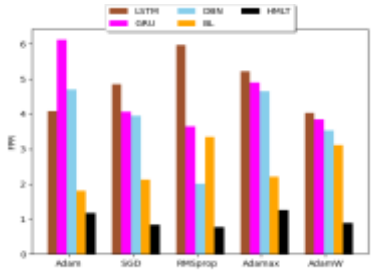
(e) (f)

(g) (h)

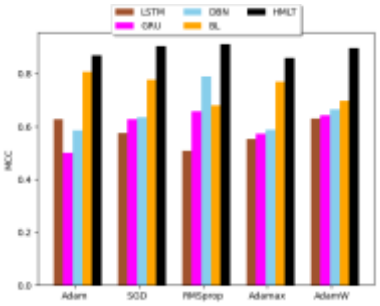
Figure 4.6: Performance Analysis of the Developed HMLT Model for Anomaly Detection in WSN Compared with Other Classifier Based on Various Optimizer in terms of "(a) Accuracy, (b) BA, (c)BM, (d) CSI, (e) F1-score, (f) FDR, (g) FM, (h) FNR"



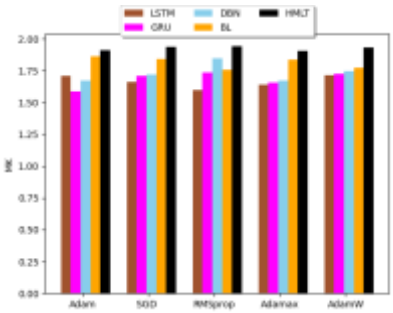
(i)



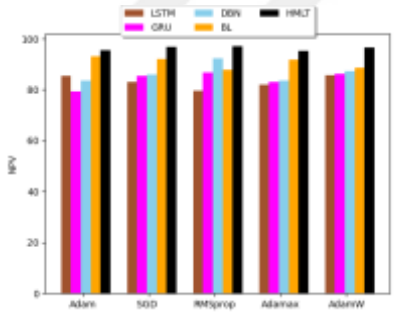
(j)



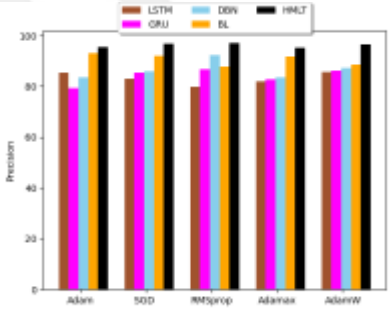
(k)



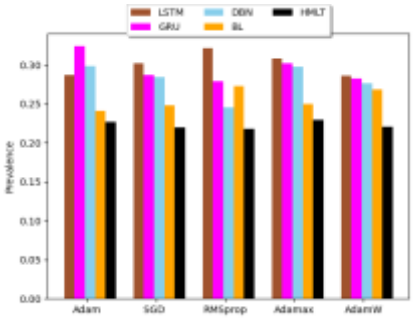
(l)



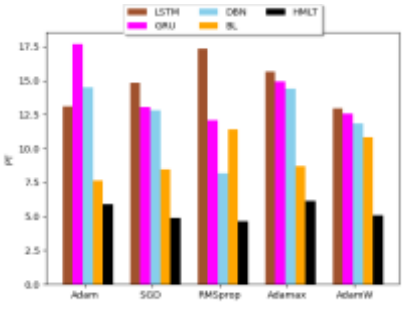
(m)



(n)



(o)



(p)

Figure 4.7: Performance Analysis of the Developed HMLT Model for Anomaly Detection in WSN Compared with Other Classifier Based on Various Optimizer in terms of "(i) FOR, (j)FPR, (k) MCC, (l) MK, (m) NPV, (n) Precision, (o) Prevalence, (p) PT"

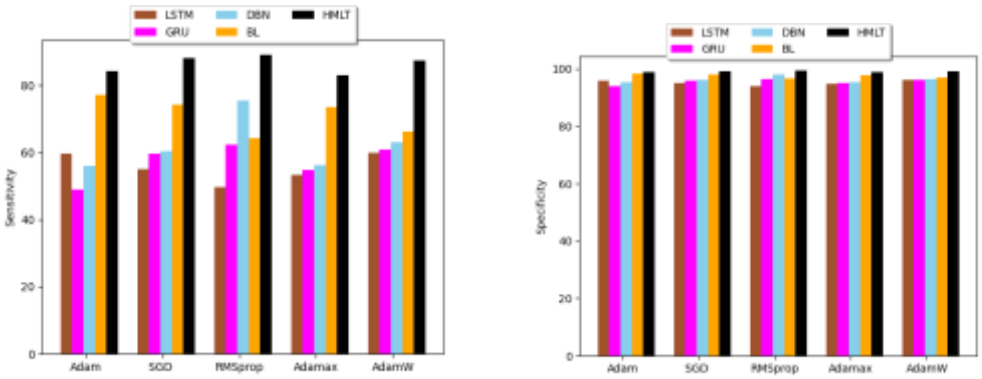


Figure 4.8: Performance Analysis of the Developed HMLT Model for Anomaly Detection in WSN Compared with Other Classifier Based on Various Optimizer in terms of "(q) Sensitivity and (r) Specificity"

4.7 STATISTICAL ANALYSIS OF THE DESIGNED SBOA OPTIMIZATION

The suggested anomaly identification model is statistically determined to assess the security, privacy, and reliability of the model using the different algorithms. The predictive accuracy is determined by this evaluation for anomaly detection to know the feasibility of the model. Determining the key factor that causes anomaly in WSN and enhancing the feature selection process to avoid future attacks of anomaly. These statistical measures are often used to analyze the convergence function of the developed model. Here the HMLT compared with other conventional algorithms based on the statistical performance are defined in Table 2. Some of the performance metrics like the worst, best, and mean median are carried out to analyze the convergence value. The best value of the suggested HMLT is enhanced by 8.2% of BWO, 10.6% of AOA, 12% of GEO, and 8.3% of MRA respectively. Measuring the statistical determination has multiple advantages by knowing the functioning of the model. From the table result, the proposed HMLT achieved higher results than other models.

Table 4.1: Statistical Validation of the Proposed Algorithm For Optimal Feature Selection.

Terms	BWO [36]	AOA [37]	GEO [38]	MRA [39]	SBOA [32]
Best	1.26450543	1.29175	1.307975	1.264972	1.16775
Worst	3.767221193	2.870113	3.241473	3.971282	4.081742
Mean	1.523832991	1.479263	1.3614	1.364943	1.317993
Median	1.26450543	1.29175	1.314171	1.264972	1.16775
Standard deviation	0.483532185	0.432998	0.269089	0.393601	0.491608

4.8 OVERALL COMPARATIVE ANALYSIS OF THE DEVELOPED ANOMALY DETECTION MODEL

The overall comparative analysis of the developed HMLT technique compared with other standard approaches is defined in Table 3. Here the epoch value is used to determine the performance of the model. This validation helps to understand how well the model learns to function in the detection process based on the epoch analysis. The calculation based on varying the epoch is one of the widely used statistical measures because it can determine the temporal evaluation of the analyzed process based on corresponding events that are used to define the epoch. The sensitivity of the HMLT attains a higher value than 23.9% of LSTM, 24.9% of GRU, 18.9% of DBN, and 5.9% of BL respectively. From the table result, it is noted that the developed approach attains a higher sensitivity than other standard models. The outcome of the research revealed that the designed HMLT excels in determining the anomaly in WSN by enhancing its security and reliability without affecting the system model of WSN.

Table 4.2: Performance Validation of the Initiated Anomaly Detection Model.

TERMS	LSTM [5]	GRU [40]	DBN [34]	BL [35]	HMLT
Epoch-100					
Accuracy	88.99239579	88.47401	83.60726	94.1229	95.66408
Sensitivity	66.89839197	65.74498	56.04506	80.01311	84.65528
Specificity	97.0021893	96.84238	95.32783	98.464	98.87851
Precision	88.99912187	88.4605	83.60918	94.12696	95.65981
FPR	2.997810702	3.157622	4.672172	1.535996	1.121494
FNR	33.10160803	34.25502	43.95494	19.98689	15.34472
NPV	88.99071427	88.47738	83.60678	94.12189	95.66515
FDR	11.00087813	11.5395	16.39082	5.873043	4.34019
F1 Score	76.38220768	75.42966	67.1069	86.49808	89.82175
MCC	0.705945881	0.693926	0.587629	0.832197	0.873425
FOR	11.00928573	11.52262	16.39322	5.878114	4.334852
PT	10.58435183	10.95768	14.43646	6.927626	5.754948
CSI	61.78900808	60.55187	50.49691	76.20847	81.52403
BA	81.95029063	81.29368	75.68645	89.23856	91.7669
FM	77.16150685	76.26161	68.4535	86.78359	89.98949
BM	1.639005813	1.625874	1.513729	1.784771	1.835338
MK	1.779898361	1.769379	1.67216	1.882488	1.91325
LR+	22.31574926	20.82104	11.99551	52.09201	75.48439
LR-	0.341245989	0.353719	0.461092	0.202987	0.155188
DOR	65.39490566	58.86317	26.01541	256.6277	486.4075
Prevalence	0.26607253	0.269102	0.298364	0.235279	0.225998
Epoch-200					
Accuracy	82.1086262	92.53939	89.91376	92.02522	94.31646
Sensitivity	53.43012704	75.61262	69.02884	74.26009	80.57471
Specificity	94.83526139	98.02593	97.27053	97.87889	98.5172
Precision	82.11369745	92.54579	89.90768	92.02292	94.3218
FPR	5.164738615	1.974073	2.729474	2.121111	1.482796
FNR	46.56987296	24.38738	30.97116	25.73991	19.42529
NPV	82.10735839	92.53779	89.91528	92.02579	94.31513
FDR	17.88630255	7.454205	10.09232	7.977078	5.6782
F1 Score	64.73692628	83.22664	78.09687	82.19277	86.90799
MCC	0.556745382	0.791545	0.727476	0.778665	0.837285
FOR	17.89264161	7.462213	10.08472	7.974209	5.684872

Table 4.2: Performance Validation of the Initiated Anomaly Detection Model "Table Continued".

PT	15.5453704	8.078942	9.942467	8.450335	6.782836
CSI	47.86001419	71.27194	64.0647	69.76886	76.84715
BA	74.13269421	86.81927	83.14968	86.06949	89.54596
FM	66.23703863	83.65184	78.77958	82.66578	87.1777
BM	1.482653884	1.736385	1.662994	1.72139	1.790919
MK	1.642210558	1.850836	1.79823	1.840487	1.886369
LR+	10.34517543	38.30285	25.29016	35.01	54.33972
LR-	0.491060733	0.248785	0.318402	0.262977	0.197177
DOR	21.06699791	153.9596	79.42833	133.1295	275.5891
Prevalence	0.307368528	0.244789	0.260493	0.24784	0.234123
Epoch-300					
Accuracy	80.51849539	85.76164	91.56416	92.50827	96.82652
Sensitivity	50.81813113	60.09457	73.0706	75.53351	88.40995
Specificity	94.29552019	96.01179	97.74926	98.01479	99.18714
Precision	80.51571954	85.74978	91.56678	92.50522	96.82593
FPR	5.704479814	3.988209	2.250737	1.985208	0.812862
FNR	49.18186887	39.90543	26.9294	24.46649	11.59005
NPV	80.51918935	85.7646	91.56351	92.50903	96.82666
FDR	19.48428046	14.25022	8.433224	7.494775	3.174069
F1 Score	62.30927324	70.6657	81.27971	83.16231	92.42675
MCC	0.524738754	0.633436	0.767286	0.790737	0.905742
FOR	19.48081065	14.2354	8.436493	7.490972	3.173335
PT	16.75207788	12.88076	8.775281	8.105937	4.794329
CSI	45.25306439	54.63802	68.4632	71.17764	85.91983
BA	72.55682566	78.05318	85.40993	86.77415	93.79854
FM	63.96607221	71.78507	81.79755	83.58974	92.5223
BM	1.451136513	1.561064	1.708199	1.735483	1.875971
MK	1.610349089	1.715144	1.831303	1.850143	1.936526
LR+	8.908460155	15.06806	32.46519	38.04815	108.7638
LR-	0.521571638	0.41563	0.275495	0.24962	0.11685
DOR	17.0800318	36.2535	117.8433	152.4241	930.7955
Prevalence	0.316877924	0.285383	0.250625	0.244938	0.219039
Epoch-400					
Accuracy	85.35871094	84.42512	87.14945	91.40327	95.65848
Sensitivity	59.31099474	57.54121	62.90317	72.66042	84.6374

Table 4.2: Performance Validation of the Initiated Anomaly Detection Model "Table Continued".

Specificity	95.88266861	95.58785	96.4408	97.70471	98.87714
Precision	85.33741169	84.41177	87.13424	91.41117	95.65474
FPR	4.117331391	4.412152	3.559203	2.295288	1.122856
FNR	40.68900526	42.45879	37.09683	27.33958	15.3626
NPV	85.36403575	84.42846	87.15325	91.40129	95.65941
FDR	14.66258831	15.58823	12.86576	8.588831	4.345261
F1 Score	69.98275198	68.4333	73.06204	80.96434	89.80945
MCC	0.62468167	0.604766	0.663966	0.763355	0.873273
FOR	14.63596425	15.57154	12.84675	8.598707	4.340591
PT	13.17377714	13.84541	11.89351	8.886682	5.759051
CSI	53.82574469	52.01415	57.55728	68.01688	81.50376
BA	77.59683167	76.56453	79.67198	85.18257	91.75727
FM	71.14384566	69.6933	74.03391	81.49831	89.9776
BM	1.551936633	1.531291	1.59344	1.703651	1.835145
MK	1.707014474	1.688402	1.742875	1.828125	1.913141
LR+	14.40520306	13.04153	17.67338	31.65634	75.37689
LR-	0.424362461	0.444186	0.384659	0.279818	0.155371
DOR	33.94551678	29.36051	45.94557	113.1317	485.1426
Prevalence	0.287762537	0.293396	0.277042	0.251612	0.226034
Epoch-500					
Accuracy	88.76018587	88.37648	90.63591	94.84387	96.49529
Sensitivity	66.37771182	65.52352	70.75556	82.14508	87.31166
Specificity	96.93158367	96.82035	97.4843	98.65608	99.10137
Precision	88.76103998	88.39111	90.64434	94.83186	96.50004
FPR	3.068416328	3.179646	2.5157	1.343925	0.898633
FNR	33.62228818	34.47648	29.24444	17.85492	12.68834
NPV	88.75997235	88.37282	90.6338	94.84687	96.4941
FDR	11.23896002	11.60889	9.355658	5.168139	3.499964
F1 Score	75.95464917	75.25856	79.47454	88.03374	91.6762
MCC	0.70055697	0.691792	0.744742	0.851243	0.896432
FOR	11.24002765	11.62718	9.3662	5.153125	3.505903
PT	10.75018674	11.0144	9.42799	6.395385	5.072536
CSI	61.23135503	60.33164	65.94004	78.62523	84.63163
BA	81.65464775	81.17194	84.11993	90.40058	93.20652
FM	76.7577666	76.10319	80.0849	88.26081	91.79095

Table 4.2: Performance Validation of the Initiated Anomaly Detection Model "Table Continued".

BM	1.633092955	1.623439	1.682399	1.808012	1.86413
MK	1.775210123	1.767639	1.812781	1.896787	1.929941
LR+	21.63256375	20.60717	28.1256	61.12327	97.16051
LR-	0.34686618	0.356087	0.299991	0.180981	0.128034
DOR	62.36573347	57.87115	93.75472	337.7322	758.8655
Prevalence	0.267442301	0.2698	0.256218	0.230889	0.221047

5. CONCLUSION

In this paper, the anomaly detection framework was presented to detect anomalous events in the WSN system using efficient machine learning models. At first, the needed data information was collected from the available resources. The dataset contained the attack details that happened in the WSN. The collected data were sent to optimal feature selection. The feature selection employs SBOA for the optimization of the extracted feature from the given data. Here the relevant features from the given original data get taken out by eliminating the unnecessary information. Further, the feature was optimally tuned using the SBOS for the optimal selection of features. This helps to improve the ability to identify anomalies. Further, the HMLT framework was designed to meet the requirement of high detection ability. The resultant optimal feature was given to HMLT for detecting the anomaly. The HMLT was constructed by the combination of the DBN and BL model. The feature passed towards the DBN model which performs the probabilistic behavior and offered the feature. These features were given to the BL model for detecting the anomalous event in the given feature. The outcome from the developed hybrid model detected the anomaly with high accuracy. From Table IV, the accuracy of the developed HMLT has enhanced by 8.01% of LSTM, 8.4% of GRU, 6.0% of DBN, and 1.7% of BL. From the result, it was noted that the HMLT achieved a better result in detecting the anomaly present in the WSN.

5.1 FUTURE SCOPE

For the future enhancement of anomaly detection in WSN, some of the modifications can be included in this technique, which are listed as follows.

The implemented model does not utilize the high dimensional dataset, which includes the different possible types of attacks in WSN. This resulted in the limited performance of the designed anomaly detection model. Hence the technique will be trained using a huge range of data in future for the effective analysis.

a. In the future, it will be better to implement additional functionality for the feature extraction process, which includes the enhanced concept in the optimization algorithm to present the efficient feature set for further analysis.

b. The implementation of security features in the WSN will be considered in the future by exploring multiple security mechanisms. It is to enhance the integrity and confidentiality of the data, by ensuring the proposed detection system will be resilient against the attack.
c. Future research will explore advanced methods to detect the complex anomaly pattern by initiating the effective deep learning model, which has the potential to perform significantly improved anomaly detection in the WSN.

REFERENCES

[1] I. Gethzi Ahila Poornima, B. Paramasivan, "Anomaly detection in wireless sensor network using machine learning algorithm", Computer Communications, Vol. 151, pp.331-337, 2020.

[2] B. Bertalanič, J. Hribar and C. Fortuna, "Visibility Graph-Based Wireless Anomaly Detection for Digital Twin Edge Networks," IEEE Open Journal of the Communications Society, vol. 5, pp. 3050-3065, 2024.

[3] M. Matar, T. Xia, K. Huguenard, D. Huston and S. Wshah, "Anomaly Detection in Coastal Wireless Sensors via Efficient Deep Sequential Learning," IEEE Access, vol. 11, pp. 110260-110271, 2023.

[4] C. Yao, Y. Yang, K. Yin and J. Yang, "Traffic Anomaly Detection in Wireless Sensor Networks Based on Principal Component Analysis and Deep Convolution Neural Network," IEEE Access, vol. 10, pp. 103136-103149, 2022.

[5] Suriyan Kannadhasan, Ramalingam Nagarajan, "Intrusion detection in machine learning based E-shaped structure with algorithms, strategies and applications in wireless sensor networks", Vol.10, issue.9, May 03, 2024.

[6] Syed Muhammad Salman Bukhari, Muhammad Hamza Zafar, Mohamad Abou Houran, Syed Kumayl Raza Moosavi, Majad Mansoor, Muhammad Muaaz, Filippo Sanfilippo, "Secure and privacy-preserving intrusion detection in wireless sensor networks: Federated learning with SCNN-Bi-LSTM for enhanced reliability", Ad Hoc Networks, Vol. 155, no.103407, 15 March 2024.

[7] Mohit Mittal, Martyna Kobielnik, Swadha Gupta, Xiaochun Cheng & Marcin Wozniak, "An efficient quality of services based wireless sensor network for anomaly detection using soft computing approaches", Journal of Cloud Computing, Vol. 11, no.70, 2022.

[8] S. Gayathri & D. Surendran, "Unified ensemble federated learning with cloud computing for online anomaly detection in energy-efficient wireless sensor networks", Journal of Cloud Computing, Vol. 13, no.49, 2024.

[9] A. Fascista, A. Coluccia and C. Ravazzi, "A Unified Bayesian Framework for Joint Estimation and Anomaly Detection in Environmental Sensor Networks," IEEE Access, vol. 11, pp. 227-248, 2023.

[10] G. Cerar, H. Yetgin, B. Bertalanic and C. Fortuna, "Learning to Detect Anomalous Wireless Links in IoT Networks," IEEE Access, vol. 8, pp. 212130-212155, 2020.

[11] K. Zhang, K. Yang, S. Li, D. Jing, and H. -B. Chen, "ANN-Based Outlier Detection for Wireless Sensor Networks in Smart Buildings," IEEE Access, vol. 7, pp. 95987-95997, 2019.

[12] A. Siva Kumar, S. Raja, N. Pritha, Havaldar Raviraj, R. Babitha Lincy, J. Jency Rubia, "An adaptive transformer model for anomaly detection in wireless sensor networks in real-time", Measurement: Sensors, Vol.25, no.100625, February 2023.

[13] Vaishnavi Sivagaminathan, Manmohan Sharma & Santosh Kumar Henge, "Intrusion detection systems for wireless sensor networks using computational intelligence techniques", Cybersecurity, vol.6, no.27, 2023.

[14] Xiong Yang, Yuling Chen, Xiaobin Qian, Tao Li, Xiao Lv, "BCEAD: A Blockchain-Empowered Ensemble Anomaly Detection for Wireless Sensor Network via Isolation Forest", Security and Communication Networks, 10 November 2021.

[15] Biao Lu, Wansu Liu, "Nonuniform Clustering of Wireless Sensor Network Node Positioning Anomaly Detection and Calibration", Journal of Sensors, 16 October 2021.

[16] Gebrekiros Gebreyesus Gebremariam, J. Panda &S. Indu, "Design of advanced intrusion detection systems based on hybrid machine learning techniques in hierarchically wireless sensor networks", Connection Science, no. 2246703, 22 Aug 2023.

[17] Qinghao Zhang, Miao Ye &Xiaofang Deng, "A novel anomaly detection method for multimodal WSN data flow via a dynamic graph neural network", Connection Science, Vol.34, issue.1, 14 Jun 2022.

[18] Z. -M. Wang, G. -H. Song and C. Gao, "An Isolation-Based Distributed Outlier Detection Framework Using Nearest Neighbor Ensembles for Wireless Sensor Networks," IEEE Access, vol. 7, pp. 96319-96333, 2019.

[19] N. Berjab, H. H. Le and H. Yokota, "Recovering Missing Data via Top-k Repeated Patterns for Fuzzy-Based Abnormal Node Detection in Sensor Networks," IEEE Access, vol. 10, pp. 61046-61064, 2022.

[20] D. Arnaiz, E. Alarcón, F. Moll and X. Vilajosana, "On Anomaly-Aware Structural Health Monitoring at the Extreme Edge," IEEE Access, vol. 11, pp. 90227-90253, 2023.

[21] W. Wang, O. Abbasi, H. Yanikomeroglu, C. Liang, L. Tang, and Q. Chen, "A Vertical Heterogeneous Network (VHetNet)-Enabled Asynchronous Federated Learning-Based Anomaly Detection Framework for Ubiquitous IoT," IEEE Open Journal of the Communications Society, vol. 5, pp. 332-348, 2024.

[22] W. Meng, W. Li, C. Su, J. Zhou, and R. Lu, "Enhancing Trust Management for Wireless Intrusion Detection via Traffic Sampling in the Era of Big Data," IEEE Access, vol. 6, pp. 7234-7243, 2018.

[23] G. Sivapalan, K. K. Nundy, S. Dev, B. Cardiff, and D. John, "ANNet: A Lightweight Neural Network for ECG Anomaly Detection in IoT Edge Sensors," IEEE Transactions on Biomedical Circuits and Systems, vol. 16, no. 1, pp. 24-35, Feb. 2022.

[24] A. Shahnejat Bushehri, A. Amirnia, A. Belkhiri, S. Keivanpour, F. G. de Magalhães and G. Nicolescu, "Deep Learning-Driven Anomaly Detection for Green IoT Edge Networks," IEEE Transactions on Green Communications and Networking, vol. 8, no. 1, pp. 498-513, March 2024.

[25] Y. Du, J. Xia, J. Ma, and W. Zhang, "An Optimal Decision Method for Intrusion Detection System in Wireless Sensor Networks with Enhanced Cooperation Mechanism," IEEE Access, vol. 9, pp. 69498-69512, 2021.

[26] Priyajit Biswas & Tuhina Samanta, "Anomaly detection using ensemble random forest in wireless sensor network", International Journal of Information Technology, Vol. 13, pp. 2043-2052, 2021.

[27] Yang Zhang, Nirvana Meratnia, Paul J.M. Havinga, "Distributed online outlier detection in wireless sensor networks using ellipsoidal support vector machine", Ad Hoc Networks, Vol. 11, Issue 3, pp.1062-1074, May 2013.

[28] Ahod Alghuried, "A Model for Anomalies Detection in Internet of Things (IoT) Using Inverse Weight Clustering and Decision Tree", Computer and Information Science, vol. 103, 2017.

[29] M. Revanesh, Sheetal S. Gundal, J. R. Arunkumar, P. Joel Josephson, S. Suhasini & T. Kalavathi Devi, "Artificial neural networks-based improved Levenberg–

Marquardt neural network for energy efficiency and anomaly detection in WSN", Wireless Networks, vol. 30, pp. 5613-5628, 2024.

[30] M. Xie, J. Hu, S. Han and H. -H. Chen, "Scalable Hypergrid k-NN-Based Online Anomaly Detection in Wireless Sensor Networks," IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 8, pp. 1661-1670, Aug. 2013.

[31] Mnahi Alqahtani, Abdu Gumaei, Hassan Mathkour, and Mohamed Maher Ben Ismail, "A Genetic-Based Extreme Gradient Boosting Model for Detecting Intrusions in Wireless Sensor Networks", vol. 19, no.4383, 2019.

[32] Youfa Fu, Dan Liu, Jiadui Chen & Ling He, "Secretary bird optimization algorithm: a new metaheuristic for solving global optimization problems", Artificial Intelligence Review, Vol.57, no.123, 2024.

[33] Seung-Ho Kang & Kuinam J. Kim, "A feature selection approach to find optimal feature subsets for the network intrusion detection system", Cluster Computing, vol.19, pp.325-333, 2016.

[34] Y. Zhang, P. Li, and X. Wang, "Intrusion Detection for IoT Based on Improved Genetic Algorithm and Deep Belief Network," IEEE Access, vol. 7, pp. 31711-31722, 2019.

[35] Andrew Kirk, Jonathan Legg, and Edwin El-Mahassni, "Anomaly Detection and Attribution Using Bayesian Networks", Defence Science and Technology, no.2975, 2017.

[36] VahidehHayyolalam, and Ali AsgharPourhaji Kazem, "Black Widow Optimization Algorithm: A novel meta-heuristic Approach for solving engineering optimization problems", Engineering Applications of Artificial Intelligence, vol.87, January 2020.

[37] Fatma A. Hashim, Kashif Hussain, Essam H. Houssein, Mai S. Mabrouk and Walid Al-Atabany, "Archimedes optimization algorithm: a new metaheuristic algorithm for solving optimization problems", Applied Intelligence, Vol. 51, pp. 1531-1551, 2021.

[38] Abdolkarim Mohammadi-Balani, Mahmoud Dehghan Nayeri, Adel Azar, Mohammadreza Taghizadeh-Yazdi, "Golden eagle optimizer: A nature-inspired metaheuristic algorithm", Computers & Industrial Engineering, Vol. 152, pp.107050, February 2021.

[39] A. S. Desuky, M. A. Cifci, S. Kausar, S. Hussain and L. M. El Bakrawy, "Mud Ring Algorithm: A New Meta-Heuristic Optimization Algorithm for Solving

Mathematical and Engineering Challenges," IEEE Access, vol. 10, pp. 50448-50466, 2022.

[40] Zhou Jingjing, Yang Tongyu, Zhang Jilin, Zhang Guohao, Li Xuefeng, Pan Xiang, "Intrusion Detection Model for Wireless Sensor Networks Based on MC-GRU", Wireless Communications and Mobile Computing, 2022.

[41] Iman Almomani, Bassam Al-Kasasbeh, Mousa AL-Akhras,"WSN-DS: A Dataset for Intrusion Detection Systems in Wireless Sensor Networks", Journal of sensors, 2016.

[42] Satish R. Jondhale, R. Maheswar & Jaime Lloret, "Fundamentals of Wireless Sensor Networks", Received Signal Strength Based Target Localization and Tracking Using Wireless Sensor Networks, pp.1-19, 2021.

[43] S. Ullo; M. Gallo; G. Palmieri; P. Amenta; M. Russo; G. Romano; M. Ferrucci; A. Ferrara; M. De Angelis, "Application of wireless sensor networks to environmental monitoring for sustainable mobility," IEEE Environmental Engineering (EE), Milan, Italy, pp. 1-7, 2018.

[44] Wu, M., Tan, L. and Xiong, N., "Data prediction, compression, and recovery in clustered wireless sensor networks for environmental monitoring applications", Information Sciences, 329, pp.800-818, 2016.

[45] Shalli Rani, Syed Hassan Ahmed & Ravi Rastogi, "Dynamic clustering approach based on wireless sensor networks genetic algorithm for IoT applications", Wireless Networks, vol.26, pp. 2307-2316, 2020.

[46] N. R. Patel and S. Kumar, "Wireless Sensor Networks' Challenges and Future Prospects," System Modeling & Advancement in Research Trends (SMART), Moradabad, India, pp. 60-65, 2018.

[47] Hitesh Mohapatra, Amiya Kumar Rath, "Fault-tolerant mechanism for wireless sensor network", vol.10, pp.23-30, 2020.

[48] Rizwan, R., Khan, F.A., Abbas, H. and Chauhdary, S.H., "Anomaly detection in wireless sensor networks using immune-based bioinspired mechanism", International journal of distributed sensor networks, vol.11(10), pp.684952, 2015.

[49] Anton Kanev; Aleksandr Nasteka; Catherine Bessonova; Denis Nevmerzhitsky; Aleksei Silaev, "Anomaly detection in wireless sensor network of the "smart home" system," Open Innovations Association (FRUCT), St. Petersburg, Russia, 2017, pp. 118-124, 2017.

[50] Mohammad GhasemiGol, Abbas Ghaemi-Bafghi, Mohammad Hossein Yaghmaee-Moghaddam & Hadi Sadoghi-Yazdi, "Anomaly detection and foresight response strategy for wireless sensor networks", vol.21, pp. 1425-1442, 2015.

[51] C. Gao, Y. Chen, Z. Wang, H. Xia and N. Lv, "Anomaly detection frameworks for outlier and pattern anomaly of time series in wireless sensor networks," Networking and Network Applications, pp. 229-232, 2020.

[52] Ifzarne, S., Tabbaa, H., Hafidi, I. and Lamghari, N., "Anomaly detection using machine learning techniques in wireless sensor networks", In Journal of Physics, Vol. 1743, No. 1, pp. 012021, 2021.

[53] Yu, X., Lu, H., Yang, X., Chen, Y., Song, H., Li, J. and Shi, W., "An adaptive method based on contextual anomaly detection in internet of things through wireless sensor networks" International Journal of Distributed Sensor Networks, vol.16(5), pp.15501, 2020.

[54] Saeedi Emadi, H. and Mazinani, S.M., "A novel anomaly detection algorithm using DBSCAN and SVM in wireless sensor networks. Wireless Personal Communications, 98, pp.2025-2035, 2018.

[55] T. Luo and S. G. Nagarajan, "Distributed Anomaly Detection Using Autoencoder Neural Networks in WSN for IoT," Communications system, 2018.

[56] Ding, Z.G., Du, D.J. and Fei, M.R., "An isolation principle based distributed anomaly detection method in wireless sensor networks", International Journal of Automation and Computing, vol.12(4), pp.402-412, 2015.

[57] Wazid, M. and Das, A.K., "An efficient hybrid anomaly detection scheme using K-means clustering for wireless sensor networks", Wireless Personal Communications, vol.90, pp.1971-2000, 2016.

[58] Cauteruccio, F., Fortino, G., Guerrieri, A., Liotta, A., Mocanu, D.C., Perra, C., Terracina, G. and Vega, M.T., "Short-long term anomaly detection in wireless sensor networks based on machine learning and multi-parameterized edit distance", Information Fusion, vol.52, pp.13-30, 2019.

[59] Shanmuganathan V, Suresh A., "LSTM-Markov based efficient anomaly detection algorithm for IoT environment", Applied Soft Computing, Vol.136, , pp.110054, March 2023.

[60] Wen, W., Shang, C., Dong, Z., Keh, H.C. and Roy, D.S., "An intrusion detection model using improved convolutional deep belief networks for wireless sensor networks, International Journal of Ad Hoc and Ubiquitous Computing, vol.36(1), pp.20-31, 2021.