2023 لسنة A10 العدد
No.10A - Septembr 2023
المجلة العراقية للبحوث الانسانية والاجتماعية والعلمية
Iraqi Journal of Humanitarian, Social and Scientific Research
Print ISSN 2710-0952-Electronic ISSN 2790-1254

كشف الشذوذ في شبكات الاستشعار اللاسلكية باستخدام الشبكة العصبية الاصطناعية

الحكم عامر نصيف
alhukmaljibaara@gmail.com
وزارة التربية / المديرية العامة لتربية صلاح الدين

الملخص

أصبحت شبكات الاستشعار اللاسلكية (WSNs) منتشرة في مختلف المجالات، بدءًا من المراقبة البيئية إلى الأتمتة الصناعية .ومع ذلك، فإن نشر WSNs في التطبيقات الهامة يتطلب آليات أمنية قوية، بما في ذلك تقنيات فعالة للكشف عن الشذوذ .نظرًا لضعف شبكات الاستشعار اللاسلكية، ليس من العملي الاعتماد على أمان البروتوكولات القياسية، نظرًا لطبيعة اتصالات المستشعرات وطوبولوجيا الشبكة المتغيرة باستمرار . من أجل توفير خدمات السلامة في شبكات WSN من خلال الجمع بين خبرة المراقبة واتخاذ القرار، تعد الشبكات العصبية الاصطناعية (ANN) إحدى الطرق المقترحة .في هذه الورقة نناقش أهمية الكشف عن الشذوذ في الشبكات اللاسلكية WSN ودورها الحاسم في ضمان سلامة الشبكة وموثوقيتها .تم تسليط الضوء على قيود طرق اكتشاف الشذوذ التقليدية في شبكاتWSN ، مما يؤدي إلى استكشاف شبكات ANN كبديل واعد .يفحص البحث أيضًا مقاييس التقييم ومجموعات البيانات المعيارية المستخدمة بشكل شائع في تقييم أداء تقنيات اكتشاف الشذوذ .تتم مناقشة معايير التقييم المختلفة، مثل دقة الكشف، والمعدل الإيجابي الخاطئ، ووقت الكشف، لتوفير إطار تقييم شامل لمقارنة الأساليب المختلفة القائمة على الشبكات العصبية الاصطناعية .أخيرًا، تحدد الورقة التحديات الحالية واتجاهات البحث المستقبلية في مجال الكشف عن الشذوذ في شبكات WSN باستخدام الشبكات العصبية الاصطناعية .تشمل هذه التحديات كفاءة الطاقة، وقابلية التوسع، والقدرة على التكيف مع ظروف الشبكة الديناميكية .يُقترح التكامل المحتمل للتقنيات الناشئة، مثل الحوسبة المتطورة والتعلم الموحد، كطريقة لمواجهة هذه التحديات والنهوض بهذا المجال.

يفحص البحث أيضًا مقاييس التقييم ومجموعات البيانات المعيارية المستخدمة بشكل شائع في تقييم أداء تقنيات اكتشاف الشذوذ .تتم مناقشة معايير التقييم المختلفة، مثل دقة الكشف، والمعدل الإيجابي الخاطئ، ووقت الكشف، لتوفير إطار تقييم شامل لمقارنة الأساليب المختلفة القائمة على الشبكات العصبية الاصطناعية.

أخيرًا، تحدد الورقة التحديات الحالية واتجاهات البحث المستقبلية في مجال الكشف عن الشذوذ في شبكات WSNباستخدام الشبكات العصبية الاصطناعية .تشمل هذه التحديات كفاءة الطاقة، وقابلية التوسع، والقدرة على التكيف مع ظروف الشبكة الديناميكية .يُقترح التكامل المحتمل للتقنيات الناشئة، مثل الحوسبة المتطورة والتعلم الموحد، كطريقة لمواجهة هذه التحديات والنهوض بهذا المجال.

الكلمات المفتاحية: WSN، كشف الشذوذ، الأمن، السلامة، الحماية، الشبكات العصبونية الاصطناعية، التعلم الآلي.

Anomaly Detection In Wireless Sensor Networks Using Artificial Neural Network

Alhakam Amer Naseef

Abstract

Wireless Sensor Networks (WSNs) have become pervasive in various domains, ranging from environmental monitoring to industrial automation. However, the deployment of WSNs in critical applications necessitates robust security

mechanisms, including effective anomaly detection techniques. Due to the weakness of wireless sensor networks, it is not practical to depend on the safety of the standard protocols, because of the nature of sensor communication and the constantly shifting topology of the network. In order to provide safety services in WSNs by combining expertise of surveillance and decision, artificial neural networks (ANN) are one of the suggested methods. In this paper we discussing the significance of anomaly detection in WSNs and its crucial role in ensuring network integrity and reliability. The limitations of traditional anomaly detection methods in WSNs are highlighted, leading to the exploration of ANNs as a promising alternative.The research also examines the evaluation metrics and benchmark datasets commonly used in assessing the performance of anomaly detection techniques. Different evaluation criteria, such as detection accuracy, false positive rate, and detection time, are discussed to provide a comprehensive evaluation framework for comparing different ANN-based approaches.Finally, the paper identifies current challenges and future research directions in the field of anomaly detection in WSNs using ANNs. These challenges include energy efficiency, scalability, and adaptability to dynamic network conditions. The potential integration of emerging technologies, such as edge computing and federated learning, is proposed as a way to address these challenges and advance the field.

Keywords: WSN, Anomaly detection, security, safety, protection , ANN, Machine Learning.

1. Introduction:

Wireless Sensor Networks (WSNs) have emerged as a critical technology in various domains, ranging from environmental monitoring and industrial automation to healthcare applications. These networks consist of a large number of autonomous sensor nodes that collaborate to collect and transmit data to a central entity. However, due to their distributed nature and exposure to unpredictable environments, WSNs are susceptible to various anomalies and malicious activities, such as sensor failures, communication disruptions, and intrusion attacks. Timely and accurate detection of these anomalies is crucial to ensure the reliability, security, and efficient operation of the network [1].

Artificial Neural Networks (ANNs) have shown remarkable success in various machine learning tasks, including classification, regression, and pattern recognition. Their ability to learn complex patterns from large datasets makes them a promising candidate for anomaly detection in WSNs. This research aims to

explore the potential of using ANN-based models for detecting anomalies in WSNs. By leveraging the power of neural networks, we seek to develop a robust and adaptive system capable of identifying abnormal behavior and events in real-time, enabling proactive measures to mitigate potential damages and enhance the overall network performance [2].

In this research, we will delve into the design and implementation of the proposed ANN-based anomaly detection system for WSNs. We will investigate different neural network architectures, activation functions, and training algorithms to optimize the performance of the detection model. Additionally, the impact of varying network parameters, such as node density, communication range, and deployment environment, will be studied to understand their influence on the anomaly detection accuracy.

The significance of this research lies in its potential to enhance the reliability and security of WSNs in critical applications. By employing an intelligent anomaly detection system based on artificial neural networks, we aim to contribute to the development of more resilient and dependable wireless sensor networks, capable of withstanding unforeseen challenges and ensuring uninterrupted data transmission and monitoring. Ultimately, this research can pave the way for the integration of advanced machine learning techniques into WSNs, fostering a new generation of smart and adaptive sensing systems for a diverse range of real-world applications.

2. Literature reviews:

A five insurance factors are dissected in [3],i.e. trademark limitation danger assurance necessities and countermeasure and six insurance related qualities for example energy framework versatility organization availability and heterogeneity in view of the examination of writing connected with WSN security and showed the pertinence of every security component [3].

It was adequately viewed as different viewpoints for determining the fundamental security prerequisites and showed the insurance necessities required for the utilization of six attributes of WSN that are firmly connected with assurance [3].

A system for establishing a safe climate of WSNs contains of four stages [3]:

Step 1: it was first concentrate every one of qualities of WSN that associated with insurance.

Step 2: It was analyzed the limitations of the security related qualities of the WSN distinguished in stage 1 and examine the dangers brought about by these limitations

Step 3: it was to infer the assurance prerequisites considering the dissected outcome from stage 2 it was somewhat embraced the SLR strategy to extract these proven research works.

Step 4: counter measures are determined they relieve a few dangers where insurance prerequisites can't be covered however there is no question that the insurance necessities charge a major piece of security they can't get all ground on the grounds that various conditions exist to this end measures are required.

In [4] it supplies a reasonable reference for the infrastructure of WSN and the safety challenges. It likewise talks about the chance of benefit acquired from AI calculations by lessening the security cost of WSN in various areas.

In addition of the protection challenges and the solutions to improve the sensors' capability to characterize threats attacks risks and malicious nodes depending on their capacity for learning and self-advancement utilizing AI calculations. Besides, this paper examines open inquiries connected with adjusting AI calculations to the capacity of sensors in this sort of networks.

This paper is introduced an investigation of the remote sensor in the network framework, its current circumstance, applications, working interaction, and safety challenges related with it. It was audited the ML calculations were utilized, and led a scientific investigation of the new examinations that attempted to further develop security in WSNs utilizing ML calculations. It is likewise represented the upsides and downsides of each review.

The detection of assaults that is a fundamental errand to secure the data and networks [5]. The point is to supply a method to intrusion detection suitable with the qualities of WSN [5]. First and foremost, the information gain ratio is utilized to choose the appropriate highlights of sensor's information. Also, the online passive aggressive algorithm is prepared for identifying and arranging different kind of DOS attacks [5].

Focus has been done on the examination work on the systems' security for the insurance of WSNs against the attacks and threats, also the patterns that arise in different nations joined with future exploration lines [6]. According to the systemic perspective, this examination is appeared through the investigation of

works ordered in datasets like Springer, Scopus, ACM, and IEEE. The exploration raised improvements, for example, progresses in safety standards and defense systems, which have prompted the plan of countermeasures in intrusion discovery. At last, the outcomes show the interest of the scientific community in the utilization of AI and ML to enhance performance measurements.

An Online Locally Weighted Projection Regression (OLWPR) uses for anomaly detection in WSN [7]. OLWPR techniques are non-parametric and the ongoing expectations are carried out by local functions that utilization just the subset of data. In this way, the complexity is low which is one of the necessities in WSN. The dimensionality decrease in LWPR is done online by Principal Component Analysis (PCA) to deal with the superfluous and excess data in the information. After the prediction cycle, the threshold is determined dynamically to track down the deviations of anticipated esteem from the real detected esteem [7]

It complete the online detection of irregular data in the data of sensor caught progressively in three stages. The principal stage incorporates the data compression and the second incorporates prediction utilizing LWPR. At long last, the detection stage utilizes the dynamic threshold to distinguish irregular data [7]. The main problem of this work is that consumes huge memory for executing the calculation.

3. Artificial neural networks:

Artificial neural networks are considered as a computational system consisting of a number of interconnected processing units and are characterized by their dynamic and parallel nature in processing the data entering them [8]. The artificial neuron is the building unit of the artificial neural network. The cell consists of an arithmetic unit with multiple inputs and an output signal, and for each output signal there is a weight that modifies the input signal and stimulates the cell to produce a response signal when the value is positive or suppress it when its value is negative [9].

An artificial neural network (ANN) and a biological neural network (BNN) share the same basic principle of information processing, but they are fundamentally different in their implementation and purpose. Here's an overview of their relationship and differences [10]:

1. Inspiration: The artificial neural network is inspired by the biological neural network. The concept of ANN was developed to mimic the way neurons in the brain process information, learn from it, and make decisions.
2. Structure and Function: Biological neural networks refer to the complex interconnected web of neurons in the brain and nervous system of living organisms. These networks are responsible for carrying out various functions like sensory perception, motor control, memory formation, and decision-making. Artificial neural networks, on the other hand, are mathematical models designed to simulate the behavior and learning capabilities of biological neural networks. ANNs are predominantly used for various machine learning tasks, such as pattern recognition, classification, regression, and more.
3. Components: Both BNNs and ANNs are composed of interconnected units, but with different names and functionalities. In a biological neural network, the basic unit is a neuron, which receives input signals through dendrites, processes the information in its cell body, and sends output signals through an axon to other connected neurons. In an artificial neural network, the basic unit is an artificial neuron or node, which receives input data, performs computations using weighted connections, and produces an output that is further propagated through the network.
4. Learning: Biological neural networks learn through a process called synaptic plasticity, which involves strengthening or weakening connections between neurons based on repeated patterns of activity. In contrast, artificial neural networks learn through various learning algorithms, such as backpropagation for supervised learning and reinforcement learning algorithms.
5. Speed and Complexity: Biological neural networks are incredibly complex and highly parallel in their operations. The brain can process information in real-time and perform intricate tasks with ease. Artificial neural networks, while powerful for specific tasks, are generally slower and less versatile than biological neural networks. However, ANNs have shown great promise in various fields, such as image and speech recognition, natural language processing, and game playing.
6. Scalability: Biological neural networks can reorganize and adapt throughout an organism's life in response to new experiences and learning. Artificial neural networks, while they can adapt to new data to some extent, often require significant retraining when faced with drastic changes.

In summary, the relationship between artificial neural networks and biological neural networks is that the former is an attempt to model and replicate the basic principles of the latter, but with a focus on solving specific computational problems rather than perfectly emulating the complexity and intricacies of the human brain.

The following figure represents the architecture of the ANN:

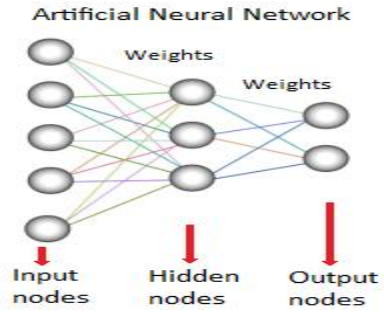

Figure 1 ANN architecture

The following figure represents the calcuations of the ANN:

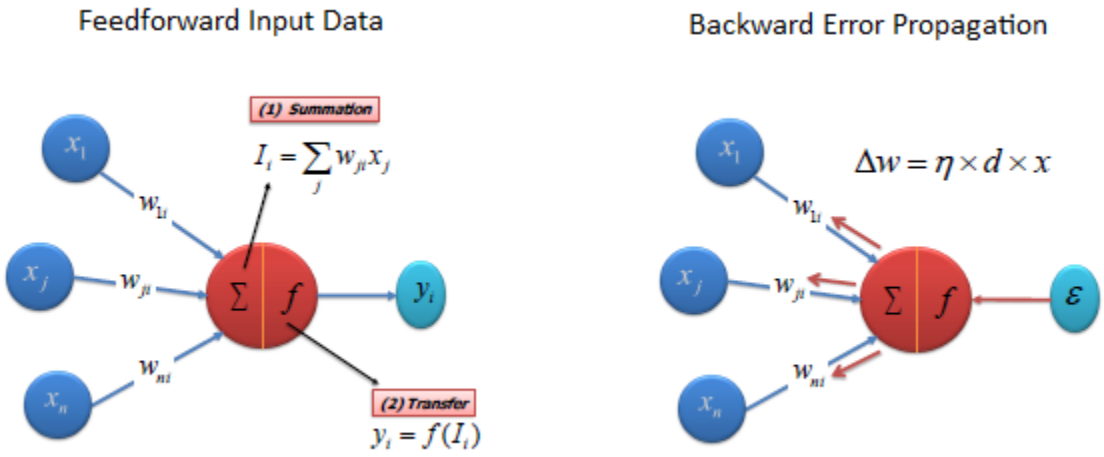

Figure 2 ANN calculations

In the context of Artificial Neural Networks (ANNs), a transfer function (also known as an activation function) is a mathematical function applied to the output of each neuron (or node) in a neural network layer. The primary purpose of a transfer function is to introduce non-linearity into the network,

allowing the neural network to model complex relationships in the data it is learning from [11].

When a neuron receives input signals from the previous layer or directly from the input data, it performs a weighted sum of these inputs, often referred to as a linear combination. The transfer function then takes this linear combination as input and applies a non-linear transformation to it. The transformed output becomes the output of the neuron, which is then passed to the next layer of the neural network [11].

The choice of transfer function is essential because it influences how the neural network learns and performs on various tasks. Some commonly used transfer functions in ANNs include:

- Unit step (threshold): It takes an input value, and if the input is greater than or equal to a certain threshold value, it returns an output of 1 (or any positive value). Otherwise, it returns an output of 0 (or any non-positive value).

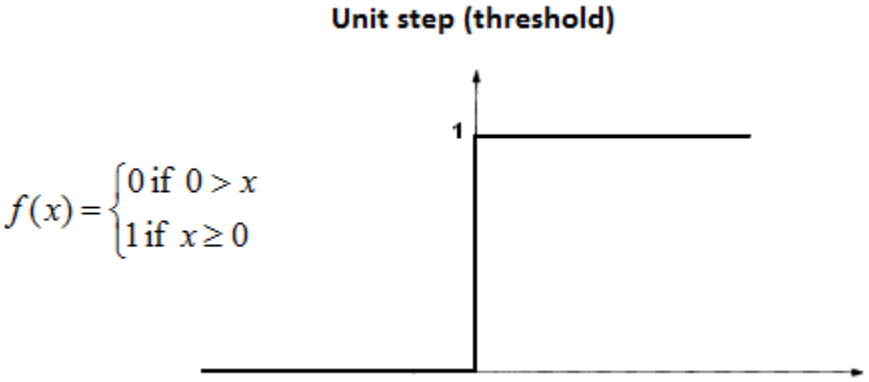

Figure 3 Unit step transfer function

- Sigmoid: It takes an input value and applies a mathematical transformation that maps the input to an output value between 0 and 1.

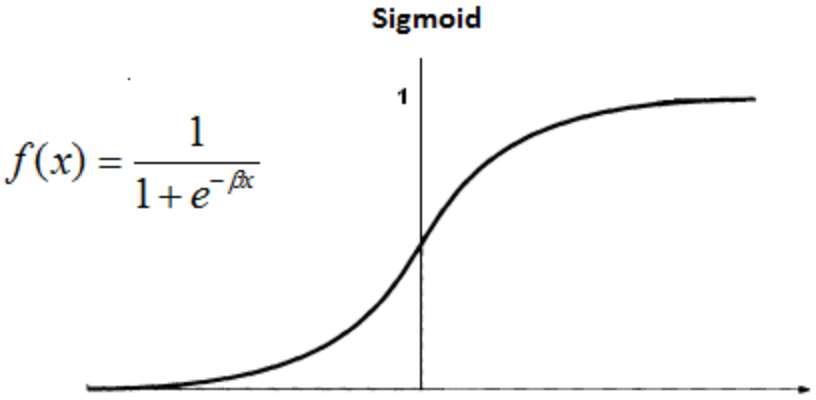

Figure 4 Sigmoid transfer function

- Piecewise Linear: It applies a linear transformation to the input within certain ranges, creating a piecewise linear relationship between the input and output of the neuron

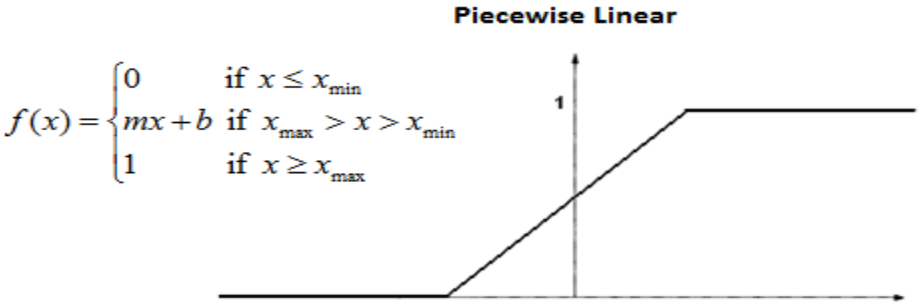

Figure 5 Piecewise Linear transfer function

- Gaussian: It computes the output of a neuron as a function of its input, using a Gaussian distribution centered around a certain mean value.

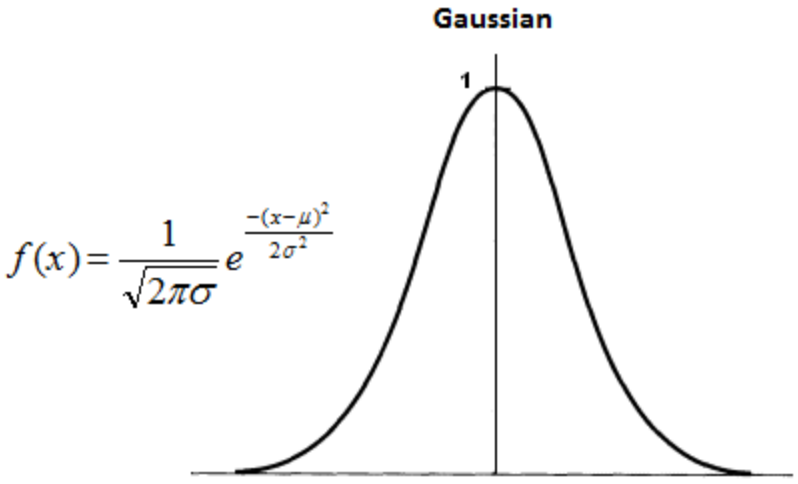

Figure 6 Gaussian transfer function

- Linear: It computes the output of a neuron as a linear function of its input, with no non-linear transformation.

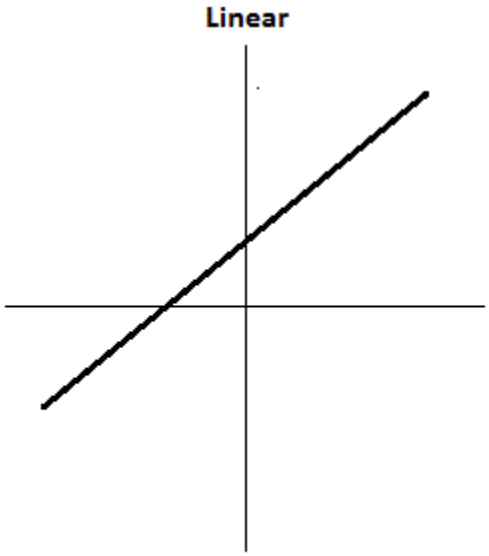

Figure 7 Linear transfer function

- Rectified Linear Unit (ReLU): It calculates the output by computing the maximum between the input value and zero. If the input is positive, it passes through unchanged (rectified); otherwise, it outputs zero [12].

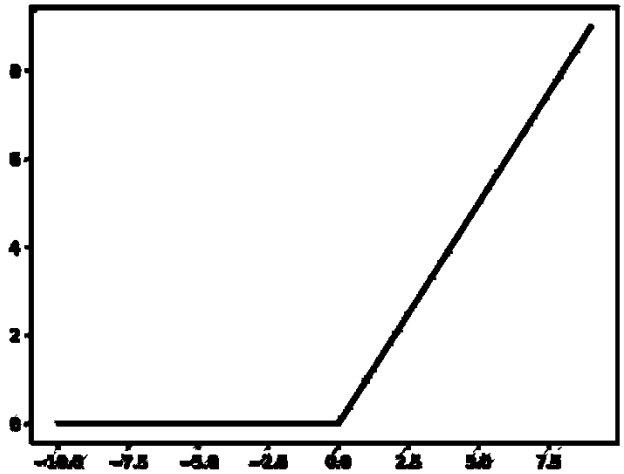

Figure 8 RELU transfer function

7. Methodology:

In this research, the experimental approach [13] was adopted to obtain the structure of the proposed neural network. In the beginning, one layer consisting of ten neurons was relied upon and the results extracted, then the number of neurons was increased by ten by ten until we reached the number of neurons of 150, after which the accuracy began to decrease. A second hidden layer was added and the same scenario as the first layer was used, so the best accuracy we got was when the number of neurons was 100 neurons. Then a third hidden layer was added and the same method mentioned above was used until we got the best classification accuracy when the number of neurons is 50 neurons. When adding a fourth layer, we noticed a decrease in the classification accuracy, so we deleted the fourth layer. So the result that achieved the best classification accuracy was a neural network architecture with three-hidden-layers:

- The first layer has 150 neurons.
- The second layer has 100 neurons.
- The third layer has 50 neurons.

We used the ADAM training algorithm which refers to a stochastic gradient-based optimizer proposed in [14]. ADAM works pretty well on relatively large datasets (with thousands of training samples or more) in terms of both training time and validation score.

In order to utilizing the stochastic gradient descent with the errors backpropagation for training ANN, we need the activation function. This function should be providing more sensitivity to the activation sum input and avoid easy saturation so, we will utilize RELU [15]. Adoption of ReLU may easily be considered one of the few milestones in the deep learning revolution, e.g. the techniques that now permit the routine development of very deep neural networks

Based on the above mentioned we used ReLU (Rectified Linear Unit) transfer function. ReLU (Rectified Linear Unit) is the most recently function has become popular. It is neither smooth nor bounded, but works well in applications that have very large numbers of data.

The mathematical representation of the ReLU transfer function is as follows:

$$g(z) = \max\{0, z\}$$

where "x" is the input to the function, and "g(x)" is the output of the ReLU function.

The properties of RELU can be showed as follows:

1. The ReLU function is piecewise linear and introduces non-linearity, which is crucial for modeling complex relationships in data.
2. It is computationally efficient since it involves simple element-wise operations (comparing with zero and selecting the maximum value) without involving any complex mathematical functions like exponentials or logarithms.
3. ReLU does not suffer from the vanishing gradient problem for positive inputs, allowing for more stable and efficient training of deep neural networks compared to sigmoid and tanh activation functions.

ReLU is one of the most commonly used activation functions in deep learning, particularly in the hidden layers of deep neural networks. It is well-suited for tasks like image recognition, object detection, and natural language processing, where complex and hierarchical patterns need to be learned from the data.So we can be summarized our methodology in the following steps:

1. Read data from dataset.
2. Perform pre-processing operations on the data:
   2.1 Over/Under sampling data to balance classes to optimizing training process.
   2.2 Select the best K features from the columns in dataset to optimizing training process.
   2.3 Transform features by scaling each feature to a given range.
   2.4 Split data into training 80% and testing 20% sets.
3. Training the proposed neural network using training dataset.
4. After training process is finished, using test dataset in order to test the model resulting from the training process.

5. Results and discussion:

In the simulation, we used WSN-DS data set to detection of intrusion in WSN [16]. It contains five classes of attack types (Blackhole (BH), Grayhole (GH), Flooding (F), and TDMA Scheduling) in addition to normal (N) status which refers that the node is not an attacker.

5.1 Measurement parameters:

A confusion matrix is a table used to evaluate the performance of a classification model in ML, [17]. It provides a summary of the predictions by compare them to the actual true labels of the data. The matrix is particularly useful for tasks with multiple classes or categories, allowing us to understand how well the model is classifying instances into each class.

A confusion matrix is a square matrix representing the counts of true positive (TP), true negative (TN), false positive (FP), and false negative (FN) predictions made by a classification model for each class in the dataset. Each row of the matrix corresponds to the actual class, and each column corresponds to the predicted class [18].

The confusion matrix provides valuable insights into the performance of a classification model, helping to assess its accuracy, precision, recall, and F1-score for each class. From the matrix, various evaluation metrics can be derived, such as the overall accuracy of the model, sensitivity

(recall), specificity, and the precision-recall trade-off. Figure 9 shows the architecture of confusion matrix:

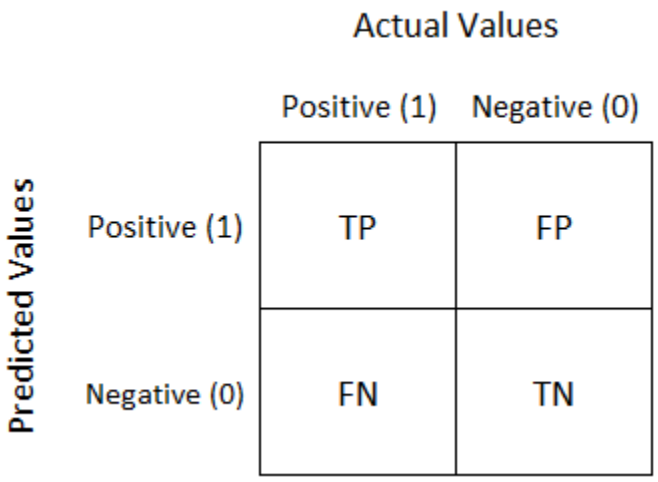

Figure 9 Confusion matrix architecture

It is extremely useful for measuring Recall, Precision and Accuracy.

- TP (True Positive): It refers that we predicted positive and it is true.
- TN (True Negative): It refers that we predicted negative and it is true.
- FP (False Positive): It is type one error and refers that predicted positive and it is false.
- FN (False Negative): It is type two error and refers that predicted negative and it is false.

These parameters are used to calculate recall, precision and accuracy.

$$\text{Re}call = \frac{TP}{TP + FN}$$

The above equation can be discovered as "for all classes which are positive, how many correctly predicted classes [19].

Recall should be high as possible.

$$\text{Pr}ecision = \frac{TP}{TP + FP}$$

The above equation can be discovered as "from all predicted positive classes, how many are positive actually [20].

Precision should be high as possible.

The accuracy is defined as the percentage of true classifications that a trained ML model achieves [21]. The equation of accuracy is given as follows:

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

5.2 Results:

The simulations were performed using machine learning libraries of the Python programming language. The results of the proposed methodology were compared with Decision Tree (DT) [22], Naïve Bayes (NB) [23] and Logistic Regression (LR) [24].

The following table 1 represents the confusion matrix of Decision Tree algorithm.

	BH	F	GH	N	TDMA
BH	1678	0	24	341	0
F	1	623	6	1	0
GH	67	0	2165	753	0
N	7	71	25	67862	0
TDMA	2	0	0	158	1149

Table 1 confusion matrix of Decision Tree algorithm

We note from Table 1 that the decision tree algorithm correctly classified the Blackhole attack type for 1678 of the test samples while it incorrectly classified 24 as Grayhole and also incorrectly classified 341 as normal. In this way, the algorithm correctly classified the Flooding .attack type for 623 of the test samples while it incorrectly classified 1 sample as Blackhole, 6 samples as Grayhole and 1 sample as normal status.

For Grayhole attack the algorithm correctly classified 2165 samples as Grayhole, while it incorrectly classified 67 samples as Blackhole and 753 as normal status.

For normal status, the algorithm correctly classified 67862 samples as normal status, while it incorrectly classified 7 samples as Blackhole, 71 samples as Flooding and 25 samples as Grayhole.

For TDMA, the algorithm correctly classified 1149 samples, while it incorrectly classified 2 samples as Blackhole and 158 samples as normal status.

In the same way, the confusion matrices shown in Tables 2, 3, and 4 are read.

	BH	F	GH	N	TDMA
BH	2043	0	0	0	0
F	0	630	1	0	0
GH	1159	7	1819	0	0
N	7	303	1537	6612	6
TDMA	291	44	58	74	842

Table 2 confusion matrix of Naïve Bayes algorithm

	BH	F	GH	N	TDMA
BH	1560	0	482	1	0
F	0	568	0	63	0
GH	791	0	1918	269	7
N	0	79	304	67564	18
TDMA	0	0	0	90	1213

Table 3 confusion matrix of Logistic Regression algorithm

	BH	F	GH	N	TDMA
BH	2009	0	32	0	2
F	0	606	2	23	0
GH	38	0	2932	14	1
N	0	35	9	67917	4
TDMA	3	0	1	83	1222

Table 4 confusion matrix of proposed methodology

The measurement parameters mentioned in paragraph 5.1 represent a summary of the confusion matrix and show the performance of each algorithm based on the resulting confusion matrix.

The following figure shows a comparison between the previous algorithms and the proposed methodology in terms of: precision, recall and accuracy.

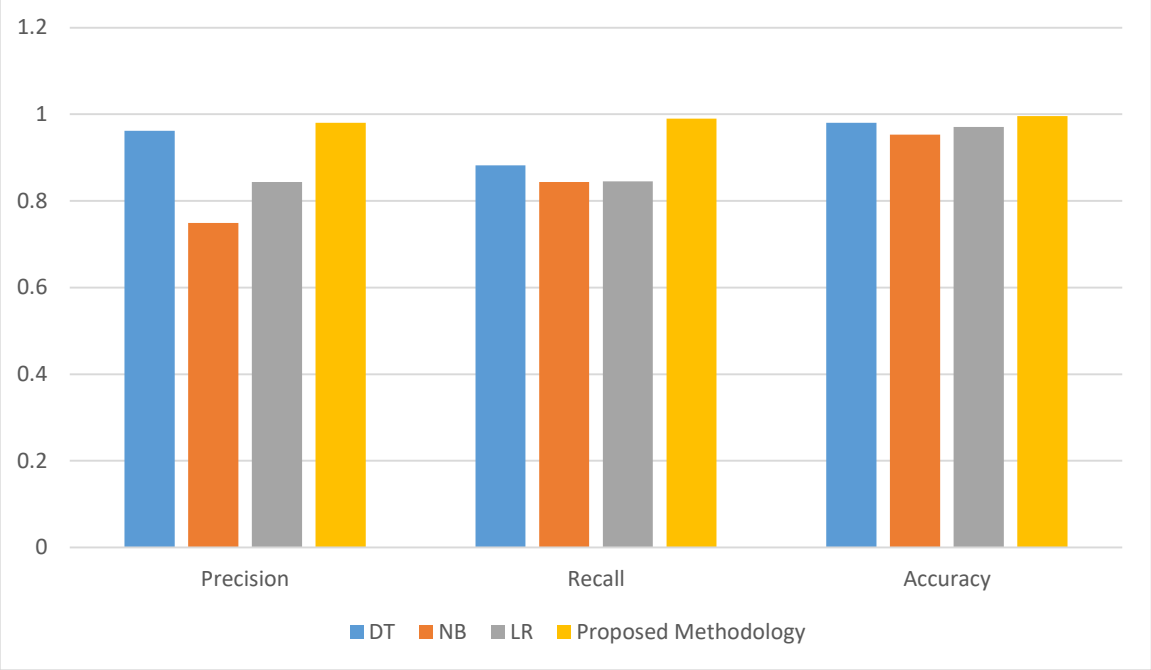

Figure 10 Compassion between DT, NB, LR and proposed methodology

We note from the previous results that the proposed algorithm is superior to the rest of the algorithms. This is because neural networks have ability to learning from dataset and can be utilized for solving the complex problems. Neural networks are also capable of processing huge amounts of data with high speed and accuracy.

The mathematical reason behind the better accuracy of our approach is that these algorithms works better for small dataset and in our experimentation, we have used large dataset. Our classifier accuracy is high because it works better with huge data set like data set which utilized in our simulation.

The proposed algorithm exhibited the highest prediction accuracy among all the algorithms, making it the most effective in detecting attacks in WSNs. The proposed algorithm has capability for learning the complex relationships and patterns within the data, allowing them to adapt to varying attack scenarios.

Linear Regression performed adequately but lacked the sophistication to handle complex attack patterns effectively. It is well-suited for simpler, linearly separable data. In the context of WSN attack detection, where data relationships can be highly nonlinear, Linear Regression falls short compared to more advanced algorithms

The Decision Tree algorithm achieved respectable accuracy, though it was outperformed by our methodology. Decision Trees are easy to interpret, providing insights into the detection process. However, they are prone to overfitting and may struggle with complex datasets, limiting their effectiveness in highly dynamic and sophisticated attack scenarios.

Naive Bayes yielded the lowest prediction accuracy among all the algorithms. Its assumption of independence among features might be too simplistic for the intricate relationships present in attack data. Although computationally efficient, Naive Bayes struggles to handle complex and overlapping feature distributions in real-world attack scenarios.

6. Conclusion and recommendations:

The findings from this study have significant implications for the practical implementation of attack detection systems in WSNs. The superior performance of our methodology emphasizes the importance of leveraging advanced machine learning techniques for more accurate and reliable attack detection.

For researchers and practitioners, this study highlights the potential of ensemble methods and deep learning techniques in improving attack detection performance. However, it is essential to consider the associated computational overhead, especially when deploying such algorithms on resource-constrained sensor nodes.

Furthermore, while Linear Regression and Naive Bayes may not be suitable for complex attack detection tasks, they can still find applications in less demanding scenarios or as part of hybrid detection systems

In conclusion, this study conducted a comparative analysis of various algorithms for attack detection in wireless sensor networks. Based on our findings, we observed that our methodology demonstrated the highest

prediction accuracy, outperforming Decision Tree, Linear Regression, and Naive Bayes. The study underlines the importance of selecting appropriate algorithms based on the complexity of the attack patterns and the available computational resources.

To enhance the security of wireless sensor networks, future research should focus on investigating ensemble techniques and deep learning approaches further. Additionally, exploring hybrid models that combine the strengths of different algorithms could be a promising direction to achieve even higher accuracy in WSN attack detection.

References:

[1] R. Chaudhry and N. Kumar, ‘‘A multi-objective meta-heuristic solution for green computing in software-defined wireless sensor networks,’’ *IEEE Trans. Green Commun. Netw.*, early access, Oct. 21, 2021, doi: 10.1109/TGCN.2021.3122078.

[2] H. I. Kobo, A. M. Abu-Mahfouz, and G. P. Hancke, ‘‘Efficient controller placement and reelection mechanism in distributed control system for software defined wireless sensor networks,’’ *Trans. Emerg. Telecommun Technol.*, vol. 30, no. 6, Jun. 2019, Art. no. e3588.

[3] Yu, J. Y., Lee, E., Oh, S. R., Seo, Y. D., & Kim, Y. G. (2020). A survey on security requirements for WSNs: focusing on the characteristics related to security. *IEEE Access*, *8*, 45304-45324.

[4] Ahmad, R., Wazirali, R., & Abu-Ain, T. (2022). Machine learning for wireless sensor networks security: An overview of challenges and issues. *Sensors*, *22*(13), 4730.

[5] Ifzarne, S., Tabbaa, H., Hafidi, I., & Lamghari, N. (2021). Anomaly detection using machine learning techniques in wireless sensor networks. In *Journal of Physics: Conference Series* (Vol. 1743, No. 1, p. 012021). IOP Publishing.

[6] Gutiérrez-Portela, F., Almenárez-Mendoza, F., Calderón-Benavides, L., & Romero-Riaño, E. (2021). Security prospective of wireless sensor networks

Prospectiva de seguridad de las redes de sensores inalámbricos. *Revista UIS Ingenierías*, *20*(3), 189-202.

[7] Puri, D., & Bhushan, B. (2019, October). Enhancement of security and energy efficiency in WSNs: Machine Learning to the rescue. In *2019 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)* (pp. 120-125). IEEE.

[8] Singha, A. K., Zubair, S., Malibari, A., Pathak, N., Urooj, S., & Sharma, N. (2023). Design of ANN Based Non-Linear Network Using Interconnection of Parallel Processor. *Computer Systems Science & Engineering*, *46*(3).

[9] Yang, J. Q., Wang, R., Ren, Y., Mao, J. Y., Wang, Z. P., Zhou, Y., & Han, S. T. (2020). Neuromorphic engineering: from biological to spike-based hardware nervous systems. *Advanced Materials*, *32*(52), 2003610.

[10] Tang, J., Yuan, F., Shen, X., Wang, Z., Rao, M., He, Y., ... & Wu, H. (2019). Bridging biological and artificial neural networks with emerging neuromorphic devices: fundamentals, progress, and challenges. *Advanced Materials*, *31*(49), 1902761.

[11] Atangana, A., & Akgül, A. (2020). Can transfer function and Bode diagram be obtained from Sumudu transform. *Alexandria Engineering Journal*, *59*(4), 1971-1984.

[12] Zhao, M., Zhong, S., Fu, X., Tang, B., Dong, S., & Pecht, M. (2020). Deep residual networks with adaptively parametric rectifier linear units for fault diagnosis. *IEEE Transactions on Industrial Electronics*, *68*(3), 2587-2597.

[13] Khatir, S., Boutchicha, D., Le Thanh, C., Tran-Ngoc, H., Nguyen, T. N., & Abdel-Wahab, M. (2020). Improved ANN technique combined with Jaya algorithm for crack identification in plates using XIGA and experimental analysis. *Theoretical and Applied Fracture Mechanics*, *107*, 102554.

[14] Zhou, P., Feng, J., Ma, C., Xiong, C., & Hoi, S. C. H. (2020). Towards theoretically understanding why sgd generalizes better than adam in deep learning. *Advances in Neural Information Processing Systems*, *33*, 21285-21296.

[15] Daubechies, I., DeVore, R., Foucart, S., Hanin, B., & Petrova, G. (2022). Nonlinear approximation and (deep) ReLU networks. *Constructive Approximation*, *55*(1), 127-172.

[16] Almomani, I., Al-Kasasbeh, B., & Al-Akhras, M. (2016). WSN-DS: A dataset for intrusion detection systems in wireless sensor networks. *Journal of Sensors*, *2016*.

[17] Haghighi, S., Jasemi, M., Hessabi, S., & Zolanvari, A. (2018). PyCM: Multiclass confusion matrix library in Python. *Journal of Open Source Software*, *3*(25), 729.

[18] Markoulidakis, I., Kopsiaftis, G., Rallis, I., & Georgoulas, I. (2021, June). Multi-class confusion matrix reduction method and its application on net promoter score classification problem. In *The 14th pervasive technologies related to assistive environments conference* (pp. 412-419).

[19] Roth, K., Pemula, L., Zepeda, J., Schölkopf, B., Brox, T., & Gehler, P. (2022). Towards total recall in industrial anomaly detection. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition* (pp. 14318-14328).

[20] MacEachern, S. J., & Forkert, N. D. (2021). Machine learning for precision medicine. *Genome*, *64*(4), 416-425.

[21] Fu, G., Sun, P., Zhu, W., Yang, J., Cao, Y., Yang, M. Y., & Cao, Y. (2019). A deep-learning-based approach for fast and robust steel surface defects classification. *Optics and Lasers in Engineering*, *121*, 397-405.

[22] Charbuty, B., & Abdulazeez, A. (2021). Classification based on decision tree algorithm for machine learning. *Journal of Applied Science and Technology Trends*, *2*(01), 20-28.

[23] Chen, S., Webb, G. I., Liu, L., & Ma, X. (2020). A novel selective naïve Bayes algorithm. *Knowledge-Based Systems*, *192*, 105361.

[24] Shipe, M. E., Deppen, S. A., Farjah, F., & Grogan, E. L. (2019). Developing prediction models for clinical use using logistic regression: an overview. *Journal of thoracic disease*, *11*(Suppl 4), S574.