International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 2s
DOI: https://doi.org/10.17762/ijritcc.v10i2s.5920
***Article Received**: 18 October 2022 **Revised**: 22 November 2022 **Accepted**: 26 December 2022*

An Intrusion Detection Using Machine Learning Algorithm Multi-Layer Perceptron (MlP): A Classification Enhancement in Wireless Sensor Network (WSN)

G.Vinoda Reddy[1], Sreedevi Kadiyala[2], Chandra Srinivasan Potluri[3], P. Shanthi Saravanan[4], G.Athisha[5], M.A.Mukunthan[6], M.Sujaritha[7]

[1]Department of Computer Science and Engineering (AI&ML), CMR Technical Campus
Kandlakoya, Medchal (M), Hyderabad, Telangana-501401
Email:vinodareddy.cse@cmrtc.ac.in
[2]Department of Computer Science and Engineering, Guru Nanak University
Secunderabad, Telangana 500009
Email:sreedevikadiyala@gmail.com
[3]Department of Computer Science and Engineering, Werabe University,
Ethiopia.Email: pcsvas@gmail.com
[4]JJ College of Engineering and Technology
Poolangulathupatti, Trichy, Tamil Nadu 620009,India
Email: shanthisaravanan09@gmail.com
[5]Department of Electronics and Communication Engineering,
PSNA College of Engineering and Technology
Dindigul, Tamil Nadu, 624622, India
E-mail:hodece@psnacet.edu.in
[6]Department of Computer Science and Engineering,
Veltech Rangarajan Dr.Sagunthala R and D Institute of Science and Technology,
Avadi, Chennai-600062
Email: drmamukunthan@veltech.edu.in
[7]Sri Krishna College of Engineering and Technology,
Kuniyamuthur, Tamil Nadu 641008, India
Email:sujaritham@skcet.ac.in

Abstract— During several decades, there has been a meteoric rise in the development and use of cutting-edge technology. The Wireless Sensor Network (WSN) is a groundbreaking innovation that relies on a vast network of individual sensor nodes. The sensor nodes in the network are responsible for collecting data and uploading it to the cloud. When networks with little resources are deployed harshly and without regulation, security risks occur. Since the rate at which new information is being generated is increasing at an exponential rate, WSN communication has become the most challenging and complex aspect of the field. Therefore, WSNs are insecure because of this. With so much riding on WSN applications, accuracy in replies is paramount. Technology that can swiftly and continually analyse internet data streams is essential for spotting breaches and assaults. Without categorization, it is hard to simultaneously reduce processing time while maintaining a high level of detection accuracy. This paper proposed using a Multi-Layer Perceptron (MLP) to enhance the classification accuracy of a system. The proposed method utilises a feed-forward ANN model to generate a mapping for the training and testing datasets using backpropagation. Experiments are performed to determine how well the proposed MLP works. Then, the results are compared to those obtained by using the Hoeffding adaptive tree method and the Restricted Boltzmann Machine-based Clustered-Introduction Detection System. The proposed MLP achieves 98% accuracy, which is higher than the 96.33% achieved by the RBMC-IDS and the 97% accuracy achieved by the Hoeffding adaptive tree.

Keywords- WSN, Multi-Layer Perceptron (MLP), RBMC-IDS, Machine Learning, Classification.

I. INTRODUCTION

The Internet is a massive source of various inventions which connect human life and technology effectively. IoT is a technological advancement becoming unavoidable and the most significant technology in our daily lives. It enables the communication between a wide range of intelligent electronic gadgets and sensors. Another fast-evolving technology in IoT systems is wireless sensor networks (WSN). WSN's significant features are low-power, inexpensive nodes and smart devices with constrained computational capabilities. WSNs are widely used in most real-time applications (figure 1), including healthcare, home automation, smart city, urban monitoring, environment monitoring, critical military surveillance, flora and fauna, security and surveillance, etc. [1,2]. Ruili Wang et

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 2s
DOI: https://doi.org/10.17762/ijritcc.v10i2s.5920
***Article Received**: 18 October 2022 **Revised**: 22 November 2022 **Accepted**: 26 December 2022*

al. (2020) talked about how existing schemes like smart cities, WSN, biometric systems, and surveillance have become more and more important. Sensitive to information security issues.

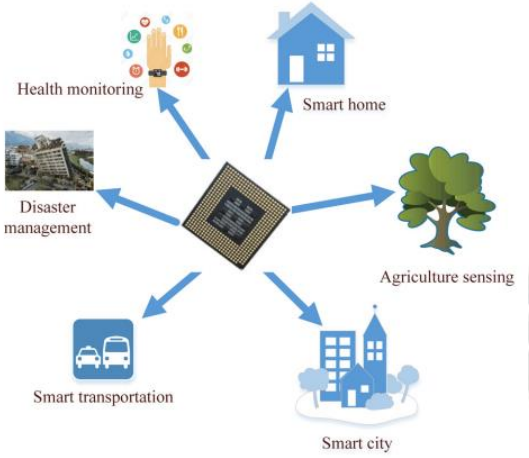

Figure 1: WSN in real-time applications

The WSN has several resource limitations, such as low energy, restricted computing power, poor bandwidth, storage in each node, and short communication ranges. Maintaining each node after installation is problematic since sensor nodes are deployed randomly and cannot move anywhere. The network's lifetime is greatly influenced by the energy consumption of the sensors, which has evolved into the main performance criterion in this area. Additionally, these SNs might target malicious and disruptive operations in a setting that could seriously impair the network's ability to function. Hence to overcome these drawbacks and achieve classification accuracy, Machine learning classification algorithms are essential [3-5].

There are three types of machine learning: supervised learning, unsupervised learning, and reinforcement learning. There are three types of machine learning: reinforcement learning, unsupervised learning, and supervised learning. With supervised machine learning, labeled datasets are used to instruct the system. Unsupervised machine learning, in contrast to supervised machine learning, makes learning decisions independently even without correctly labeled data. Unsupervised machine learning relies on training samples to provide the system with information, and it is up to the machine to extract underlying patterns from the dataset. For reinforcement learning, the system assumes the role of an agent that seeks to identify the best appropriate actions through experimentation and environment observation [6.7].

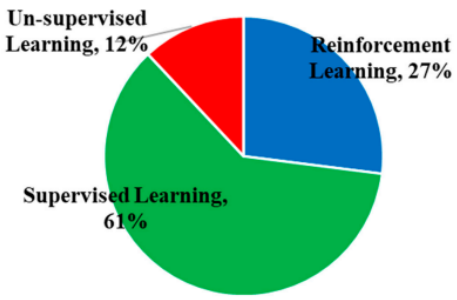

Figure 2: Supervised, unsupervised, and RL learning algorithms in WSN-IoT

Several research projects have been done to find ways to use wireless networks of sensors and the Internet - Of - things with machine learning algorithms [8-11]. In real-time applications, massive data generation and its various types make classification very complex. Hence the traditional detection techniques are insufficient for achieving a higher classification accuracy and detecting harmful network intrusions. Some of the common WSN attacks and their effects are listed below; **Eavesdropping:** In WSN, security-related limitations such as unreliable communication, dynamic nodes, and a hostile environment make it easier for hackers to eavesdrop on nodes' communications. As a result, radio fading and maximization have a huge impact on scattering or frequency transmission. **Jamming:** Jamming is considered the most critical attack among private wireless networks. It frequently disregards security precautions, which can lead to significant issues. The main issue of jamming is the unavailability of services because of the radio frequency noise and interference. **Collision:** The sensors can be located in various environments, with the maximum possibility of malicious interruptions. Malicious nodes can interfere with neighboring nodes and broadcasts by sending a short noise packet since they do not follow the Intermediate Access Control Protocol. This attack has the potential to cause significant network failures. Additionally, determining the origin node is challenging due to the features of wireless transmission.

Traffic Monitoring: Traffic analysis in WSNs is a method for determining node communication patterns. The analysis takes advantage of information obtained by monitoring node-to-node communication. This attack mainly targets the sink or access point nodes containing sensitive data and positional information about those nodes. If the attack succeeds, certain pieces of knowledge are revealed, and the system gets failure. **Spoofing:** Spoofing damages the routing data and leads to routing loops, fake error messages, increased end-to-end latency, routing loops, network traceability, and root path expansions. **DoS:** DoS attack is familiar in all WSN layers, and its main motto is to degrade or shut down the system. A denial-of-service (DoS) attack functioned by saturating the

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 2s
DOI: https://doi.org/10.17762/ijritcc.v10i2s.5920
***Article Received**: 18 October 2022 **Revised**: 22 November 2022 **Accepted**: 26 December 2022*

target with traffic or supplying information that makes the target fail. Authenticated users are denied access to the services or resources because of the DoS attacks.

Table 1: Other attacks and security policies in WSN

S.No	Security Infrastructure	Attacks
1	Availability	Jamming, DoS, Unfairness, Collision, Exhaustion
2	Integrity	Spoofing, Selective forwarding, traffic analysis, and Eavesdropping
3	Confidentiality	Spoofing, Repudiation, Sybil, Session hijacking, Hole and Selective forwarding,

Table 2: Available protection mechanism in WSN

S.No	Security Infrastructure	Attacks
1	Confidentiality	Encryption
2	Integrity	MAC, Digital Signature
3	Availability	Redundancy, Rerouting, and Traffic Control
4	Non-repudiation	Digital certificate

To address the issue mentioned above, we proposed Multi-Layer Perceptron (MLP), a supervised learning mechanism for improving the classification accuracy of a system. Additionally, the proposed system is implemented with the combination of MLP with a feed-forward ANN model and back propagation algorithm for accurately mapping the training and testing datasets. Data routing within WSNs will be challenging owing to their dynamic architecture [24, 25].

Structuring rest of the article: Section 2 examines works that build upon the first segment, and section 3 details the suggested architecture and the method by which it operates. Section 4 focuses on the outcomes and comparisons made throughout the research. In Section 5 we get to the conclusion.

1.1 Problem statement

- Conventional models are not fit for dealing with real-time applications and lack accuracy.
- Consumption time and memory space are very high
- Still, the accuracy level can be improved
- Most of the research work deals with historical records; hence it is essential to deal with the latest dataset.
- Addressing the curse of dimensionality problems

1.2 Research motivation and Contribution

- Understanding the need for classification accuracy in WSN
- Analyzing various literature works evolved for enhancing the classification performance in WSN
- Implementing Multi-Layer Perceptron (MLP), a supervised learning method that improves a system's classification performance
- Comparing the effectiveness of the proposed MLP to current algorithms.

II. Related Work

An Ensemble learning model was presented by Tabbaa et al. [12] to detect assaults in WSN. The author presented an ensemble model for online data analysis, building on the success of the ensemble model in offline data analysis. The method described is an amalgamation of the Hoeffding Adaptive Tree (HAT) algorithm with the Adaptive Random Forest technique (ARF). All four types of attacks—Grayhole, Blackhole, Scheduling, and flooding—were categorised with the use of a WSN-DS. To detect intrusions in WSNs, R Ganesh Babu et al. [13] suggested RBMC-IDS. In order to detect and authenticate cyberattacks, the IDS process makes use of AI computation. Different categorization techniques for detecting DDoS assaults were examined by Elejla et al. [14], including Neural networks, KNNs, Decision trees, Support Vector Machines, and Naive Bayes. The article included topics including attack patterns and network traffic monitoring. Among these, the author stated that KNN is a quicker processing algorithm than the others in determining attacks.

Ifzarne et al. [15] developed an online learning classifier that works based on the collected information to select the appropriate sensor data features. The author performed DoS attack identification using the WSN-DS dataset and an online Passive aggressive method.

Algorithms for machine learning were compared by Ashraf et al. [16], including the popular ones Random Forest, J48, and Naive Bayes. The primary purpose of this study is to quantify Intrusion Detection system detection and accuracy rates. This work is focused on handling a huge amount of data and extracting its new procedures and patterns effectively.

Ugochukwu et al. [17] conducted a comparison work using the KDD Cup'99 dataset. The algorithm considered are Random Tree, Random Forest, Bayes Net, and J48. These algorithms are analyzed based on their accuracy in detecting the attacks. The classification is accomplished using the WEKA tool in which Random Tree and Random Forest are effective with the test datasets. Sujithra et al. [18] reviewed the feature extraction and data preprocessing conducted by various machine learning approaches. The author used Twitter data to predict emotion using machine learning algorithms. Bhumika Gupta et al. [19] discussed the correctness of the models using the trained data. The work is further proceeded to determine the accuracy of each model. A lightweight structure based on incremental learner ensembles was devised by Bosman et al. [20]. The primary goal of this strategy is to detect irregularities in real time for Internet of Things programmes. An innovative Internet of Things online intrusion detection system was

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 2s
DOI: https://doi.org/10.17762/ijritcc.v10i2s.5920
***Article Received**: 18 October 2022 **Revised**: 22 November 2022 **Accepted**: 26 December 2022*

created by Martindale et al. [21]. Several different KDDCup99 subsets are used in a large-scale online analysis (MOA) methodology. The Online Sequential Extreme Learning Machine (OS-ELM), created by Alrashdi et al. [22], employs a voting mechanism to identify outliers. Using the NSL-KDD framework, we analyse how well the suggested system works.

III. Proposed Work

In this study, we suggest using a MLP, an improved form of the classic feed forward neural network, which consists of an input neurons, a fully connected layer, and a pooling neurons. MLPs are efficient in prediction, recognition, pattern classification, and approximation. Initially, the proposed framework begins with preprocessing using the WEKA tool. WEKA is an open-source data preprocessing tool based on the combination of instances, attributes, and the sum of weights. Next, the proposed MLP is applied to the training and testing data. Finally, the obtained results are examined to determine the achieved accuracy rate. Figure 3 demonstrates the proposed architecture and its workflow. Each module involved in the proposed system is discussed in detail in the below sections.

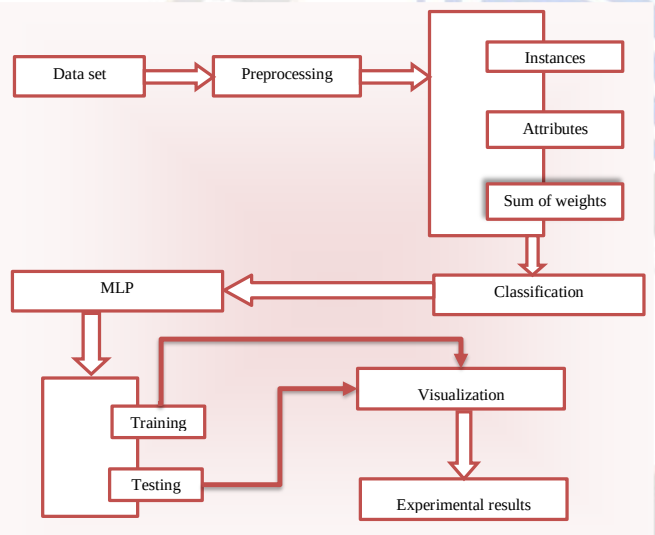

Figure 3: Projected design

3.1 Data preprocessing

Data preprocessing is crucial in machine learning terminology, particularly computational biology. At the training step, it removes extraneous irregular and noisy information from the images. This process is not complicated, but time consumption is high. It is because of multiple stages of data creation and filtering process. Data preprocessing is the combined process of several sub-process such as feature extraction, feature selection, standardization, filtering, instance determination, and transformation. Most approaches demonstrate data preprocessing is common in the machine learning technique.

3.2 Information Mining Tools

WEKA is an open-source tool similar to SAS Enterprise Miner. WEKA is an effective tool that enables the user to modify the calculation's source code. Weka should also allow for re-executing a few common information mining calculations using C4.5, also known as J48. WEKA is more advance than Enterprise Miner, as it can only be used through methods for a graphical user interface (GUI). It makes it difficult to automate tests and is inappropriate for making several investigation types. However, WEKA features a different task mode that makes experimentation simple.

3.3 Multi-Layer Perceptron (MLP)

The proposed MLP is an extension feed-forward ANN mechanism used to classify the input images by mapping them. Mapping is done based on the training and testing dataset's features by employing a back propagation algorithm. The MLP creates nodes as directed graphs that are then connected. Every node in the graph has its own quasi activation function. Additionally, supervised learning approaches were used to train the MLP datasets, which are equally useful for categorizing non-linear data. To resolve the difficulties, it uses a stochastic fitness function.

IV. Result & Discussion

Experimental work is carried out in the WEKA tool. Sensors like baby monitors, lights, motion sensors, security cameras, smoke detectors, sockets, thermostats, TV, and watch are considered to determine classification accuracy. The evaluation factors involved in determining the accuracy level are Recall precision, and F-measure. The dataset with the sensors mentioned above is processed with the WEKA tool by employing the proposed MLP. The obtained results are tabulated and graphically represented for better understanding. Finally, the obtained accuracy rate by the proposed system is compared with the existing Hoeffding adaptive tree mechanism and RBMC-IDS approach.

4.1 Recall

The recall is a value obtained from total correctly classified positive examples from total positive examples. The high recall values, such as a small number of FN, determine the correctly recognized example. Recall can be stated as below;

$$\text{Recall} = \frac{TP}{TP+FN} \quad (1)$$

4.2 Precision

Precision is the value attained by correctly classifying positive examples from total predicted positive examples. The

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 2s
DOI: https://doi.org/10.17762/ijritcc.v10i2s.5920
***Article Received**: 18 October 2022 **Revised**: 22 November 2022 **Accepted**: 26 December 2022*

positive value, such as a small number of FP, determines the high precision. Precision can be stated as below;

$$\text{Precision} = \frac{TP}{TP+FP} \quad (2)$$

4.3 F-measure

F-Measure is measured by evaluating the Recall and Precision. Instead of employing Arithmetic Mean (AM), the F-measures apply Harmonic Mean because AM damages the extreme values. F-Measure is always less than the Recall and precision. F-measure is stated as below;

$$\text{F-measure} = \frac{2*Recall*Precision}{Recall+Precision} \quad (3)$$

Time is taken to build the model: 13.25 seconds

=== Evaluation on training set ===

Time is taken to test the model on training data: 0.06 seconds

=== Summary ===

Table 3: Evaluation metrics and their obtained values

Correctly Classified Illustrations	840	98.3333 %
Incorrectly Classified Illustrations	60	2.6667 %
Kappa indicator		0.925
Mean absolute error		0.0198
Root mean squared error		0.0981
Relative absolute error		10.0018 %
Root relative squared error		31.2244 %
Total Number of Instances		900

As was previously noted, the training dataset test takes 0.06 seconds while the model construction process takes 13.25 seconds. The Kappa statistic, the mean absolute error, the Root mean squared error, the Relative absolute error, and the Root relative squared error are the metrics used to evaluate the effectiveness of machine learning. Out of a total of 900 cases, 840 are properly categorised and 60 are misclassified. Percentages indicate the sum of the values obtained for the evaluation measures; see table 3.

=== Detailed Accuracy by Class ===

Table 4: Prediction table

TP Rate	FP Rate	Precision	Recall	F-Measure	MCC	ROC Area	PRC Area	Class
1.000	0.000	1.000	1.000	1.000	1.000	1.000	1.000	Baby monitor
0.800	0.050	0.667	0.800	0.727	0.693	0.969	0.710	lights
1.000	0.000	1.000	1.000	1.000	1.000	1.000	1.000	motion sensor
1.000	0.000	1.000	1.000	1.000	1.000	1.000	1.000	security camera
1.000	0.000	1.000	1.000	1.000	1.000	1.000	1.000	smoke detector
0.600	0.025	0.750	0.600	0.667	0.635	0.969	0.789	socket
1.000	0.000	1.000	1.000	1.000	1.000	1.000	1.000	thermostat
1.000	0.000	1.000	1.000	1.000	1.000	1.000	1.000	TV
1.000	0.000	1.000	1.000	1.000	1.000	1.000	1.000	watch

=== Confusion Matrix ===

```
  a  b  c  d  e  f  g  h  i  <-- classified as
100  0  0  0  0  0  0  0  0 |
  0 80  0  0  0 20  0  0  0 |
  0  0 100  0  0  0  0  0  0 |
  0  0  0 100  0  0  0  0  0 |
  0  0  0  0 100  0  0  0  0 |
  0 40  0  0  0 60  0  0  0 |
  0  0  0  0  0  0 100  0  0 |
  0  0  0  0  0  0  0 100  0 |
  0  0  0  0  0  0  0  0 100 |
```

The models' predictions are TP Rate, FP Rate, Precision, Recall, F-Measure, MCC, ROC Area, and PRC Area concerning the class. The obtained values respective to each parameter are mentioned in the above table 4. The obtained values are in tabular format; hence it is known as a confusion matrix.

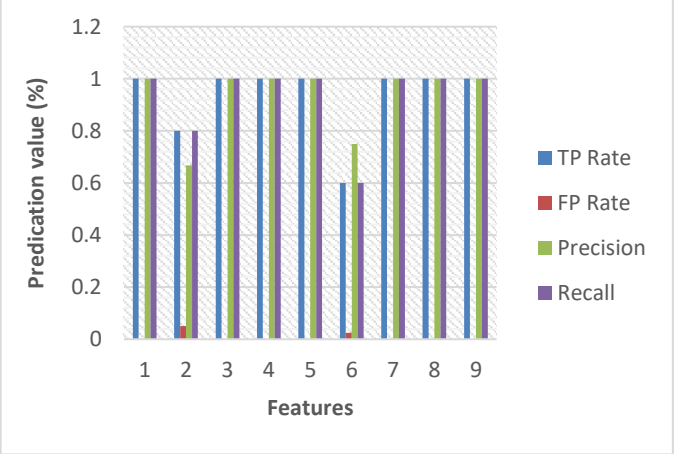

Figure 4: Predication value vs. Features

Figure 4 determines the features and their prediction values. The x-axis shows the prediction values in percentage, and the y-axis shows the features. The prediction parameters are TP rate, FP rate, Precision, and Recall.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 2s
DOI: https://doi.org/10.17762/ijritcc.v10i2s.5920
***Article Received**: 18 October 2022 **Revised**: 22 November 2022 **Accepted**: 26 December 2022*

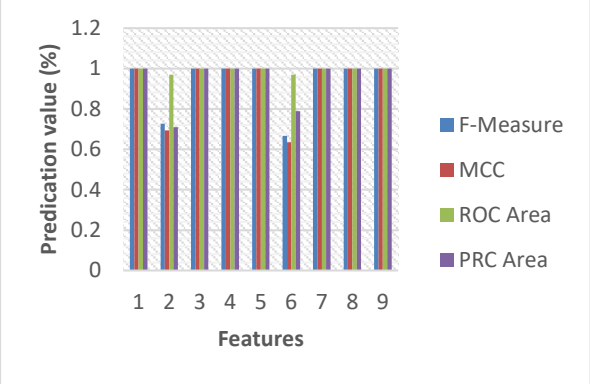

Figure 5: Predication value vs. Features

Figure 5 determines the features and their prediction values. The x-axis shows the prediction values in percentage, and the y-axis shows the features. The prediction parameters are F-Measure, MCC, ROC Area, and PRC Area.

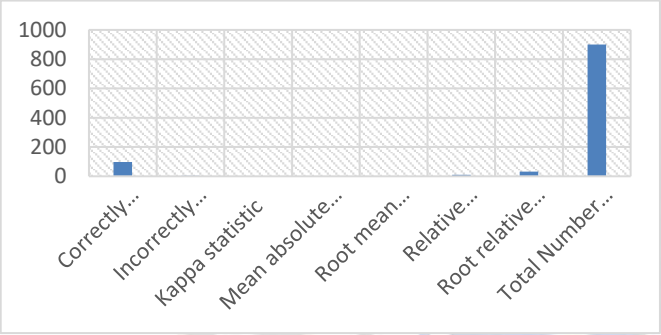

Figure 5: Summary report

Figure 6 shows the summary report of the proposed execution. It is the graphical representation of Evaluation metrics and their obtained values.

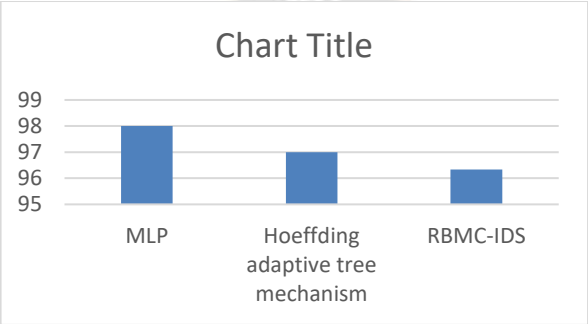

Figure 7: Comparison report on the accuracy

Table 7: Comparison table for accuracy

Algorithms	Accuracy in %
MLP	98
Hoeffding adaptive tree mechanism	97
RBMC-IDS	96.33

Figure 7 shows the comparison work conducted between the proposed MLP with Hoeffding adaptive tree mechanism and RBMC-IDS. The obtained values are mentioned in the above table 7. The values are plotted with the algorithms on the x-axis; the obtained values in percentage on the y-axis. According to this, the proposed MLP accurate rate is 98% which is better than the algorithms Hoeffding adaptive tree mechanism with 97% and RBMC-IDS with 96.33%.

V. Conclusion

The proposed work Multi-Layer Perceptron (MLP) for enhancing classification accuracy using machine learning procedures. This work focused on improving accuracy concerning real-time scenarios and huge datasets. Various works related to classification accuracy are discussed in the related work section. It motivates several ideas for developing the proposed mechanism. The MLP is a popular machine learning approach under a supervised learning model. Initially, the proposed framework begins with data preprocessing, and the contained results undergo classification in the WEKA. WEKA is an open-source tool for the classification of the dataset. Here, MLP applies mapping based on the training and testing dataset's features by employing a backpropagation algorithm. The obtained accuracy performance of the proposed MLP is obtained through the experimental work. Next, a comparison work is carried out between the proposed MLP with the Hoeffding adaptive tree mechanism and RBMC-IDS. 98% accuracy in comparisons using the suggested MLP demonstrates its effectiveness.

In the future, we will improve the performance of our system using second layer of this multi-layer detection model uses deep learning to detect more types of attacks, which appear in the second layer of the WSN.

References

[1] Marriwala N and Rathee P. An approach to increasing the wireless sensor network lifetime. The 2012 World Congress on Information and Communication Technologies, pages 495–499. IEEE, 2012.

[2] Nedumaran A, Ganesh Babu R, Kass MM and Karthika P. 2020. Machine Level Classification Using Support Vector Machine. AIP Conference Proceedings of International Conference on Sustainable Manufacturing, Materials and Technologies (ICSMMT 2019). vol. 2207, pp.020013-1020013-10, October 25-26.

[3] Rami Ahmad, Raniyah Wazirali, and Tarik Abu-Ain, "Machine Learning for Wireless Sensor Networks Security: An Overview of Challenges and Issues," Sensors 2022, 22, 4730. https://doi.org/10.3390/s22134730

[4] Lee, C.C. Security and privacy in wireless sensor networks: Advances and challenges. Sensors 2020, 20, 744

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 10 Issue: 2s
DOI: https://doi.org/10.17762/ijritcc.v10i2s.5920
***Article Received**: 18 October 2022 **Revised**: 22 November 2022 **Accepted**: 26 December 2022*

[5] Finogeev, A.G.; Finogeev, A.A. Information attacks and security in wireless sensor networks of industrial SCADA systems. ACM Int. Conf. Proc. Ser. 2020

[6] Endut n, Hamzah WMAFW, Ismail I, Yusof MK, Abu Baker Y, YusoffH. A Systematic Literature Review on Multi-Label Classification based on Machine Learning Algorithm. TEM Journal. 11; 2: 658-666, ISSN 2217-8309, DOI: 10.18421/TEM112-20, May 2022.

[7] Kotsiantis SB. Supervised Machine Learning: A Review of Classification Techniques. Informatica 31 (2007) 249–268 251

[8] Muhammad Rana, Quazi Mamun, Rafiqul Islam. Lightweight cryptography in IoT networks: A survey, Future Generation Computer Systems,Volume 129, 2022, Pages 77-89, ISSN 0167-739X.

[9] Cui, L., Yang, S., Chen, F. et al. A survey on application of machine learning for Internet of Things. Int. J. Mach. Learn. & Cyber. 9, 1399–1417 (2018).

[10] Kumar DP, Amgoth T, Annavarapu CSR. Machine learning algorithms for wireless sensor networks: A survey. Inf. Fusion. 2019; 49: 1–25

[11] Agarwal A, Sharma P, Alshehri M, Mohamed AA, Alfarraj O. Classification model for accuracy and intrusion detection using machine learning approach. PeerJ Comput Sci. 2021 Apr 7;7:e437. doi: 10.7717/peerj-cs.437.

[12] Tabbaa H and Ifzarne S. An Online Ensemble Learning Model for Detecting Attacks In Wireless Sensor Networks. IOP Conf. Ser.: Mater. Sci. Eng. 1055 012089

[13] Babu RG, Vijay M, Parameswaran G, Anandhan C and Maurya S. Intrusion Detection Using Machine Learning in Sensor Network. IOP Conf. Ser.: Mater. Sci. Eng. 1055 012089

[14] Elejla OE, Belaton B, Anbar M, Alabsi B and Al-Ani AK. (2019). Comparison of Classification Algorithms on ICMPv6-Based DDoS Attacks Detection Lecture Notes in Electrical Engineering (2018): n. pag.

[15] Ifzarne S, Tabbaa H, Hafidi I and Lamghari N. Anomaly detection using machine learning techniques in wireless sensor networks. In Journal of Physics: Conference Series. 1743: 012021. IOP Publishing, 2021.

[16] Ashraf N, Ahmad W, Ashraf R. 2018. A comparative study of data mining algorithms for high detection rate in the intrusion detection system. Annals of Emerging Technologies in Computing 2(1):49–57.

[17] Ugochukwu CJ, Bennett EO, Harcourt P. 2018. An intrusion detection system using a machine learning algorithm. International Journal of Computer Science and Mathematical Theory 4(1):2545–5699

[18] Kawade, Dipak R., and Kavita S. Oza. "Sentiment analysis: machine learning approach." International Journal of Engineering and Technology 9, no. 3 (2017): 2183-2186

[19] Cliche, Mathieu. "BB_twtr at SemEval-2017 task 4: Twitter sentiment analysis with CNNs and LSTMs." arXiv preprint arXiv:1704.06125 (2017).

[20] Hedde HWJ Bosman, Giovanni Iacca, Arturo Tejada, Heinrich J Wörtche, and Antonio Liotta. Ensembles of incremental learners to detect anomalies in ad hoc sensor networks. ad hoc networks, 35:14–36, 2015.

[21] Nathan Martindale, Muhammad Ismail, and Douglas A Talbert. Ensemble-based online machine learning algorithms for network intrusion detection systems using streaming data. Information, 11(6):315, 2020

[22] Ibrahim Alrashdi, Ali Alqazzaz, Raed Alharthi, Esam Aloufi, Mohamed A Zohdy, and Hua Ming. Fbad: Fog-based attack detection for IoT healthcare in smart cities. In 2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), pages 0515–0522. IEEE, 2019.

[23] Gopalakrishnan Subburayalu, Hemanand Duraivelu, Arun Prasath Raveendran, Rajesh Arunachalam, Deepika Kongara & Chitra Thangavel (2021) Cluster Based Malicious Node Detection System for Mobile Ad-Hoc Network Using ANFIS Classifier, Journal of Applied Security Research, DOI: 10.1080/19361610.2021.2002118

[24] S. Srinivasa Rao, K. Chenna Keshava Reddy and S. Ravi Chand (2022), A Novel Optimization based Energy Efficient and Secured Routing Scheme using SRFIS-CWOSRR for Wireless Sensor Networks. IJEER 10(3), 644-650. DOI: 10.37391/IJEER.100338.

[25] G. Vinoda Reddy, Kavitha Thandapani, N. C. Sendhilkumar, C. Senthilkumar, S. V. Hemanth, S. Manthandi Periannasamy and D. Hemanand (2022), Optimizing QoS-Based Clustering Using a Multi-Hop with Single Cluster Communication for Efficient Packet Routing. IJEER 10(2), 69-73. DOI: 10.37391/IJEER.100203

[26] Ruili Wang, Wanting Ji, "Computational Intelligence for Information Security: A Survey", IEEE Transactions on Emerging Topics in Computational Intelligence, vol.4, no.5, pp.616-629, 2020.