

Intrusion detection in clustering wireless network by applying extreme learning machine with deep neural network algorithm

Palaniraj Rajidurai Parvathy¹, Satheeshkumar Sekar¹, Bharat Tidke², Rudraraju Leela Jyothi³,
Venugopal Sujatha⁴, Madappa Shanmugathai⁵, Subbiah Murugan⁶

¹Project Manager, Mphasis Corporation, Chandler, Arizona, United States of America

²Symbiosis Institute of Technology Nagpur Campus, Symbiosis international (Deemed) University, Pune, India

³Department of Computer Science and Engineering, Sagi Rama Krishnam Raju Engineering College (A), Bhimavaram, India

⁴Department of Computer Applications, S.A. Engineering College, Chennai, India

⁵Department of English, Sri Sairam Engineering College, Chennai, India

⁶Department of Biomedical Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Saveetha University, Chennai, India

Article Info

Article history:

Received Feb 24, 2024

Revised Oct 26, 2024

Accepted Nov 11, 2024

Keywords:

Clustering

Deep neural network

Extreme learning machine
algorithm

Intrusion detection

Wireless network

ABSTRACT

Nowadays, intrusion detection systems (IDSs) have growingly come to be considered as an important method owing to their possible to expand into a key factor, which is crucial for the security of wireless networks. In wireless network, when there is a thousand times more traffic, the effectiveness of normal IDS to identify hostile network intrusions is decreased by an average factor. This is because of the exponential growth in network traffic. This is due to the decreased number of possibilities to discover the intrusions. This is because there are fewer opportunities to see possible risks. We intend an extreme learning machine with deep neural network (DNN) algorithm-based intrusion detection in clustering (EIDC) wireless network. The main objective of this article is to detect the intrusion efficiently and minimize the false alarm rate. This mechanism utilizes the extreme learning machine (ELM) with a deep neural network algorithm for optimizing the weights of input and hidden node biases to deduce the network output weights. Simulation outcomes illustrate that the EIDC mechanism not only assures a better accuracy for detection, considerably minimizes an intrusion detection time, and shortens the false alarm rate.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Bharat Tidke

Symbiosis Institute of Technology Nagpur Campus, Symbiosis international (Deemed) University

Pune, India

Email: batidke@gmail.com

1. INTRODUCTION

Because of the enhanced association between nodes, the receptivity of wireless network operation areas, and the transition capability, the wireless network is susceptible to intrusions. This results in a significant increase in the disclosure of dangers that intimidate the availability of information systems in the network system infrastructure [1]. An IDS to observe, identify, and notify about hostile activity [2]. Several studies analyze the detection and prevention models; moreover, there needs to be more consistency in the opportunistic developments in the models [3]. In addition, the currently used models come with a number of restrictions that need to be investigated before any new security models can be developed. IDS stands for intelligent data security and is a system that coordinates the operations of hosts and networks. This performs an analysis of the packets that are being transported over the network, searches for potentially malicious occurrences, and then processes the alert signal [4]. IDS have garnered much attention, and several prominent

models have been presented to create an intensive security framework. Within this framework, the function of IDS is to examine the fresh difficulties to discover viable ways to solve the concerns in the detection models. The various current detection methods in terms of performance, usage of available bandwidth, amount of time required for detection, and overloading of processors [5].

It is a major issue that may lead to a breach in security and is one of the key causes of security breaches since a single instance of intrusion can remove data from a wireless network in seconds or delete it totally. Since, intrusion is one of the primary causes of security breaches [6]. An intrusion might potentially cause physical damage to a network. In addition, an intrusion may result in massive financial losses and put the crucial infrastructure of information technology at risk, which can eventually contribute to an information disadvantage in the event of a cyber-conflict. Consequently, both the prevention of intrusions and the identification of those that have already occurred are obligatory and essential tasks [7].

The accuracy of these many ways for detecting intrusions is still an issue since accuracy is based on the detection rate as well as the rate of false alarms. Although there are a range of methods for detecting intrusions, the accuracy of these methods still needs to be improved. Finding a solution to the problem of accuracy is important in order to reduce the false alarm count and increase the proportion of successful detections [8]. The investigation that was carried out was prompted by the notion that was presented here. The support vector machine (SVM), random forest (RF), and ELM techniques are all methods that have been proven to be effective in their ability to tackle the classification task. Compared to the SVM, RF, and ELM mechanisms, the ELM algorithm performs better than other algorithms [9].

In order to identify intrusions, an IDS was used, and for this purpose, ML algorithms were utilized. Traditional ML algorithms, such as the SVM, the knee-highest neighbor (KNN), and filter-based feature selection, often resulted in inaccurate classifications and low levels of precision. The method is the Boruta feature selection with grid search random forest (BFSF). The objective of this algorithm is to enhance the classifier's performance by using a feature selection approach. BFSF mechanism that formulates a free-from-noise as well as false forecasting. However, This mechanism increases the training time during arriving new attacks [10].

It is an IDS's role to notice any acts that might possibly be detrimental. It may refer to a broad group of systems, the input of which is a traffic source and the output of which is a classification judgment on whether or not a given instance is malicious. Host-based and network-based IDS are two primary classifications. IDS that are host-based gather data from the immediate area, but IDS that are network-based have access to information on a global scale. Either individual network packets or the whole flow of packets may be examined and analyzed in order to determine whether or not a certain action on the network is harmful. From the moment they are conceived until the moment they are put into operation, network IDS are faced with a challenge in the form of a rise in the count of associated devices and a continual development in the methods and strategies that attackers use. This technique separates the risk of malevolent behavior depending on ML [11].

An enhanced deep belief network (DBN). Traditional neural network training techniques, such as Back Propagation (BP), begin training a model with fixed parameters, such as the randomly initialized weights and thresholds. This might bring about certain drawbacks, such as drawing the model to the local optimum solutions or needing a lengthy training time, but it is still the most common approach. Kernel-based extreme learning machine (KELM) that has the capability of supervised learning and will restore the Back Propagation method. In light of the issue of inadequate classification operation explicitly often brought on by arbitrarily launching kernel parameters with KELM, an improved grey wolf optimizer (EGWO) has been developed to optimize the network. A unique optimization approach that combines inner and outer hunting has been created to increase the search as well as optimization ability [12].

A technique for detecting network intrusion by applying decision tree (DT) double SVM with hierarchical clustering. This approach is able to identify a variety of various types of IDS successfully. To begin, the hierarchical clustering algorithm is used to build the DT for the network traffic data. The bottom-up merging method is utilized in order to enhance the disconnection of the upper nodes that, in turn, minimizes the error collection that occurs during the building of the DT. The intrusion detection model is then implemented by embedding twin SVM into the created DT. This model is able to identify the intrusion type [13] successfully. The IDS are based on deep learning (DL) and presents an in-depth review as well as a categorization of these schemes. It does this by dividing these strategies into categories by the many kinds of DL approaches that are used in each of them. It explains how accurate recognition of intrusions may be achieved via DL networks in intrusion detection [14].

ML-based Network IDS functions on flow characteristics gathered via flow exportation mechanisms. These features are used to detect and prevent network intrusions. The ML and DL-based NIDS solutions presuppose that flow information is received from all the packets that make up the flow. Even if sampling is present, it is possible to conduct a reliable assessment of ML-based NIDSs by analyzing the

effect that packet sampling has on the performance and efficiency of these systems. As a result of our sampling studies, we discovered that malicious flows of a smaller size (in terms of the number of packets), have a higher probability of going undetected even with low sample rates. Following that, using the assessment process that had been suggested, we studied the influence that different sampling strategies had on the NIDS detection rate as well as the false alarm [15].

A network IDS operates on the principle of self-supervised learning and makes it possible to do hierarchical detection. The method that has been offered consists of various phases of detection, one of which is the early identification of extreme outliers, which, if left unchecked, might do significant harm to the system. In addition, it does in-depth reexaminations by using the hidden areas with specialized anomaly scores, which ultimately results in high detection accuracy [16]. Unsupervised machine learning methods are especially attractive to IDS because of their ability to identify known and undiscovered forms of assaults, in addition to zero-day intrusions. An unsupervised anomaly detection approach that detects assaults without any previous information by combining sub-space clustering and one class SVM [17].

The performance and prediction accuracy of anomaly-based ML-enabled IDS (AML-IDSs) during detecting intrusions is much lower than that of DL IDS. Particularly ineffective in detecting intrusions are AML-IDS systems that make use of low-complexity models, such as the principal component machine approach and the one-class SVM algorithm. Additionally, the differences between the data used for testing and the data used for training lead to a progressively greater percentage of false positives, which have low rates of false alarms and high levels of predictability. The use of optimization strategies to improve the performance of single-learner [18].

IDS is established on ML to ensure security. The big data-based hierarchical DL system makes use of both behavioral and content aspects in order to get an understanding of the characteristics of network traffic as well as data that is carried in the payload. Every DL model part of the BDHDLs focuses all its attention and energy on mastering one cluster's particular data distribution. Compared to the systems that relied on a single learning model in the past, this method has the potential to have a higher rate of detection for intrusive attacks [19]. IDS utilizes a deep learning algorithm for observing critical structures and detecting the intrusion sensor node present in the network. However, this mechanism raises the false alarm rate [20]. Sample chosen ELM method can store exceptionally huge volumes of training data. As a result, they are saved, calculated, and sampled by the servers housed in the cloud. After that, the chosen specimen is sent as training material to the hosts of the fog nodes. Although it is a lightweight method, the intrusion detection process using it takes a much longer period of time [21]. Deep extreme learning machine (DELM) that initially builds the evaluation of safety characteristics, which leads to their importance and then creates an adaptive IDS focused on the relevant characteristics. DELM stands for deep learning extreme machine. The DELM-based IDS carries out dataset evaluations and analyzes the performance aspects to evaluate the system's dependability [22].

IDS, which is based on deep learning with ELM, is made up of numerous auto-encoders to extract in-depth features from the initial input. Following that, the extracted features are inserted into the ELM at the very bottom of the hidden layers using supervised learning in order to recognize the various forms of attacks. However, it requires a large amount of time to detect an abnormal node [23]. The network security in cyberspace mechanism scope is to examine ML methods for cyber security concentrating on regions for example intrusion detections, spam detections, and malware detections on network [24], [25]. The ML algorithm utilized to improve the Sports and fitness [26]. It can examine a huge volume of data, find patterns, and it improve the performance and training [27].

2. PROPOSED METHOD

2.1. Network creation

The number of wireless nodes installed in the region being monitored and these nodes self-organize into a network. The network contains several wireless nodes, base station (BS) and user. The wireless network is clustered to make administration processes as simple as possible in order to guarantee the network's consistent functioning. The wireless node energy, distance between node and BS, and communication ratio parameters decide the cluster head (CH). The CH nodes broadcast the data that they have gathered to the BS node via a multi-hop relay, and this data eventually makes its way to the user via the Internet. Through the user has the ability to remotely set up or administer the network, as well as perform monitoring tasks. Figure 1 explains the architecture of the EIDC mechanism.

From Figure 1, three components make up the network: a number of sensor nodes that are dispersed over the observing region, BS that is spread, and a user. The following are the roles that each component plays: i) sensor: this element of the WSN serves as the network's foundation and its primary responsibility is to gather the data of every range, process the information that has been gathered, and then send the processed data to the higher node. This component contains both usual sensor nodes and CH nodes, ii) BS: combines

the data that is supplied by the CH sensor, and next sends it to the user via internet, and iii) user: this node is geared toward the end user.

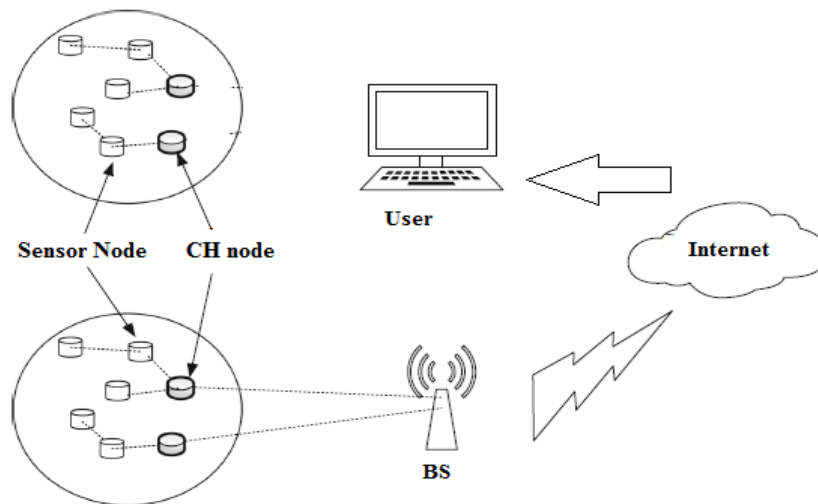


Figure 1. Architecture of EIDC mechanism

Utilized to monitor the operational condition, carry out intrusion detection and analysis on the data that is forwarded by the BS, and carry out functions that are appropriate to these tasks. In addition, the user has the capability of actively transmitting a query request to the wireless network. It has both usual sensor nodes and CH nodes within its structure. In order to sense and gather data in the monitoring region, usual sensor nodes are used, and CH nodes are utilized to summarize the data supplied by current typical nodes. It is responsible for the collection of information. First, all of the data that has been transmitted by the network and CH nodes is gathered. After that, the data are combined, and the characteristics of the IDS is derived.

2.2. Intrusion detection system

The intrusion detection module is in charge of receiving data information from the BS and assessing possible intrusions. Because it is the most important component of an IDS, this module's success is directly tied to the precision and timeliness of the data and information analysis it does. For prediction and classification of the testing dataset, this module uses the ELM detection method as a classifier. The output of the ELM is handling anomaly that is responsible for analyzing the final result and taking the appropriate actions in response.

2.2.1. ELM with DNN-based IDS

This mechanism utilizes an ELM mechanism, and it is a combination of DNN with a hidden layer. It is a possibility based on several wireless node attack detection to follow incidents in a wireless network. It has been shown that ELM, an example of a single-hidden-layer feed-forward neural network, is beneficial for the IDS.

The ELM is a basic and efficient approach that does not need any training data to perform to its full potential. Instead, a least-squares solution is used to generate the output weights, and the weights of the hidden layer are initialized with an arbitrary beginning point. While the weights of the hidden layer are initialized, they are also given an arbitrary beginning point. ELM may be taught in a very short amount of time. This is because the weights of the hidden layer are launched based on an arbitrary value, but the weights of the output layer is generated with a solution that is established on the least squares. This leads to the observed result. ELM is qualified by a great degree of accuracy. This is since the solution that employs least squares guarantees that the output weights are optimized for the data that was trained on. The level of background noise that ELM can tolerate is rather high. This is because the initialization of the hidden layer is established on arbitrary integers that serve to prevent the wireless network from overfitting the training data. The reason for this can be seen in the previous sentence. The ELM is effective in detecting a variety of intrusions and it has a greater computing capability, better learning ability, and quicker training speed. This is

because there is no pre-existing feedback error iteration computation. Figure 2 explains the structure of ELM with the DNN algorithm.

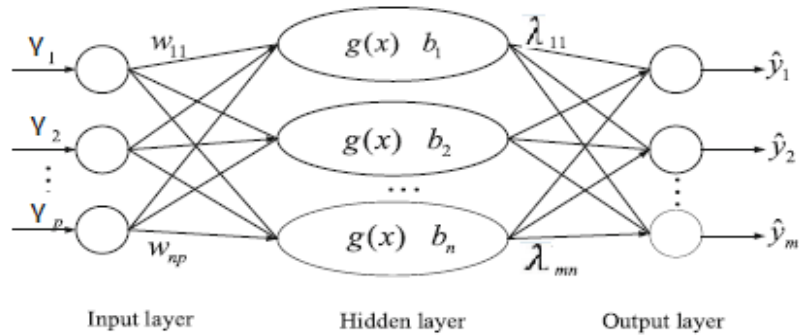


Figure 2. Structure of ELM with DNN algorithm

From Figure 2, d represents the count of input layer nodes, k indicates the count of hidden layer nodes, and n denotes the count of output layer nodes. The training samples are $\gamma_1; \gamma_2; \dots; \gamma_d$, and the equivalent labels are $l_1; l_2; \dots; l_k$. ω_j depicts the weight vector among the hidden as well as the input layer j^{th} node, λ indicates the matrix of weight, λ_j indicates the weight vector between the j -th node for the hidden layer and the input layer, b_j represents the bias value of the j^{th} node in the hidden layer. The ELM method output and K hidden neurons is conveyed as (1) and the output matrix hidden layer is denoted as (2).

$$Y = \sum_{j=1}^K \lambda_j g(\omega_j^T + b_j) \tag{1}$$

$$H = \begin{bmatrix} g(\omega_1^T \gamma_1 + b_1) & \dots & g(\omega_1^T \gamma_d + b_1) \\ \vdots & \ddots & \vdots \\ g(\omega_k^T \gamma_1 + b_k) & \dots & g(\omega_k^T \gamma_d + b_k) \end{bmatrix} \tag{2}$$

Here, $h(x_j) = g(\omega_j^T \gamma_j + b_j)$ denotes the hidden layer function that is linked to γ_j . After that, the purpose of optimization ELM is specified in (3). Here, R indicates the regularization factor. Furthermore, the categorization of the ELM can be conveyed as (4).

$$\min_{\lambda} \|H\lambda - T\|^2 + \frac{R}{2} \|\lambda\|^2 \tag{3}$$

$$f(x) = \text{sign} \left(h(x)H^T \left(\frac{Y}{C} + HH^T \right)^{-1} T \right) \tag{4}$$

ELM is adapted by updating the input weights variables and the hidden biases to reach more accuracy. This method raises the accuracy. This is used to build the network weights of output. Owing to, it is feasible to optimize the weights of input as well as the biases of hidden node. In this mechanism, the data is collected may comprise the activity of user, traffic of the network, and logs system. Gathered data from traffic can be examined to spot abnormal patterns in that travel, for example, a raise packet count arriving from a sender. The system action logs may be analyzed to determine abnormal happenings, for example, a quick rise in the count of ineffective efforts to log in. Data on user action may be examined to determine abnormal user patterns behaviour, that is an unexpected increase in the amount of items that are being transferred.

The features that are elicited from the data may be applied to depict the data in a method that the IDS more promptly realizes. The ports employed by the sender IP address and the receiver IP address sort data packets, which are forwarded and remove data from traffic. The hosts of the sender and receiver, the occurrence of the time and date, and other applicable data may be recovered from the logs system. The file name, and user's name that are admittance, and access time and date may be among the expressions gained from the user's activity data. After the model has been "trained" on the extracted features, it may be applied

to the data in order to classify it as normal or abnormal. To do this, a comparison will be made between the model that has been trained and the new data. When the model discovers an anomaly, it is possible to use it to determine whether or not an intrusion has occurred, depending on whether or not the abnormality is present.

2.2.2. Intrusion detection procedure

This mechanism utilizes the EIDC method to categorize the data. Initially, the raw data is treated utilizing data processing to create it better approachable. In the following procedure, "training", in which EIDC is subjected to normal as well as attack data. In the categorization, the fundamental features communicate to the two categories of normal as well as intrusion, while in the event of multi-class categorization, the characteristics class communicate to normal as well as several types of attack. This mechanism procedure is specified below:

Assume M arbitrary nodes, K hidden nodes and P denotes the action function. Launched every node individual factor vector that comprise parameters of an entire hidden nodes. It contains three functions, such as node creation, intersects, and picked-out forwarder node, that are accomplished to generate the vector for the new node. This procedure is repeated till the discontinue situation is fulfilled. Build a perfect estimating model with better accuracy of testing by altering the type of P and raising the K count increasingly from one. Decide the weights of output λ , Y_{alt} , and T . Then, compare existing and proposed mechanism forecasting and relate their accurateness.

3. EXPERIMENTAL RESULTS

This study uses the NSL knowledge discovery and data mining (KDD) dataset [28], which is an updated version of the original KDD dataset and is acknowledged as a standard in the assessment of algorithms for intrusion detection. We dealt with the experiments utilizing the ELM algorithm and the EIDC mechanism to evaluate the effect that features on the function of the model [29]. The ELM algorithm optimizes the network weights of output and the hidden node parameters. The EILM mechanism has the potential to reach a better accuracy.

Figure 3 explains the amount of time essential to identify an intrusion and the accuracy level reached by the BFSF and EIDC mechanisms. From Figure 3, the proposed mechanism has the greatest accuracy percentage than the existing EIDC mechanism. The EIDC mechanism reaches 97%, but the existing mechanism reaches only 80%. The ELM is effective in detecting a variety of intrusions and it has a greater computing capability, better learning ability, and quicker training speed. This is because there is no pre-existing feedback error iteration computation. Figure 4 explains the detection accuracy comparison among BFSF and EIDC mechanisms based on wireless nodes.

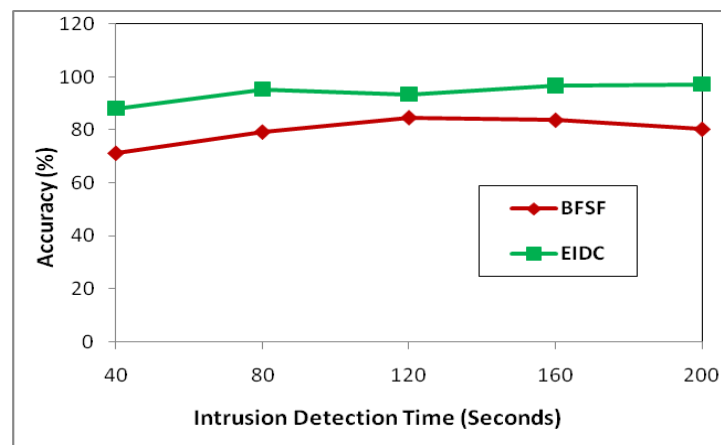


Figure 3. Percentage of detection accuracy for BFSF and EIDC mechanisms based on intrusion detection time

Figure 4 displays that when the wireless node count is raised from 40 to 200, the percentage of detection accuracy is reduced. Proposed EIDC mechanism, compared to the baseline BFSF mechanism, the EIDC mechanism provides the highest intrusion detection accuracy since it utilizes the ELM with DNN

algorithm to detect the intrusion well. At present, with 200 wireless nodes, the percentage of detection accuracy is 97%. However, the existing BFSF mechanism detection ratio is only 65.82%. Since the EIDC mechanism improves the scalability performance. Figure 5 explains the False alarm rate for BFSF and EIDC mechanisms based on Wireless Nodes between 40 to 200.

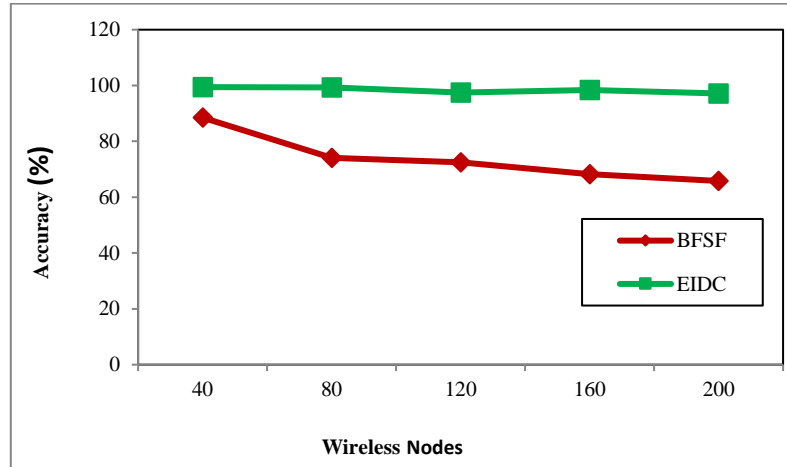


Figure 4. Percentage of accuracy for BFSF and EIDC mechanisms based on wireless nodes

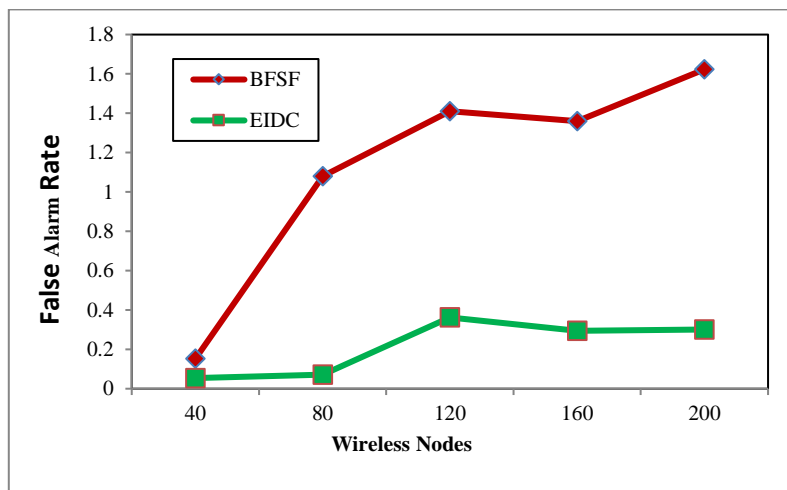


Figure 5. False alarm rate for BFSF and EIDC mechanisms based on wireless nodes

The EIDC mechanism compares to the BFSF mechanism; the EIDC mechanism's false alarm rate is below 0.5% at 200 wireless nodes. It detects the intrusion efficiently by applying ELM with the DNN algorithm. However, the existing BFSF mechanism has a higher false alarm rate; that is, the false alarm rate percentage value is 1.63% at 200 wireless nodes. The ELM is a basic and efficient approach that does not need any training data to perform to its full potential. The ELM is effective in detecting various intrusions and minimizes the false alarm rate.

4. CONCLUSION

In wireless networks, intrusion detection is a necessary and significant parameter. This article presents an extreme learning machine (ELM) with DNN-based Intrusion detection in a clustering wireless network. The introduced method can remove more interpreter characteristics and enhance intrusion detection accuracy. Initially, the wireless network is clustered to make administration processes as simple as possible in order to guarantee the network's consistent functioning and select the CH based on node ability. This

mechanism utilizes an ELM mechanism, a combination of DNN with a hidden layer, which is a possibility based wireless node attack detection. Then, we, using the Simulation outcomes, demonstrate that the EIDC mechanism enhances the detection accuracy and shortens the time for intrusion detection compared to the baseline mechanism. Furthermore, it minimizes the false alarm rate. Yet, the EIDC mechanism using the static nodes, in the future, gives the mobility parameter and separates which types of attacks in wireless networks.




REFERENCES

- [1] S. Maesaroh, L. Kusumaningrum, N. Sintawana, D. P. Lazirkha, and R. D. O., "Wireless network security design and analysis using wireless intrusion detection system," *International Journal of Cyber and IT Service Management*, vol. 2, no. 1, pp. 30–39, Feb. 2022, doi: 10.34306/ijcitsm.v2i1.74.
- [2] R. Kumar, A. Malik, and V. Ranga, "An intellectual intrusion detection system using hybrid hunger games search and remora optimization algorithm for IoT wireless networks," *Knowledge-Based Systems*, vol. 256, p. 109762, Nov. 2022, doi: 10.1016/j.knosys.2022.109762.
- [3] M. J. Kumar, S. Mishra, E. G. Reddy, M. Rajmohan, S. Murugan, and N. A. Vignesh, "Bayesian decision model based reliable route formation in internet of things," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 34, no. 3, pp. 1665–1673, Jun. 2024, doi: 10.11591/ijeecs.v34.i3.pp1665-1673.
- [4] M. Amru *et al.*, "Network intrusion detection system by applying ensemble model for smart home," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 14, no. 3, pp. 3485–3494, Jun. 2024, doi: 10.11591/ijece.v14i3.pp3485-3494.
- [5] A. Heidari and M. A. Jabraeil Jamali, "Internet of Things intrusion detection systems: a comprehensive review and future directions," *Cluster Computing*, vol. 26, no. 6, pp. 3753–3780, Dec. 2023, doi: 10.1007/s10586-022-03776-z.
- [6] S. Ghayyad, S. Du, and A. Kurien, "The flaws of internet of things (IoT) intrusion detection and prevention schemes," *International Journal of Sensor Networks*, vol. 38, no. 1, pp. 25–36, 2022, doi: 10.1504/IJSNET.2022.120270.
- [7] M. Prasad, S. Tripathi, and K. Dahal, "An intelligent intrusion detection and performance reliability evaluation mechanism in mobile ad-hoc networks," *Engineering Applications of Artificial Intelligence*, vol. 119, p. 105760, Mar. 2023, doi: 10.1016/j.engappai.2022.105760.
- [8] C. Zhang, D. Jia, L. Wang, W. Wang, F. Liu, and A. Yang, "Comparative research on network intrusion detection methods based on machine learning," *Computers & Security*, vol. 121, p. 102861, Oct. 2022, doi: 10.1016/j.cose.2022.102861.
- [9] I. Ahmad, M. Basher, M. J. Iqbal, and A. Rahim, "Performance comparison of support vector machine, random forest, and extreme learning machine for intrusion detection," *IEEE Access*, vol. 6, pp. 33789–33795, 2018, doi: 10.1109/ACCESS.2018.2841987.
- [10] S. Subbiah, K. S. M. Anbananthen, S. Thangaraj, S. Kannan, and D. Chelliah, "Intrusion detection technique in wireless sensor network using grid search random forest with Boruta feature selection algorithm," *Journal of Communications and Networks*, vol. 24, no. 2, pp. 264–273, Apr. 2022, doi: 10.23919/JCN.2022.000002.
- [11] G. De Carvalho Bertoli *et al.*, "An end-to-end framework for machine learning-based network intrusion detection system," *IEEE Access*, vol. 9, pp. 106790–106805, 2021, doi: 10.1109/ACCESS.2021.3101188.
- [12] Z. Wang, Y. Zeng, Y. Liu, and D. Li, "Deep belief network integrating improved kernel-based extreme learning machine for network intrusion detection," *IEEE Access*, vol. 9, pp. 16062–16091, 2021, doi: 10.1109/ACCESS.2021.3051074.
- [13] L. Zou, X. Luo, Y. Zhang, X. Yang, and X. Wang, "HC-DTTSVM: a network intrusion detection method based on decision tree twin support vector machine and hierarchical clustering," *IEEE Access*, vol. 11, pp. 21404–21416, 2023, doi: 10.1109/ACCESS.2023.3251354.
- [14] J. Lansky *et al.*, "Deep learning-based intrusion detection systems: a systematic review," *IEEE Access*, vol. 9, pp. 101574–101599, 2021, doi: 10.1109/ACCESS.2021.3097247.
- [15] J. Alikhanov, R. Jang, M. Abuhamad, D. Mohaisen, D. Nyang, and Y. Noh, "Investigating the effect of traffic sampling on machine learning-based network intrusion detection approaches," *IEEE Access*, vol. 10, pp. 5801–5823, 2022, doi: 10.1109/ACCESS.2021.3137318.
- [16] H. Kye, M. Kim, and M. Kwon, "Hierarchical detection of network anomalies : a self-supervised learning approach," *IEEE Signal Processing Letters*, vol. 29, pp. 1908–1912, 2022, doi: 10.1109/LSP.2022.3203296.
- [17] G. Pu, L. Wang, J. Shen, and F. Dong, "A hybrid unsupervised clustering-based anomaly detection method," *Tsinghua Science and Technology*, vol. 26, no. 2, pp. 146–153, Apr. 2021, doi: 10.26599/TST.2019.9010051.
- [18] G. Abdelmoumin, D. B. Rawat, and A. Rahman, "On the performance of machine learning models for anomaly-based intelligent intrusion detection systems for the internet of things," *IEEE Internet of Things Journal*, vol. 9, no. 6, pp. 4280–4290, Mar. 2022, doi: 10.1109/JIOT.2021.3103829.
- [19] W. Zhong, N. Yu, and C. Ai, "Applying big data based deep learning system to intrusion detection," *Big Data Mining and Analytics*, vol. 3, no. 3, pp. 181–195, Sep. 2020, doi: 10.26599/BDMA.2020.9020003.
- [20] S. Otoum, B. Kantarci, and H. T. Mouftah, "On the feasibility of deep learning in sensor network intrusion detection," *IEEE Networking Letters*, vol. 1, no. 2, pp. 68–71, Sep. 2019, doi: 10.1109/nlet.2019.2901792.
- [21] X. An, X. Zhou, X. Lü, F. Lin, and L. Yang, "sample selected extreme learning machine based intrusion detection in fog computing and MEC," *Wireless Communications and Mobile Computing*, vol. 2018, no. 1, Jan. 2018, doi: 10.1155/2018/7472095.
- [22] M. A. Khan, A. Rehman, K. M. Khan, M. A. Al Ghamdi, and S. H. Almotiri, "Enhance intrusion detection in computer networks based on deep extreme learning machine," *Computers, Materials & Continua*, vol. 66, no. 1, pp. 467–480, 2020, doi: 10.32604/cmc.2020.013121.
- [23] B. Liu, "RETRACTED ARTICLE: Hybrid extreme learning machine-based approach for IDS in smart Ad Hoc networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2023, no. 1, p. 84, Aug. 2023, doi: 10.1186/s13638-023-02297-6.
- [24] R. Raman, V. Sujatha, C. Bhupeshbhai Thacker, K. Bikram, M. B. Sahaai, and S. Murugan, "Intelligent parking management systems using iot and machine learning techniques for real-time space availability estimation," in *2023 International Conference on Sustainable Communication Networks and Application (ICSCNA)*, Nov. 2023, pp. 286–291, doi: 10.1109/ICSCNA58489.2023.10370636.




- [25] T. Meenakshi, R. Ramani, A. Karthikeyan, N. S. Vanitha, and S. Murugan, "Power quality monitoring of a photovoltaic system through IoT," in *2023 International Conference on Sustainable Communication Networks and Application (ICSCNA)*, Nov. 2023, pp. 413–418, doi: 10.1109/ICSCNA58489.2023.10370494.
- [26] C. S. Ranganathan, R. Raman, K. K. Sutaria, R. A Varma, and S. Murugan, "Network security in cyberspace using machine learning techniques," in *2023 7th International Conference on Electronics, Communication and Aerospace Technology (ICECA)*, Nov. 2023, pp. 1755–1759, doi: 10.1109/ICECA58529.2023.10394962.
- [27] R. Raman, M. Kaul, R. Meenakshi, S. Jayaprakash, D. Rukmani Devi, and S. Murugan, "IoT applications in sports and fitness: enhancing performance monitoring and training," in *2023 Second International Conference On Smart Technologies For Smart Nation (SmartTechCon)*, Aug. 2023, pp. 137–141, doi: 10.1109/SmartTechCon57526.2023.10391301.
- [28] M. R Sudha, G. B. H. Malini, R. Sankar, M. Mythily, P. S. Kumaresh, M.N. Varadarajan, and S. Sujatha, "Predictive modeling for healthcare worker well-being with cloud computing and machine learning for stress management," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 15, no. 1, 2025, doi: 10.11591/ijece.v15i1.pp1218-1228.
- [29] D. Javaheri, S. Gorgin, J.-A. Lee, and M. Masdari, "Fuzzy logic-based DDoS attacks and network traffic anomaly detection methods: Classification, overview, and future perspectives," *Information Sciences*, vol. 626, pp. 315–338, May 2023, doi: 10.1016/j.ins.2023.01.067.

BIOGRAPHIES OF AUTHORS






Palaniraj Rajidurai Parvathy    is a Project Manager at Mphasis Corporation in Chandler, Arizona, USA. He has 16+ years of IT experience in the BI & Analytics domain with a focus on data modeling, integration and visualization (Snowflake, Azure, AWS, GCP, azure data factory, data bricks, tableau, power BI, python, R, SAP BO, altreyx, xceptor (RPA)). Rewarded from customer for providing "Customer Value Addition" for performance tuning on schedule. He has been rewarded the "Star Performer" award of the quarter for a support project by hexaware leadership. Also, he received the "Stat Performer" award of the quarter for migration project from hexaware leadership. Moreover, rewarded "Most Valuable Player" support project from wipro-best buy account leadership. Furthermore, rewarded a "Feather in my cap" for outstanding contribution to the project business group hierarchy iteration. He was rewarded with a "Feather in my cap" award for his outstanding contribution to project business group hierarchy iteration 1. He can be contacted at email: palanirajrps@gmail.com.







Satheshkumar Sekar    with over 15 years of seasoned expertise in Information Technology, he brings a wealth of experience spanning Project and Portfolio Management, Technical Delivery, and Managed Services. My extensive background includes a strong focus on data and cloud projects, where he has excelled in system analysis, requirement gathering, design, development, testing, quality assurance, implementation, and support across banking, insurance, health care, and manufacturing domains. Notable skills include proficiency in Snowflake, azure data bricks, and Azure services, with a special emphasis on HVR Real-Time replication. He has successfully managed end-to-end Project Planning, Execution, and Management, aligning activities with core business objectives. My competencies extend to data analysis, governance, integration, quality, application tuning, and security. He has demonstrated mastery in developing custom Python utilities for seamless data migration and exhibit hands-on experience in Spark, Scala, Python, and UNIX Shell scripting. A standout achievement includes designing and building HVR ELT pipelines for various platforms, highlighting my expertise in data movement. Furthermore, my background encompasses reengineering legacy applications into microservices on the data bricks platform and executing successful Teradata to Snowflake migrations and Teradata to GCP Big Query. Well-versed in AzureDevOps and data bricks MLOps, He bring a comprehensive understanding of tools and technologies in IBM Mainframe, vision plus, and IDMS. He can be contacted at email: satheshkumar.sekar24@gmail.com.







Bharat Tidke    obtained his MTech and Ph.D. degree in Computer Engineering from Sardar Vallabhbhai National Institute of Technology, Surat, India. He is currently working with SIT Nagpur. He published many papers in reputed international journals and conferences His interests include soft computing, big data, machine learning and social network data analytics. He can be contacted at email: batidke@gmail.com.







Rudraraju Leela Jyothi     currently serve as an Assistant Professor in the Department of Computer Science and Engineering at Sagi Rama Krishnam Raju Engineering College (A), Bhimavaram, Andhra Pradesh, India. She has 8 Years of Teaching Experience. Coming to my areas of interests includes IoT, android development and web development. She can be contacted at email: rudraraju.leela92@gmail.com.







Venugopal Sujatha     received her Bachelor of Science in Mathematics from Madras University in 1994, M.C.A from Madras University. She completed Ph.D. degree from AMET University. At present; she is working as an Associate professor & HOD in S.A. Engineering College Chennai. The author is having more than 23 years of experience in teaching field. Her fields of research include wireless sensor networks, and machine learning. She has 10 papers in National/International conference and 11 Papers in International journals. She can be contacted at email: sujatha@saec.ac.in.



Madappa Shanmugathai     working as a Professor in the Department of English at Sri Sairam Engineering College, Chennai, Tamilnadu, India. She is received his Master's in English with M.Phil and Doctoral Degree having done research in the area of English for Specific Purposes (ESP) i. She is completing 28 years of Teaching for UG (Engineering) and PG (Business Studies) and in progress. She has a Heading the Department of English, Sri Sairam Engineering College. She is a Leadership in Mentor for Self Help Group-Women. She is a Coordinator in-fine arts and prevention of sexual harassment (POSH) at the institution level. Also, she is a TED organizer. She can be contacted at email: Shanmugathai.eng@sairam.edu.in.



Subbiah Murugan     is an Adjunct Professor, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai, TamilNadu, India. He published his research articles in many international and national conferences and journals. His research areas include network security and machine learning. He can be contacted at smuresjur@gmail.com.