Journal of Robotics and Control (JRC)
Volume 4, Issue 6, 2023
ISSN: 2715-5072, DOI: 10.18196/jrc.v4i6.20216

Enhancing Fault Detection in Wireless Sensor Networks Through Support Vector Machines: A Comprehensive Study

Yerik Mardenov [1], Aigul Adamova [2*], Tamara Zhukabayeva [2, 3], Mohamed Othman [4, 5]
[1] Dept. of Information Technology and Engineering, Astana International University, Astana, Kazakhstan
[2] Dept. of Computer Engineering, Astana IT University, Astana, Kazakhstan
[3] Dept. of Information Systems, L. Gumilyov Eurasian National University, Astana, Kazakhstan
[4] Dept. of Communication Tech and Networks, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor D.E., Malaysia
[5] Lab of Computational Science and Mathematical Physics, Institute for Mathematical Research, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor D.E., Malaysia
Email: [1] emardenov@gmail.com, [2] aigul.adamova@astanait.edu.kz, [3] tamara_kokenovna@mail.ru, [4] mothman@upm.edu.my
*Corresponding Author

***Abstract*—The Wireless Sensor Network (WSN) consists of many sensors that are distributed in a specific area for the purpose of monitoring physical conditions. Factors such as hardware limitations, limited resources, unfavourable WSN deployment environment, and the presence of various attacks on nodes can lead to the presence of Faulty Nodes in a WSN. This raises the problem of detecting Faulty Nodes and avoiding Data loss. Detecting Faulty Nodes in real-world scenarios will improve the quality of a WSN. The research was aimed at developing an algorithm to determine the location of Faulty Nodes in a WSN. The algorithm uses characteristics of Machine Learning and Support Vector Machines (SVM), which use the classification of Data into true and false. A Mathematical Model for determining Faulty Nodes using the SVM is considered. A methodology for detecting a Faulty Node is demonstrated, which consists of Data Collection, Feature Extraction, Training, and Testing the Model. The Results of simulated experiments that were conducted with different numbers of nodes from 50 to 320 are shown. The Model is tested on Data very similar to real-world sensing Data to evaluate the ability of the Model to detect failed nodes and calculate training and testing errors. As a result, the training error is 4.6667%, the accuracy of detecting faulty nodes was 97%. The simulation results demonstrate the high stability of the proposed algorithm and are suitable for network environments with irregular node distribution or coverage gaps. In real scenarios, it can provide a high level of uninterrupted operation of the WSN and lossless data transmission. Shortcomings and prospects in research on fault detection in WSN, such as studying real-world hardware issues and its security, were presented.**

Keywords—Wireless Sensor Network; SVM; Faulty Node Detection; Attacked Node; Machine Learning.

I. INTRODUCTION

Today, Wireless Sensor Networks (WSN) act as a core component of the concept of the Internet of Things [1]. WSNs are growing rapidly due to rapid deployment and low cost, as well as deployment and use in environments where there are difficulties in using cable networks. WSN technologies are used in various fields, for example, science, agro-industry [2], medicine [3], military affairs, industry, robotics and much more [4]. As in all communication networks, WSNs have an important place to deal with the issue of ensuring the quality of network changes, which is the main one by reducing overhead costs [5], minimising delay time during data transmission [6], localising network nodes [7], saving energy [8], reducing losses and delays during packet transport [9].

Connectivity is one of the main indicators of network functioning quality, which is defined as the ability of each node to determine the path for data transmission [10]. Each node will expand with a limited Radius, and can find other nodes within the node's connection Radius. Node link Radius, Antennas, and Network node locations are all factors in whether there is connectivity between two nodes and are characterised by the connectivity probability [11]. It is important to note that through the probability of connection, it is possible to obtain the physical possibility of data delivery. However, this capability is not a sufficient condition for successful data delivery, which is also noted in the papers [12]-[17]. The quality of each of the channels on each leg of the route affects the actual probability of data delivery. data delivery may not be possible if the network is overloaded with traffic, and there are also malfunctions due to interference between nodes or third-party interference [18]-[20].

A decrease in network performance is a sign of the presence of faulty sensor nodes, resulting in an increased packet loss and delay time in the wireless sensor network as congestion occurs due to limited bandwidth. The authors of [21]-[26] consider various approaches for localising failed nodes. Identifying failed sensor nodes can improve network performance. Thus, one of the important areas of research in WSN is the continuous diagnosis of sensory nodes and obtaining their status. This helps to ensure continuous network service despite the failure of individual nodes in the network [27]-[31]. This article discusses some pressing issues associated with distributed fault diagnosis for intermittent sensor failures in WSNs. In other words, diagnosing WSN failures is critical for maintaining network quality. There are traditional methods for detecting a faulty sensor node, but their performance is low under various conditions, for example, when deploying a network in

adverse conditions [32]-[34]. In this regard, Machine Learning algorithms have achieved good performance as a method of using experience to improve the performance of the system itself in order to establish an efficient, accurate, and reliable method for self-detection of nodes [35]-[38].

In recent years, various classifications of faults have been proposed in the WSN. The main malfunction of the WSN is a node in which at least one of the main parameters goes beyond the established operating norm. One of the reasons for failure, after which the object goes into an inoperable state, may be the presence of errors due to different software. To solve such problems, various fault detection methods are used [39]-[42].

Featured learning with a teacher occurs using labelled inputs. Algorithms such as Random Forest, and Logistic Regression, and their behaviour with a range of predictor variables and sample sizes are among the main supervised learning algorithms [43]-[46].

The Research presents an algorithm for determining Faulty Nodes in a WSN. Contribution of the study is the methodology for detecting a Faulty Node based on a mathematical model using the SVM and k-Nearest Neighbors (kNN); modelling to achieve high algorithm stability for network environments with uneven distribution of nodes or coverage gaps.

The research paper is organised as follows: **Section II** presents a research methodology, such as systematic scientific literature review of fault detection in WSNs and introduces a mathematical description of the SVM. An analysis of experimental studies and a description of the software implementation are given in **Section III**. Finally, this article concludes and explains further research in **Section IV**.

II. RESEARCH METHODOLOGY

A. Survey Methodology

In this section, we briefly show a Survey methodology on the fault node detection in WSN described in this work.

This work is devoted to the study of methods for detecting node defects for WSNs based on Machine Learning - SVM, identifying gaps and problems, as shown in Fig. 1. The search methodology was based on the results of a number of studies, first of all, keywords were identified before the main meaning and content, as a result of which a search and study of works in the databases of Google Scholar, IEEE Xplore, Springer link, Web of Science, Scopus and Science Direct was carried out by key words: "Wireless Sensor Network", "Node Attacks", "Faulty Node Detection", "IoT Security", "Machine Learning", "Support Vector Machine" for 2022-2023. At the third stage, an analysis of the works was carried out, repetitions were excluded, and at the next stage, research papers were selected regarding the direction of the study. At the final stage, works with open access were selected for the analysis of the proposed solutions, if there were not enough works, then it would be necessary to repeat all the steps starting from the first one.

As a result, 81 papers were selected from the above databases, reflecting current issues and methods in the area of work.

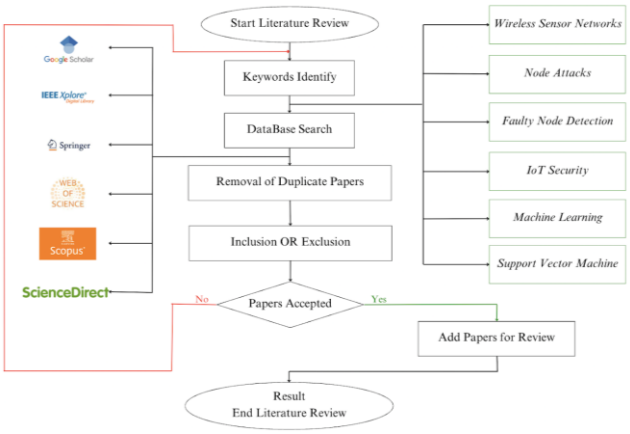

Fig. 1. Methodology of research

B. Geographical Distribution of Publication

When working with the literature, the number of publications by country for 2022-2023 was analysed by searching for a study, and then the country mentioned in the affiliation of the first author was selected. At the next stage, the number of works by country was summarised. A total of 484 articles were selected, the results are shown in Fig. 2. The Fig. 3 also shows a map with the geographical location of the countries with the largest number of publications on determining faulty nodes in a WSN.

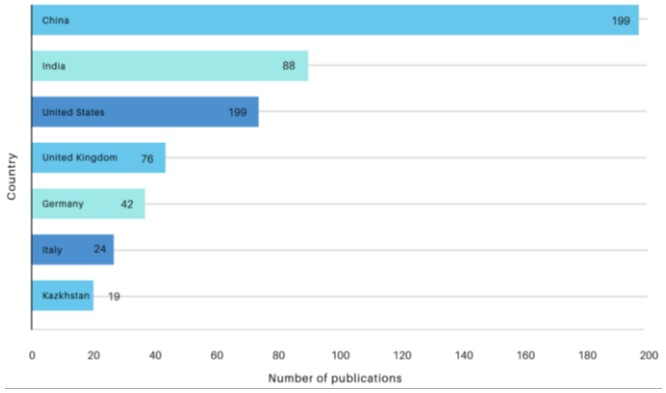

Fig. 2. Total publication of a country

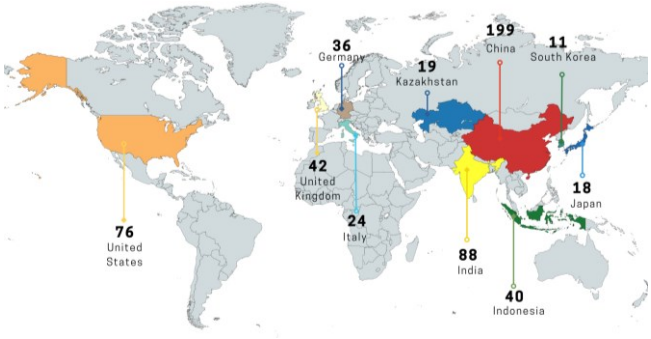

Fig. 3. Regional rank of countries of publication between 2022 and 2023

The histogram shows countries by the number of publications, the average number of publications for the specified period is 69 publications, the country with a high

rate of publications in the proposed direction is China with an indicator of 199 publications, in Kazakhstan - 19; and for the United States, the number of publications reaches 76, which were obtained with the help of the ACM Digital Library system. Due to the increase in the number of devices in various applications, the number of works and scientists will increase every year, offering their unique solutions for detecting faulty nodes in a WSN, which generally ensures security and privacy when interacting with the Internet of Things.

At the same time, 899 discussions and more than 120,000 publications were found in the Research Gate scientific information social network on the scientific topic "Internet of Things", according to the results of the analysis, scientists with a high number of citations were identified and tabulated in Table I.

From the above study, we can conclude that by combining various Machine Learning methods with each other, you can get a good result. Table II provides examples of the application of various Machine Learning methods.

TABLE I. THE TOP MOST ACTIVE AUTHORS BETWEEN 2022 AND 2023

Name	Affiliation	Number of publications	Cite
Hong-Ning Dai	Hong Kong Baptist University, China	58	202
Tie Qiu	Tianjin University, China	38	73
Zhibo Pang	ABB Corporate Research, Sweden	36	61
Shuang-Hua Yang	University of Reading, UK	29	92
Professor Lei Ren	Beihang University, China	28	171
L. Alfredo Grieco	Politecnico di Bari, Italy	20	17
Gerhard Hancke	City University, China	11	32

TABLE II. SOME STUDIES OF FAULT NODE DETECTION IN WSN

Paper	Year	Main idea	Conclusion
[47]	2023	The authors proposed a fault detection algorithm that does not load SN resources when evaluating the WSN failure state	The authors evaluated the proposed algorithm using Matlab, Google colab, and the effectiveness of the algorithm was determined by extensive simulation
[48]	2021	The authors return a method for detecting IoT infections using SVM	The authors added a component reflecting the reliability of the proposed solution, which gave satisfactory results in the form of an accuracy of 90.28%
[49]	2019	For knowledge discovery the authors propose a hybrid Machine Learning model with multivariate time series data	The results are obtained using a hybrid model with a Random Forest (RF) and achieve 94.86% accuracy
[50]	2023	The authors proposed a system to improve the performance of a wireless sensor network	As a result, an accuracy of 97.84% was achieved for 500 nodes, which confirms that the proposed system is competent for attack detection
[51]	2019	The authors propose to use the method with the concept of clonal selection of an artificial immune system. Detected faults are classified using a probabilistic neural approach as persistent, discontinuous and temporary networks	The probabilistic neural networks (PNN) model was used in the work and the result demonstrates 97% accuracy
[52]	2022	The authors present the results of a study, indicating the superiority of the proposed DE-SVM and GWO-SVM approaches	The RF model was used in the work and the result demonstrates 81% accuracy
[53]	2020	The paper analyzes the SVM, RF, PNN, MLP and LSTM models	The results show that as the number of faults increases, the LSTM detects a higher rate that ranges between 80 and 90%
[54]	2021	In this paper, the authors combine the CV-SVM and PSO-PNN methods	the result demonstrate identifying four states with an accuracy rate of 83.3%, 72.5%, and for identifying three states, the accuracy rate reaches 90%, 85%
[55]	2022	The paper investigates the question of the influence of the sampling method for predicting faults in the network	As a result of using the SVM model, the accuracy is between 0.29-0.83 and when using the Extra Tree model, the accuracy reaches 96%
[56]	2022	The authors presented the results of a study intended to develop and implement a global approach to fault detection	The results of the work demonstrate a fault detection accuracy of 99%
[57]	2022	The authors proposed an end-to-end deep learning environment for diagnosing sensor malfunctions	The results of the work demonstrate an accuracy of 100% when locating a faulty sensor, 98.7% when determining the type of fault, and 99% accuracy when reconstructing
[58]	2022	The authors propose a method for diagnosing machine faults based on WSN sensor calculations and a separable convolution.	The paper considers CNN and ResNet models and proposes a method whose results reach 98.3% accuracy, the amount of data is reduced, and there is a 15% energy saving
[59]	2022	In the article, the structure of the IoT is developed and implemented in real time for complex electromechanical equipment	The paper considers the long short-term memory (LSTM) model, whose results reach 90.67% and 100% accuracy
[60]	2023	This article presents a process for building an Acoustic Emission fault detection system using Machine Learning methods	The accuracy of the method based on the fine decision tree ML model reached 96.1%
[61]	2023	The authors used AD methods using a dataset to perform error diagnosis analysis using four unsupervised learning approaches with different principles	The paper considers anomaly detection in WSN for fault diagnosis using Machine Learning
[62]	2023	The authors proposed a possible approach using the theory of spatial correlation	This paper proposes a scheme for determining the fault state of deployed sensor nodes using an SVM classifier based on Grey Wolf Optimization (GWO)
[63]	2023	Authors use Machine Learning classifiers to detect faulty nodes	The authors demonstrate that the RF classifier is best suited for fault detection of WSN, with an accuracy of 92%
[64]	2023	The authors proposed a digital twin (DT) approach to detecting faulty nodes, while analysing its ability to identify one type of fault in several sensors	The highest fault diagnosis accuracy by the model proposed reached 98.7%
[65]	2023	Proposes a new method for improving the security of smart grids and fault detection in the industry using a WSN with a deep learning architecture	The accuracy of the proposed method reached 95%
[66]	2023	An improved GWAO-SVM was created by combining the GWAO and SVM	The accuracy of fault detection reached 98.875%

An overview of scientific works is presented in Table II, which focuses on the application of various methods based on Machine Learning to diagnose faulty wireless sensor network nodes. Machine Learning methods such as SVM, PNN, CNN, MLP, RF, and LSTM are widely used in practice to detect and diagnose failures in WSN and have significant performance. In most works, SVM is used in conjunction with other methods and shows high accuracy. The literature review (Table II) can be classified into the following categories:

- Fault detection algorithms that do not load WSN resources. These algorithms aim to reduce the energy consumption and computational complexity of the sensor nodes by performing fault detection at the base station or the cluster head [47].
- SVM. These methods use SVMs as a supervised learning technique to classify the sensor nodes into normal or faulty states [48].
- RF. These methods use RFs as an ensemble learning technique to detect and identify different types of faults in the sensor nodes [49].
- PNN. These methods use PNNs as a non-parametric learning technique to classify the sensor nodes based on their fault states [51].
- LSTM. These methods use LSTM networks as a deep learning technique to capture the temporal dependencies and patterns of the sensor data [53].
- Hybrid approaches. These methods combine different Machine Learning techniques to improve the performance and accuracy of fault detection [54].
- Anomaly detection. These methods use unsupervised learning techniques to detect outliers or anomalies in the sensor data that indicate faults [61].

Here are the statistics of publications over the past 10 years on the topic of detecting faulty nodes in a wireless sensor network, as shown in Table III and Fig. 4.

TABLE III. THE NUMBER OF PUBLICATION

Year	Number of publication	Year	Number of publication
2012	170	2018	7590
2013	685	2019	10700
2014	1120	2020	14900
2015	1830	2021	16800
2016	2890	2022	17400
2017	4890	2023	17100

In this study, a growth pattern is observed, which confirms the relevance of the chosen direction and the need to propose new methods for detecting faulty nodes in a WSNs.

After that, researchers reviewed a number of existing studies of fault detection methods regarding the Machine Learning methods used, such as SVM, PNN, CNN, RF, DT, LSTM and illustrated them in the taxonomy diagram in Fig. 5.

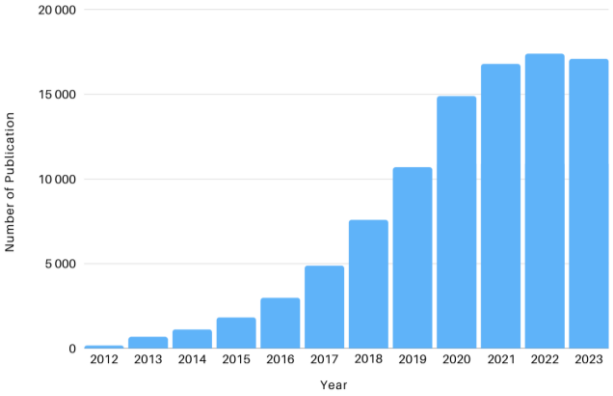

Fig. 4. Number of publication between 2012 and 2023

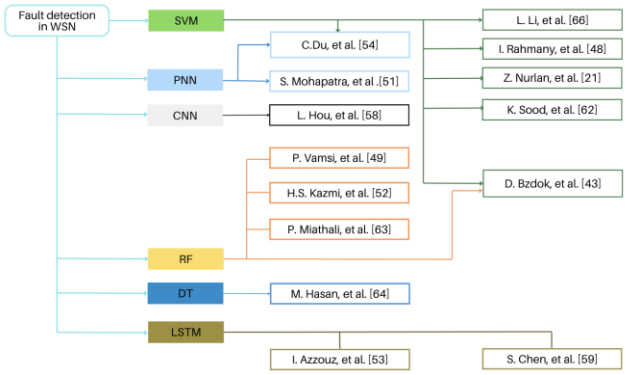

Fig. 5. Taxonomy of fault detection methods in WSN

C. A Machine Learning-based Node Positioning Concept

SVM was first proposed by Vapnik in 1995 [67], where it is said that it implements the idea of mapping an input vector into a multidimensional feature space using some nonlinear mapping selected in advance. SVM uses a dataset from a specific space. An optimal separating hyperplane is constructed in this space. The greater the distance between the separating hyperplane and the objects of the separable classes, the smaller the average error of the SVM classifier. The structure of faulty node detection based on SVM is presented in Fig. 6 [68]–[72].

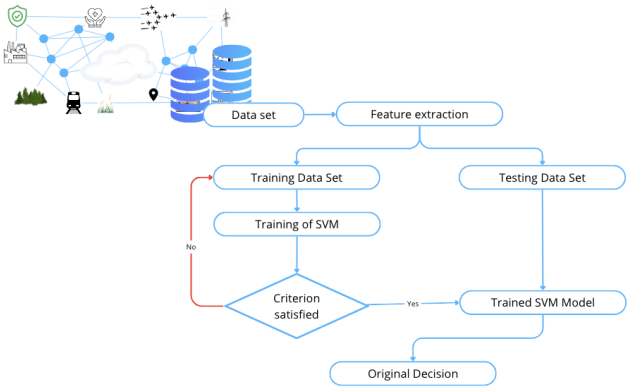

Fig. 6. Structure of fault detection based on SVM

When detecting tasks from faulty nodes in WSNs, there are different levels of complexity. One reason that can be cited for the complexity is the limitation of the resources and facilities of each node. The use of classifiers at the node level can help in solving the problem.

Suppose N=$\{x_i, y_i\}_i^l$ is a set of training samples, where $x_i \in O^m$ is an input vector into the space O, $y_i \in \{-1,1\}$ are class labels. The optimal hyperplane is described by equation (1), where k is the classifier displacement parameter:

$$< w \cdot x > + k = 0 \quad (1)$$

where $w \in O^m, ||w = 1||, c \in O$.

The problem is to determine a hyperplane in which the space O can be divided linearly by solving the following minimization problem (2):

$$\text{min: } K = \frac{1}{2}||w||^2 \quad (2)$$

subject to $y_i \ < w \cdot x_i + b > \geq 1, i = \underline{1, l}$.

SVM is trained as a quadratic optimization problem, Lagrange formulation (3):

$$\text{min: } Q = \sum_{i=1}^{l} \quad \xi_i - \frac{1}{2}\sum_{i,j=1}^{l} \quad \xi_i \xi_j y_i y_j F(x_i \cdot x_j) \quad (3)$$

subject to $\sum_{i=1}^{l} \quad \xi_i y_i = 0$, $C \geq \xi_i \geq 0$, where parameter C is a parameter that is used to control between the margin and the learning error. $F(x_i \cdot x_j)$ - a Kernel Function [73] designed to transform input data into a high-dimensional feature space is required to implement SVM. As a result, the nonlinear SVM function is described as (4):

$$G(x) = sign\left(\sum_{i=1}^{l} \quad \xi_i y_j F(x_i \cdot x) + K\right) \quad (4)$$

where $C \geq \xi_i \geq 0$.

«One-against-all»: this method creates m binary classifiers, each of which is trained to distinguish one class from the remaining $l-1$ classes. During the testing phase, the class level is determined by a binary classifier that produces the maximum output value. This method has features such as high memory requirements and unbalanced training sample size.

“One-against-one”: this method builds $l(l-1)/2$ classifiers. The method is symmetric and, compared to the previous method, has a large classifier size, which entails a high learning rate. It is important to note that the number of classifiers becomes larger as the number of classes increases.

“Error-correcting output codes”: this method checks for erroneous data and then corrects it. There is a possibility of errors occurring during data transmission, which leads to incorrect results. The method improves performance by coding into different categories and then converting to the corresponding codes.

The fault detection mechanism presented in this section was used “One-against-one”.

III. RESULTS AND DISCUSSION

A. Performance Evaluation

To study the behaviour of the model, we conducted simulation on the MATLAB platform, which was installed on a PC with the following characteristics, CPU: Intel Core™ i7 1165G7 4 Core-Processor, GPU: Intel® Iris Xe, OS: Microsoft Windows 11 Pro 64-bit, Storage: 512GB NVMe M.2 SSD. MATLAB is used to simulate results of research. The choice of software version, hardware and operating system can affect the performance of the algorithm. MATLAB's selection feature is an animation feature that allows you to visualise the dynamic behaviour of a system in a real-time environment [74].

The program creates a model of a wireless sensor network in a two-dimensional area [1000m1000m]. The number of nodes is regulated in the GUI. In the experiment under consideration, the number of nodes is determined to be 150. Table IV shows the simulation parameters and values. The parameters determine the efficiency of the algorithm and are used to evaluate the model. To obtain the simulation results, assume parameters such as Number of nodes, Deployment area, Initial energy, Transmission range, Carrier sensing range, Population size and Maximum number of iteration. For example, initial energy characterises the node’s ability to work. As shown in Fig. 7, during the simulation, nodes are randomly located within the specified area. At the next stage of modelling, optimal connections between neighbouring nodes within the radius and the specified range are generated, the result of which is demonstrated in Fig. 8.

TABLE IV. SIMULATION PARAMETERS AND VALUES

Parameters	Values
Number of nodes	150
Deployment area	$1000m \times 1000m$
Initial energy	0,5J
Transmission range	50 m
Carrier sensing range	125 m
Population size	30
Maximum number of iteration	100

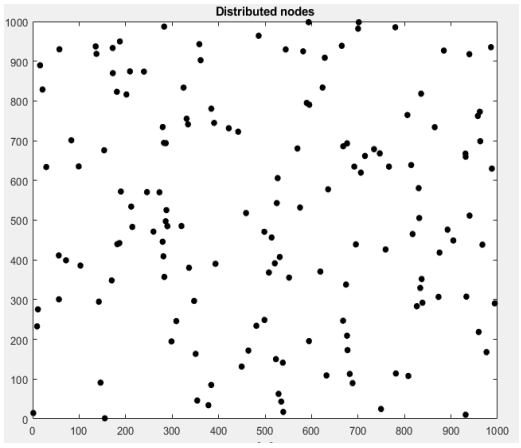

Fig. 7. Nodes distributed in the area

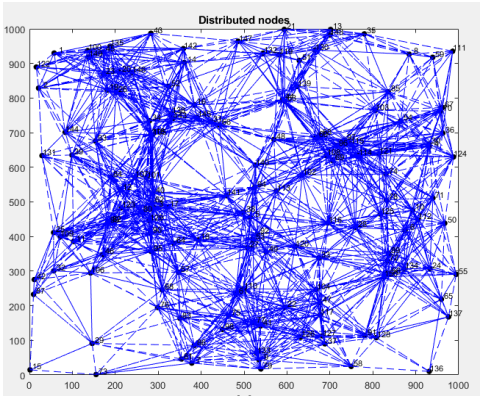

Fig. 8. Visualisation of the connection of nodes

In WSNs "trust" plays a very important role in node communication. "Trust" can be described as a set of attributes that provide security, reliability, and protection with respect to universality. The algorithm for calculating trust consists of five steps and is shown in Fig. 9, where RREQs are routing requests, RREP are responses to a request, α and β are static weighting factors. As a result of the application of the trust calculation algorithm, the modelling results were improved and are reflected in a high percentage of accuracy in detecting a faulty node.

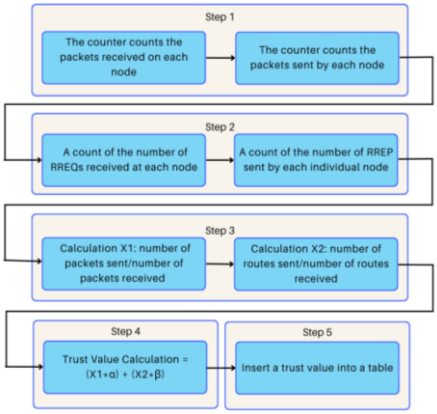

Fig. 9. Algorithm for trust calculation

B. *Experimental results and Analysis*

The node localization process consists of several stages, such as training, translation and localization (Fig. 10):

1) During the learning phase, a model has been generated: each node in the network sends an information packet to a beacon node within its wireless range and sets a beacon node outside its range as unreachable. This allows each node, counting the beacon node, to calculate a distance vector from each beacon node and store it internally. Each beacon node transmits an information packet to the receiving node. The information packet includes the identification number of the beacon node, information about the coordinates of the node itself, and information stored in the distance vector of the node. The algorithm performs SVM training for the X-axis and Y-axis at the receiving node, respectively, and computes all categories $cx_0, cx_1, \ldots, cx_{H-1}, cy_0, cy_1, \ldots, cy_{H-1}$. At the output of the training stage, the corresponding information about the SVM parameters is formulated: $\{J_i x, \alpha_i^\star x, b^\star x\}$, $\{J_i y, \alpha_i^\star y, b^\star y\}$;

2) During the broadcast phase, the receiving node transmits information about the SVM parameters $\{J_i x, \alpha_i^\star x, b^\star x\}$, and $\{J_i y, \alpha_i^\star y, b^\star y\}$ calculated during the training phase to every node of the network zones. Therefore, each node has complete information to calculate the function (4);

3) After the unknown node receives information about the parameters of the SVM in the positioning step, it classifies the SVM at the node according to the distance vector generated by itself, evaluates its area category, and calculates the centroid coordinates of the area cell $(x'(J_i), y'(J_i))$ as calculated position coordinates.

This model is tested on data very similar to real-world sounding data to evaluate the ability of this model to detect failed nodes and calculate training and testing errors. As a result, the training error was 4.6667%. Training error is a measure of how often it makes wrong predictions compared to the normal model. This simulation is close to normal and real simulation because it depends on the normal distribution of values. At the same time, the simulation carried out in the research is close to a normal and real simulation, since it depends on the normal distribution of values.

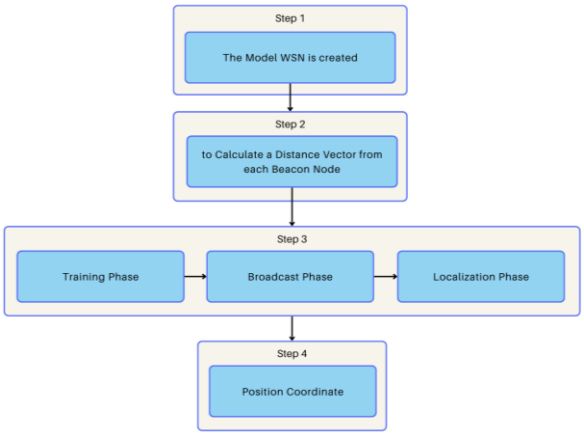

Fig. 10. The process of node localization

Fig. 11 shows attack detection is implemented as follows, the program randomly selects some nodes and sets these nodes as unknown. Then the previously trained SVM is applied and the training is repeated, i.e. tested, and the program determines which ones will be attacked. The attacked nodes are circled in red.

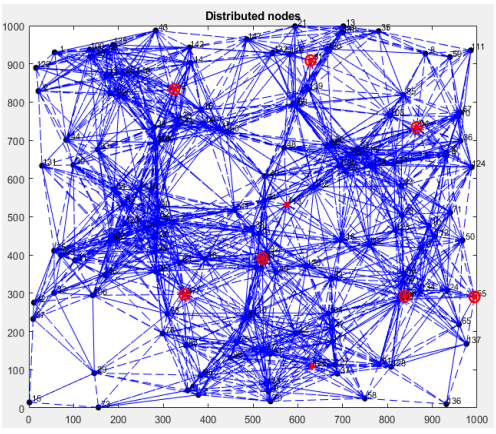

Fig. 11. Attacked nodes

For more accurate results, the experiment was repeated 10 times with the same network parameter setting, and an average of 10 experiments were also performed. In each experiment, all nodes were placed in a random order. The performance of the WSN node positioning algorithm directly affects its application, so during the study, the focus was on the performance of the algorithm in terms of positioning error, classification accuracy and range error. The experiments were conducted with a different number of nodes from 50 to 320. The results presented in Table IV showed the effect of different ratios of nodes and the radius of communication between nodes on the classification accuracy of the positioning algorithm and the positioning error.

The results of the simulation are shown as a graph: As shown in Fig. 12, for the same link radius, the more beacon nodes there are, the higher the degree of classification accuracy. The categorization accuracy increases with radius. The number of beacon nodes covered in the node's communication range increases with a larger communication radius and a higher proportion of beacon nodes, and since the distance vector produced by the positioning algorithm during the learning phase can more accurately reflect the node location information, the degree of classification accuracy is higher. The more nodes, the higher the error rate.

Fig. 12. Learning errors

Table V shows the experimental results, including the number of nodes and the corresponding training and testing error percentages (averaged over 10 trials) for different node configurations in the study.

TABLE V. THE RESULT OF THE EXPERIMENTS

Number of nodes	50	80	110	140	170	200	230	260	290	320
Training error % (mean of 10)	1	2.25	2.36	2.14	2.64	2.95	2.87	2.69	3.32	3.51
Testing error % (mean of 10)	1	0.7	0.9	0.6	1.5	1.8	1.6	1.6	1.8	1.6

With a longer communication radius and the same proportion of beacon nodes, the position inaccuracy will be the smallest, as illustrated in Fig. 13. The positioning error lowers with an increase in the proportion of beacon nodes for a given link radius, although the difference is rather minor, showing that the technique does not require high proportions of beacon nodes. As a result, we draw the conclusion that the positioning algorithm works better in networks with fewer beacon nodes. Detection of Faulty Nodes improves the quality of a WSN and helps avoid Data loss, the accuracy of detecting faulty nodes was 97%.

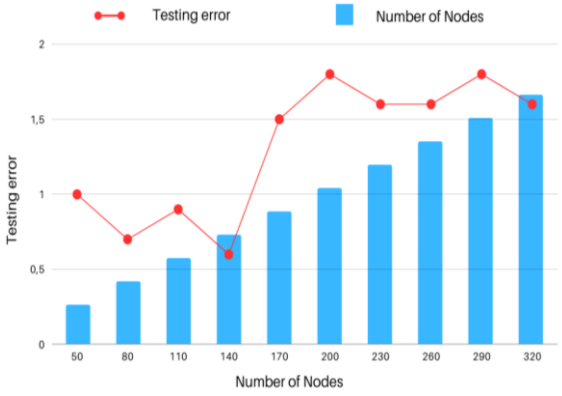

Fig. 13. Testing errors

Experimental results show that the positioning algorithm does not impose high requirements on the ratio of beacon nodes. However, classification accuracy and location error are more suited to network environments with sparse beacon nodes and high range errors because they are reasonably tolerant to range error variations. The algorithm has high reliability, high stability, and flexibility.

The proposed approach was simulated in MATLAB, but when applying the algorithm in real scenarios, it is important to take into account hardware, software, energy efficiency, type of communication, scalability, testing and integration factors. Careful consideration is necessary for equipment selection, compatibility, energy efficiency, data management, communication protocols, and security to ensure the algorithm's successful implementation and reliability in practical applications.

The presented research demonstrates the high detection rate of Faulty Nodes in a WSN, but it is also important to note potential hurdles and issues that may arise during actual deployment:

- Machine Learning Methods are not capable of ensuring complete security in WSN [75-77];
- The Hardware used is not always suitable for the Learning Process [78, 79];
- Protecting Confidential Data [80, 81].

IV. CONCLUSION AND FURTHER WORK

With advances in Machine Learning, various methods for detecting faulty nodes in a WSN are attracting the attention of academic researchers and practitioners. This study presents a systematic analysis of machine learning methods that have been used in research related to faulty node detection between 2022 and 2023. An overview of research trends in Machine Learning faulty node detection based on 484 full-length research articles extracted from various databases such as Google Scholar, IEEE Xplore, Springer Link, Web of Science, Scopus, and Science Direct. Using the publishing trends of articles extracted from various databases, this study shows that the use of Machine Learning techniques to diagnose faulty nodes in a wireless sensor

network has been growing rapidly over the past 10 years. which is directly related to the sharp increase in the number of WSN applications.

Countries and academic researchers with a large number of published articles have been identified and presented in this article. The number of WSN applications is increasing every day, which contributes to the emergence of various security issues. It is impossible to single out one or another country as a Leader in terms of technological achievements, but nevertheless, the number of works and scientists offering their unique solutions for detecting faulty nodes in WSN is generally impressive and emphasises the importance of security.

In this article, the idea of Machine Learning is introduced into the node positioning technology of a wireless sensor network. Positional relationships among nodes serve as training data and linkages between beacon nodes and unknown nodes serve as test data. When wrong data is recognized, data sensors provide false information to the application, which might cause significant harm. Consequently, the SVM classifier was applied to deal with these issues because it can distinguish between accurate and false data. After the algorithm has trained the training data, it broadcasts information about the SVM parameters to every node in the network. After the unknown node receives it, it performs node location according to the ratio of the distance between it and the beacon node. Simulation results show that this positioning algorithm has better resistance to ranging errors and is more suitable for network environments with sparse beacon nodes. The algorithm has high stability and is suitable for network environments with an uneven distribution of nodes or gaps in coverage.

The goal of this work is to use SVM to detect faulty nodes in WSN. To achieve this goal, the following steps were completed:

- analysis of the mechanism for detecting faulty components;
- experimental assessment of the effectiveness of the developed method by simulating its operation in MATLAB.

We note that the proposed algorithm holds promise for real-world applications beyond its current MATLAB implementation, its successful execution hinges on addressing the multifaceted challenges related to hardware, software, energy management, scalability, communication, and security. Conducting rigorous field testing and validation is a prerequisite to ascertain its practicality and performance in diverse real-world environments. The issues under consideration that may arise in the deployment algorithm include energy management. In research, it is not always possible to predict how much energy will be spent on the training process, which may overall affect the performance of the system as a whole.

The Research solves the problem of detecting Faulty Nodes in a WSN, thereby providing a high-quality wireless network while preventing Data loss. The developed algorithm can be used in Smart City, Smart Greenhouse, etc. Applications, where the number of nodes does not exceed 320.

In the future, a comparative analysis of the SVM with other methods and modifications of SVM. The presented work can become a starting point for studying the most pressing issue and also for initiating new methods for determining faulty nodes.

ACKNOWLEDGMENT

The study was carried out as part of a Postdoctoral program and is one of the required studies to be carried out. This research was funded by the Committee of Science of the Ministry of Science and Higher Education of the Republic of Kazakhstan (Grant No. AP14973006).

REFERENCES

[1] T. M. Ghazal *et al*., "Internet of Things Connected Wireless Sensor Networks for Smart Cities," *The Effect of Information Technology on Business and Marketing Intelligence Systems*, pp.1953-1968, 2023.

[2] A. K. Koshariya *et al*., "Ai-enabled iot and wsn-integrated smart agriculture system," *Artificial Intelligence Tools and Technologies for Smart Farming and Agriculture Practices*, pp. 200-218, 2023.

[3] R. Muhajjar, A. Nahla, and A. Mishall, "A perfect security key management method for hierarchical wireless sensor networks in medical environments," *Electronics*, vol. 12, no. 4, p. 1011. 2023.

[4] H. M. Fahmy, "WSNs applications," *Concepts, applications, experimentation and analysis of wireless sensor networks*, pp. 67-242, 2023.

[5] F. Khan, S. Ahmad, H. Gürüler, G. Cetin, T. Whangbo, and C. Kim, "An Efficient and Reliable Algorithm for Wireless Sensor Network," *Sensors*, vol. 21, no. 24, p. 8355, 2021, doi: 10.3390/s21248355.

[6] Z. Nurlan, T. Z. Kokenovna, M. Othman, and A. Adamova, "Resource Allocation Approach for Optimal Routing in IoT Wireless Mesh Networks," *IEEE Access*, vol. 9, pp. 153926–153942, 2021, doi:10.1109/access.2021.3123903.

[7] S. S. Banihashemian and F. Adibnia, "A Novel Robust Soft-Computed Range-Free Localization Algorithm Against Malicious Anchor Nodes," *Cognitive Computation*, vol. 13, no. 4, pp. 992–1007, 2021, doi: 10.1007/s12559-021-09879-w.

[8] Z. Wei, S. Yu, and W. Ma, "Defending against Internal Attacks in Healthcare-Based WSNs," *Journal of Healthcare Engineering*, vol. 2021, pp. 1–10, 2021, doi: 10.1155/2021/2081246.

[9] Z. Nurlan, T. Zhukabayeva, and M. Othman, "IoT Hardware-Defined Routing Protocol for Dynamic Self-organizing Wireless Mesh Networks," *2020 IEEE 10th International Conference on Consumer Electronics*, 2020, doi: 10.1109/icce-berlin50680.2020.9352191.

[10] N. T. Hanh *et al*., "Node placement optimization under Q-Coverage and Q-Connectivity constraints in wireless sensor networks," *Journal of Network and Computer Applications*, vol. 212, p. 103578, 2023, doi: 10.1016/j.jnca.2022.103578.

[11] T. K. Dao *et al*., "An optimal WSN node coverage based on enhanced archimedes optimization algorithm," *Entropy*, vol. 24, no. 8, p. 1018, 2022.

[12] K. Jain, A. Kumar, and A. Singh, "Data transmission reduction techniques for improving network lifetime in wireless sensor networks: An up-to-date survey from 2017 to 2022," *Transactions on Emerging Telecommunications Technologies*, vol. 34. no. 1, p. e4674, 2023.

[13] U. Panahi and C. Bayılmış, "Enabling secure data transmission for wireless sensor networks based IoT applications," *Ain Shams Engineering Journal*, vol. 14, no. 2, p. 101866, 2023.

[14] A. Mubarakali *et al*., "Fog-based delay-sensitive data transmission algorithm for data forwarding and storage in cloud environment for multimedia applications," *Big Data*, vol. 11, no.2, pp. 128-136, 2023.

[15] S. Wang and Y. Chen, "Optimization of Wireless Sensor Network Architecture with Security System," *Journal of Sensors*, vol. 2021, pp. 1–11, 2021, doi: 10.1155/2021/7886639.

[16] N. Stroia, D. Moga, V. Muresan, and A. Lodin, "Estimating Environmental Variables in Smart Sensor Networks with Faulty

Nodes," *Proceedings of the 9th International Conference on Smart Cities and Green ICT Systems*, 2020, doi: 10.5220/0009394500670073.

[17] R.K. Aaditya and P. Rajpoot, "Optimized H-LEACH algorithm for clustering to improve lifetime of WSN," *2018 3rd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology* (RTEICT), 2018, doi: 10.1109/rteict42901.2018.9012605.

[18] S. Yu and J. He, "Providing trusted data for industrial wireless sensor networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2018, no. 1, 2018, doi: 10.1186/s13638-018-1307-y.

[19] C. Yi, "En-Route Message Authentication Scheme for Filtering False Data in WSNs," *Security and Communication Networks*, vol. 2021, pp. 1–18, 2021, doi: 10.1155/2021/4068507.

[20] R. Morthy *et al*., "WSN in Defence Field: A Security Overview," *2020 Fourth International Conference on I-SMAC (I-SMAC)*, 2020, doi: 10.1109/i-smac49090.2020.9243406.

[21] Z. Nurlan, T. Zhukabayeva, and M. Othman, "EZ-SEP: Extended Z-SEP Routing Protocol with Hierarchical Clustering Approach for Wireless Heterogeneous Sensor Network," *Sensors*, vol. 21, no. 4, 1021, 2021, doi: 10.3390/s21041021.

[22] G. Qiao, C. Zhao, F. Zhou, and N. Ahmed, "Distributed Localization Based on Signal Propagation Loss for Underwater Sensor Networks," *IEEE Access*, vol. 7, pp. 112985–112995, 2019, doi: 10.1109/access.2019.2934978.

[23] N. Zaarour, N. Hakem, and U. NahiKandil, "Anchor Density Minimization for Localization in Wireless Sensor Network (WSN)," *Computer Science and Information Technology Trends*, 2021, doi: 10.5121/csit.2021.112201.

[24] A. Manikandan, C. Venkataramanan, and R. Dhanapal, "A score based link delay aware routing protocol to improve energy optimization in wireless sensor network," *Journal of Engineering Research*, p. 100115, 2023, doi: 10.1016/j.jer.2023.100115.

[25] M. Ahmad *et al*., "Optimal Clustering in Wireless Sensor Networks for the Internet of Things Based on Memetic Algorithm: memeWSN," *Wireless Communications and Mobile Computing*, vol. 2021, pp. 1–14, 2021, doi: 10.1155/2021/8875950.

[26] M. S. BenSaleh, R. Saida, Y. H. Kacem, and M. Abid, "Wireless Sensor Network Design Methodologies: A Survey," *Journal of Sensors*, vol. 2020, pp. 1–13, Jan. 2020, doi: 10.1155/2020/9592836.

[27] H. Bai, X. Zhang, and F. Liu, "Intrusion Detection Algorithm Based on Change Rates of Multiple Attributes for WSN," *Wireless Communications and Mobile Computing*, vol. 2020, pp. 1–16, 2020, doi: 10.1155/2020/8898847.

[28] W. Z. Hao, G. J. Horng, and G. J. Jong, "A New Bio-Inspired for Cooperative Data Transmission of IoT," *IEEE Access*, vol. 8, pp. 161884–161893, 2020, doi: 10.1109/access.2020.3021507.

[29] Z. Nurlan, T. Zhukabayeva, M. Othman, A. Adamova, and N. Zhakiyev, "Wireless Sensor Network as a Mesh: Vision and Challenges," *IEEE Access*, vol. 10, pp. 46–67, 2022, doi: 10.1109/access.2021.3137341.

[30] S. A. Jan, N. U. Amin, M. Othman, M. Ali, A. I. Umar, and A. Basir, "A Survey on Privacy-Preserving Authentication Schemes in VANETs: Attacks, Challenges and Open Issues," *IEEE Access*, vol. 9, pp. 153701–153726, 2021, doi: 10.1109/access.2021.3125521.

[31] P. Qi, F. Wang, and S. Hong, "A Novel Trust Model Based on Node Recovery Technique for WSN," *Security and Communication Networks*, vol. 2019, pp. 1–12, 2019, doi: 10.1155/2019/2545129.

[32] A. Ullah, M. Azeem, H. Ashraf, A. A. Alaboudi, M. Humayun, and N. Jhanjhi, "Secure Healthcare Data Aggregation and Transmission in IoT—A Survey," *IEEE Access*, vol. 9, pp. 16849–16865, 2021, doi: 10.1109/access.2021.3052850.

[33] B. S. Gouda, S. Das, and T. Panigrahi, "Distributed Self Intermittent Fault Diagnosis in Dense Wireless Sensor Network," *International Journal of Computer Networks and Applications*, vol. 10, no. 4, p. 603, 2023, doi: 10.22247/ijcna/2023/223315.

[34] R. Deepa and V. Revathi, "Efficient target monitoring with fault-tolerant connectivity in wireless sensor networks," *Transactions on Emerging Telecommunications Technologies*, vol. 34, no. 2, 2022, doi: 10.1002/ett.4672.

[35] A. Srivastava and M. R. Bharti, "Hybrid Machine Learning Model for Anomaly Detection in Unlabelled Data of Wireless Sensor Networks," *Wireless Personal Communications*, vol. 129, no. 4, pp. 2693–2710, 2023, doi: 10.1007/s11277-023-10253-2.

[36] Z. Alansari, A. Prasanth, and M. R. Belgaum, "A Comparison Analysis of Fault Detection Algorithms in Wireless Sensor Networks," *2018 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)*, 2018, doi: 10.1109/3ict.2018.8855761.

[37] A. Adamova, T. Zhukabayeva, and Y. Mardenov, "Machine Learning in Action: An Analysis of its Application for Fault Detection in Wireless Sensor Networks," *2023 IEEE International Conference on Smart Information Systems and Technologies*, pp. 506-511, 2023, doi: 10.1109/SIST58284.2023.10223548.

[38] F. Fan, S.-C. Chu, J.-S. Pan, C. Lin, and H. Zhao, "An optimized Machine Learning technology scheme and its application in fault detection in wireless sensor networks," *Journal of Applied Statistics*, vol. 50, no. 3, pp. 592–609, 2021, doi: 10.1080/02664763.2021.1929089.

[39] A. Javaid *et al*., "Machine Learning Algorithms and Fault Detection for Improved Belief Function Based Decision Fusion in Wireless Sensor Networks," *Sensors*, vol. 19, no. 6, p. 1334, 2019, doi: 10.3390/s19061334.

[40] Z. Noshad *et al*., "Fault Detection in Wireless Sensor Networks through the Random Forest Classifier," *Sensors*, vol. 19, no. 7, p. 1568, 2019, doi: 10.3390/s19071568.

[41] A. Khan *et al*., "Cuckoo Search-based SVM (CS-SVM) Model for Real-Time Indoor Position Estimation in IoT Networks," *Security and Communication Networks*, vol. 2021, pp. 1–7, 2021, doi: 10.1155/2021/6654926.

[42] F. Ahamad, D. K. Lobiyal, S. Degadwala, and D. Vyas, "Inspecting and Finding Faults in Railway Tracks Using Wireless Sensor Networks," *2023 International Conference on Inventive Computation Technologies* (ICICT), 2023, doi: 10.1109/icict57646.2023.10134164.

[43] D. Bzdok, M. Krzywinski, and N. Altman, "Machine Learning: supervised methods," *Nature Methods*, vol. 15, no. 1, pp. 5–6, 2018, doi: 10.1038/nmeth.4551

[44] S. Amaran, "An Optimal Grey Wolf Optimization with Fuzzy Support Vector Machine based Intrusion Detection System in Clustered Wireless Sensor Networks," *International Journal of Advanced Trends in Computer Science and Engineering,* vol. 9, no. 3, pp. 2655–2661, 2020, doi: 10.30534/ijatcse/2020/25932020.

[45] F. Bao, Y. Wu, Z. Li, Y. Li, L. Liu, and G. Chen, "Effect Improved for High-Dimensional and Unbalanced Data Anomaly Detection Model Based on KNN-SMOTE-LSTM," *Complexity*, vol. 2020, pp. 1–17, 2020, doi: 10.1155/2020/9084704.

[46] P. Yadav and S. C. Sharma, "Q-Learning Based Optimized Localization in WSN," *2023 6th International Conference on Information Systems and Computer Networks (ISCON)*, 2023, doi: 10.1109/iscon57294.2023.10112130.

[47] R. Prasad and R. K. Baghel, "Self-detection based fault diagnosis for wireless sensor networks," *Ad Hoc Networks*, vol. 149, p. 103245, 2023, doi: 10.1016/j.adhoc.2023.103245.

[48] I. Rahmany, H. Mnassri, T. Moulahi, and S. E. Khediri, "Grey Wolf Optimizer Enhanced SVM for IoT Fault Detection," *2021 International Wireless Communications and Mobile Computing* (IWCMC), 2021, doi: 10.1109/iwcmc51323.2021.9498759.

[49] P. Vamsi and A. Chahuan, "Machine Learning Based Hybrid Model for Fault Detection in Wireless Sensors Data," *EAI Endorsed Scal Inf Syst*, vol. 7, no. 24, p. e6, 2019.

[50] A. Gautami, J. Shanthini, and S. Karthik, "A Quasi-Newton Neural Network Based Efficient Intrusion Detection System for Wireless Sensor Network," *Computer Systems Science and Engineering*, vol. 45, no. 1, pp. 427–443, 2023, doi: 10.32604/csse.2023.026688.

[51] S. Mohapatra, P. M. Khilar, and R. R. Swain, "Fault diagnosis in wireless sensor network using clonal selection principle and probabilistic neural network approach," *International Journal of Communication Systems*, vol. 32, no. 16, 2019, doi: 10.1002/dac.4138.

[52] H. S. Kazmi, N. Javaid, M. Awais, M. Tahir, S. Shim, and Y. B. Zikria, "Congestion avoidance and fault detection in WSNs using data science techniques," *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 3, 2019, doi: 10.1002/ett.3756.

[53] I. Azzouz, B. Boussaid, A. Zouinkhi, and M. N. Abdelkrim, "Multi-faults classification in WSN: A deep learning approach," *2020 20th International Conference on Sciences and Techniques of Automatic Control and Computer Engineering (STA)*, 2020, doi: 10.1109/sta50679.2020.9329325.

[54] C. Du, W. Li, Y. Rong, F. Li, F. Yu, and X. Zeng, "Research on the application of artificial intelligence method in automobile engine fault diagnosis," *Engineering Research Express*, vol. 3, no. 2, p. 026002, 2021, doi: 10.1088/2631-8695/ac01ad.

[55] L. K. Wardhani, R. A. Febriyanto, and N. Anggraini, "Fault Detection in Wireless Sensor Networks Data Using Random Under Sampling and Extra-Tree Algorithm," *2022 10th International Conference on Cyber and IT Service Management* (CITSM), 2022, doi: 10.1109/citsm56380.2022.9935888.

[56] M. Safaei, M. Driss, W. Boulila, E. A. Sundararajan, and M. Safaei, "Global outliers detection in wireless sensor networks: A novel approach integrating time-series analysis, entropy, and random forest-based classification.," *Software: Practice and Experience*, vol. 52, no. 1, pp. 277–295, 2021, doi: 10.1002/spe.3020.

[57] D. Jana, J. Patil, S. Herkal, S. Nagarajaiah, and L. Duenas-Osorio, "CNN and Convolutional Autoencoder (CAE) based real-time sensor fault detection, localization, and correction," *Mechanical Systems and Signal Processing*, vol. 169, p. 108723, 2022, doi: 10.1016/j.ymssp.2021.108723.

[58] L. Hou, L. Liu, and G. Mao, "Machine Fault Diagnosis Method Using Lightweight 1-D Separable Convolution and WSNs With Sensor Computing," *IEEE Transactions on Instrumentation and Measurement*, vol. 71, pp. 1–8, 2022, doi: 10.1109/tim.2022.3206764.

[59] S. Chen, Y. Huang, P. Wen, C. Gu, and S. Zhao, "A Fault Diagnosis Platform of Actuators on Embedded IoT Microcontrollers," *2022 Prognostics and Health Management Conference*, pp. 210-217, 2022, doi: 10.1109/PHM2022-London52454.2022.00044.

[60] R. R. Shubita, A. S. Alsadeh, and I. M. Khater, "Fault Detection in Rotating Machinery Based on Sound Signal Using Edge Machine Learning," in *IEEE Access*, vol. 11, pp. 6665-6672, 2023, doi: 10.1109/ACCESS.2023.3237074.

[61] L. Cerdà-Alabern, G. Iuhasz, and G. Gemmi, "Anomaly detection for fault detection in wireless community networks using Machine Learning," *Computer Communications*, vol. 202, pp. 191–203, 2023, doi: 10.1016/j.comcom.2023.02.019.

[62] K. Sood, M. R. Nosouhi, N. Kumar, A. Gaddam, B. Feng, and S. Yu, "Accurate Detection of IoT Sensor Behaviors in Legitimate, Faulty and Compromised Scenarios," in *IEEE Transactions on Dependable and Secure Computing*, vol. 20, no. 1, pp. 288-300, 2023, doi: 10.1109/TDSC.2021.3131991.

[63] P. G. Miathali, "Efficient Machine Learning Classifier for Fault Detection in Wireless Sensor Networks," *Wireless Sensor Networks - Research Issues and Effective Smart Solutions*, 2023, doi: 10.5772/intechopen.111462.

[64] M. N. Hasan, S. U. Jan, and I. Koo, "Wasserstein GAN-Based Digital Twin-Inspired Model for Early Drift Fault Detection in Wireless Sensor Networks," in *IEEE Sensors Journal,* vol. 23, no. 12, pp. 13327-13339, 2023, doi: 10.1109/JSEN.2023.3272908.

[65] M. Kandasamy, S. Anto, K. Baranitharan, R. Rastogi, G. Satwik, and A. Sampathkumar, "Smart Grid Security Based on Blockchain with Industrial Fault Detection Using Wireless Sensor Network and Deep Learning Techniques," *Journal of Sensors*, vol. 2023, pp. 1–13, 2023, doi: 10.1155/2023/3806121.

[66] L. Li, W. Meng, X. Liu, and J. Fei, "Research on Rolling Bearing Fault Diagnosis Based on Variational Modal Decomposition Parameter Optimization and an Improved Support Vector Machine," *Electronics*, vol. 12, no. 6, p. 1290, 2023, doi: 10.3390/electronics12061290.

[67] V. Vapnik and R. Izmailov, "Reinforced SVM method and memorization mechanisms," *Pattern Recognition,* vol. 119, p. 108018, 2021, doi: 10.1016/j.patcog.2021.108018.

[68] Z. Qin and Q. Li, "An uncertain support vector machine with imprecise observations," *Fuzzy Optimization and Decision Making*, vol. 22, no. 4, pp. 611–629, 2023, doi: 10.1007/s10700-022-09404-0.

[69] M. S. Rajan *et al*., "Diagnosis of fault node in wireless sensor networks using adaptive neuro-fuzzy inference system," *Applied Nanoscience*, vol. 13, no. 2, pp. 1007–1015, 2021, doi: 10.1007/s13204-021-01934-0.

[70] P. Yadav and S. C. Sharma, "A Systematic Review of Localization in WSN: Machine Learning and Optimization-Based approaches," *International Journal of Communication Systems*, vol. 36, no. 4, 2022, doi: 10.1002/dac.5397.

[71] F. Righetti, C. Vallati, D. Rasla, and G. Anastasi, "Investigating the CoAP Congestion Control Strategies for 6TiSCH-Based IoT Networks," I*EEE Access*, vol. 11, pp. 11054–11065, 2023, doi: 10.1109/access.2023.3241327.

[72] W. Gui, Q. Lu, M. Su, and F. Pan, "Wireless Sensor Network Fault Sensor Recognition Algorithm Based on MM* Diagnostic Model," *IEEE Access*, vol. 8, pp. 127084–127093, 2020, doi: 10.1109/access.2020.3008255.

[73] A. Karyawati, K. D. Y. Wijaya, and I. W. Supriana, "A Comparison of Different Kernel Functions of SVM Classification Method for Spam Detection," *JITK (Jurnal Ilmu Pengetahuan dan Teknologi Komputer)*, vol. 8, no. 2, pp. 91-97, 2023.

[74] S. Idris, T. Karunathilake, and A. Förster, "Survey and comparative study of LoRa-enabled simulators for internet of things and wireless sensor networks," *Sensors*, vol. 22, no.15, p. 5546, 2022.

[75] R. Ahmad, R. Wazirali, and T. Abu-Ain, "Machine learning for wireless sensor networks security: An overview of challenges and issues," *Sensors*, vol. 22, no.13, p.4730, 2022.

[76] O. S. Egwuche, A. Singh, A. E. Ezugwu, J. Greeff, M. O. Olusanya, and L. Abualigah, "Machine learning for coverage optimization in wireless sensor networks: a comprehensive review," *Annals of Operations Research*, pp. 1-67, 2023.

[77] M. Gillani, A. Niaz, and M. Tayyab, "Role of machine learning in WSN and VANETs," *International Journal of Electrical and Computer Engineering Research*, vol. 1, no.1, pp. 15-20, 2021.

[78] S. Gnanavel *et al*., "Analysis of fault classifiers to detect the faults and node failures in a wireless sensor network," *Electronics*, vol. 11, no. 10, p. 1609, 2022.

[79] G. Lăzăroiu *et al*., "Deep learning-assisted smart process planning, robotic wireless sensor networks, and geospatial big data management algorithms in the internet of manufacturing things," *ISPRS International Journal of Geo-Information*, vol. 11, no.5, p. 277, 2022.

[80] F. Mezrag, S. Bitam, and A. Mellouk, "An efficient and lightweight identity-based scheme for secure communication in clustered wireless sensor networks," *Journal of Network and Computer Applications,* vol. 200, p. 103282, 2022.

[81] R. Nagaraju *et al*., "Secure routing-based energy optimization for IOT application with heterogeneous wireless sensor networks," *Energies,* vol. 15, no.13, p. 4777, 2022.