International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8
DOI: https://doi.org/10.17762/ijritcc.v11i8.7926
***Article Received**: 30 April 2023 **Revised**: 30 June 2023 **Accepted**: 20 July 2023*

3-WAY Secured WSN with CSDSM-DNN based Intrusion Detection Model

K.Santhi[1], B.Sowmiya[2], R.Shalinirajan[3], V.Vijayashanthi[4] , V.Vasudhevan[5]
[1]Department (Computer Science and Engineering)
Panimalar Engineering College
Poonamalle,Chennai,Tamilnadu,India
santhipanimalar12@gmail.com
[2]Department (Computing Technologies)
SRM Institute of Science and Technologies
Tech park, SRMIST, Kattankulathur, Chennai.Tamilnadu,India
sowmiyab@srmist.edu.in
[3]Department (School of Computing)
Sathyabama Institute of science and Technology
Jeppiaar nagar,Rajiv Gandhi salai,Chennai,Tamilnadu,India
rshaliniphd@gmail.com
[4]Department (Artificial intelligence and Data Science)
Vel tech Multi Tech Dr.Rangarajan Dr Sakunthala Engineering College
Avadi, Tamilnadu, India
vijayashanthi.v@veltechmultitech.org
[5]Department (Electronics and Communication Enginnering)
Panimalar Engineering College
Poonamalle,Chennai,Tamilnadu, India
vasudhevan.vee@gmail.com

Abstract— In Wireless Sensor Networks (WSNs), intrusion aims indegrading or even eliminating the capacity of these networks for providing their functions. Thus, in recent years, several ideas are brought and employed. However, these techniques still did not fulfill their requirements in attaining better classification accuracy. This paper proposes a novel Cosine Similarity Distance integrated Sammon Mapping learning layer-Deep Neural Network (CSDSM-DNN)-centricIntrusion Detection Model (IDM) in WSNfor attaining better outcomes. Initially, the nodes are clustered; after that, utilizing Binomial Distribution based Dwarf Mongoose Optimization (BD-DMO), the cluster heads are selected. Then, theIdentity Matrix Function-Kalman Filter (IMF-KF) identified the optimal route. Subsequently, the data is transferred via the secured route. The transferred data is pre-processed and then, the important features are selected. Lastly, to classify whether the data is attacked or non-attacked, the selected features are given into the CSDSM-DNN. Therefore, with the prevailing approaches, the experiential outcomes are evaluated and analogized and it exhibits the proposed model's higher reliability and efficacy.

Keywords-Binomial Distribution based Dwarf Mongoose Optimization (BD-DMO) algorithm, Identity Matrix Function-Kalman Filter (IMF-KF), Cosine Similarity distance integratedSammon Mapping learning layer- Deep Neural Network (CSDSM-DNN), Wireless Sensor Networks(WSN), Intrusion Detection System(IDS).

I. INTRODUCTION

WSNs are at the heart of today's hugely distributed infrastructures like smart and cognitive environments, environmental monitoring networks, the Internet of Things, along with vehicular and mobile ad hoc networks [4]. WSN, which encloses hundreds to thousands of sensor nodes that are connected by wireless links, is a self-organized network [1]. Sensor nodes could sense, collect, and process surrounding temperature information [7]. Thus, in numerous fields, it is considered a propitious platform. Numerous researchers are concerned about the WSN's security with the smart sensor network devices' rapid development as well as broad application [20]. However, security in WSN is still challenging. Regardless of its ability to operate in an apocalyptic environment like floods, explosions, earthquakes, natural disasters, et cetera, WSN suffers as of several inherent vulnerabilities that create threats of severe attacks. These attacks might be network intrusion or device intrusion [18].

Therefore, intrusion detection is also a very effective security solution for WSNs. The aim of the Intrusion Detection System (IDS) is only to detect intrusions, thus they can detect attacks but cannot prevent them. In IDS, the attacks are

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8
DOI: https://doi.org/10.17762/ijritcc.v11i8.7926
***Article Received**: 30 April 2023 **Revised**: 30 June 2023 **Accepted**: 20 July 2023*

detected by the detection components and notified by raising an alarm or signal to the controller [3]. Intrusion detection techniques are classified into 3 categories. They are (1) Signature-based IDS, which stores the signature of known attack types and utilizes this signature base for finding similar attacks in the network traffic, (2) Anomaly-based IDS, which detects anomalies in system behavior by matching it with stored normal system behavior, and (3) Hybrid IDS, which employs both the approaches together [17]. Utilizing the signal processing approach, statistical approaches, Machine Learning (ML), as well as deep learning approaches, the evaluation of these intrusive attacks can be done [6].By utilizing the relevant features, the ML-based approach predicts the number of barriers accurately and fastens intrusion detection [15]. However, owing to minimum prediction accuracy, limited capability to predict new attacks, along with maximum false alarm rate, the prevailing IDS suffer [12].

1.1. Problem Definition

Numerous experiments have been done, which provided the solution for detecting the intrusion. However, enhancement is still required for those systems sowing to the problems given further, Security mechanisms utilized in wired and wireless networks are not that beneficial for WSNs since sensor nodes are resource constrained.

The network resources' usage pattern could be captured, but the prevailing techniques end up with a higher false positive rate. Therefore, a novel CSDSM-DNN-based IDM in WSN is proposed in this paper.

The balance of the paper is organized as: Section 2 presents prevailing IDS. Section 3 provides information on the proposed system in WSN. Section 4 illustrates the results and discussion. Finally, the paper is winded up in section 5.

II. LITERATURE SURVEY

Reference [10] propounded a WSN intelligent IDM. For classifying the attacks, the K-Nearest Neighbour algorithm (KNN) was wielded. The outcomes revealed that the presented framework had better effects along with practical application significance. However, the prediction stage might be slow with large data.

Reference [11] established an IDM for WSN grounded on the information gain ratio along with the Bagging approach. For selecting the sensor node's feature, the information gain ratio technique was employed. The outcomes displayed that the model had higher detection accuracy. But, it could be computationally expensive.

Reference [13] recommended lightweight Intelligent IDM for WSN. The classification accuracy could be significantly enhanced by the KNN approach. Superior outcomes were attained by the developed technique. Yet, the model required high memory to store all of the training data.

Reference [19] developed an Improved Convolutional Deep Belief Network-Based IDM (ICDBN-IDM). The entire network's energy consumption could be saved by redundancy detection. Outcomes exposed that the presented ICDBN-IDM had higher intrusion detection accuracy. But, higher space-time complexity was brought about by the model's deep convolutional computation.

Reference [8] established an IDS grounded on Deep Neural Network (DNN). For selecting the optimal features as of the dataset, a cross-correlation process was utilized. The outcomes proved that in contrast to the conventional approaches, the presented model performed well. However, the neural network was not suitable for the developed work owing to the small amount of data.

Reference [19] propounded a multi-correlation-centric IDM for long- and short-term memory WSNs. For extracting the intrusion detection data set's features, Bi-directional long- and short-term memory was wielded. The outcomes exhibited that the framework displayed superior classification performance. However, several issues were shown by the high-dimensional intrusion data produced in the present WSN environment.

Reference [2] revealed a multi-layer intrusion detection framework for WSN where a defense-in-depth security strategy was adopted for detecting intrusion. The results demonstrated that the developed multi-layer detection model gave a higher performance. But, it focused only on a few attacks.

Reference [14] introduced an enriched IDS. For selecting the features as of the dataset, the Grey Wolf Optimizer (GWO) algorithm was utilized. The outcomes exposed a higher detection rate of the developed system. However, the time of training the network was high.

Reference [5] demonstrated an Optimized Collaborative IDS (OCIDS) for WSNs. For optimizing the hierarchical IDS, it utilized an enhanced artificial bee colony optimization system. The outcomes displayed that the model was superior to the prevailing techniques. But, the energy consumption was too high.

Reference [16] recommended a Gaussian Process Regression (GPR) technique for the IDS. For data standardization, three GPR-centric ML models were developed. The outcomes exhibited that the k-barrier coverage probability was accurately predicted by the presented mechanism. But, it required learning a lot of historical data for training.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8
DOI: https://doi.org/10.17762/ijritcc.v11i8.7926
***Article Received**: 30 April 2023 **Revised**: 30 June 2023 **Accepted**: 20 July 2023*

III. PROPOSED INTRUSION DETECTION MODEL

To detect intrusion, this paper proposes a novel CSDSM-DNN. Initially, the high probability of the route is created; after that, the data is transferred. Lastly, to detect intrusion, the transferred data is classified. Figure 1 depicts the block diagram for the proposed system,

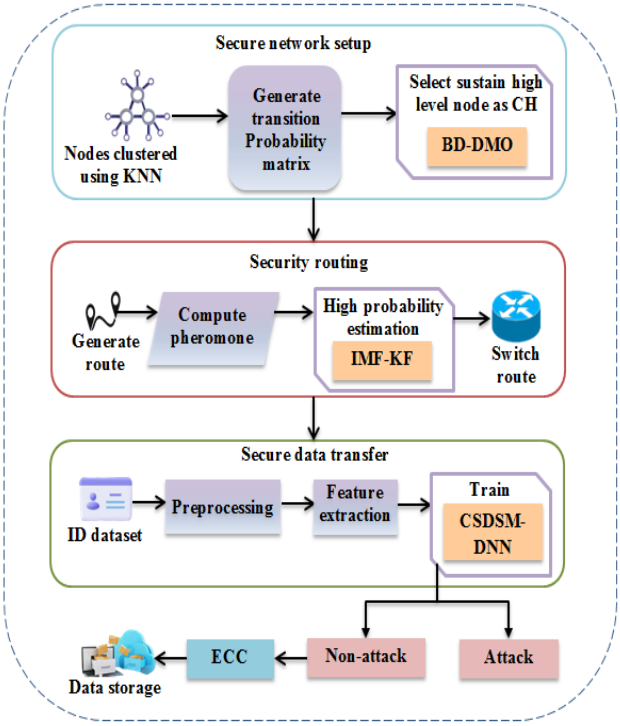


Figure 1: Block diagram of the proposed methodology

3.1. Secure Network Setup

With the step of network setup, the proposed model is explicated. It comprises three steps. After initializing nodes randomly in the WSN environment, all these steps are executed. The complexity of problems could be reduced by a proper node deployment and it is initialized as,

$$\Im_n = \Im_1, \Im_2, \Im_3, \ldots . \Im_N \quad where, i = 1,2,3, \ldots . N \tag{1}$$

Here, the number of initialized sensor nodes is signified as $\Im_n$. The steps are,

3.1.1. Node Clustering

Here, utilizing the KNN algorithm, the initialized nodes are clustered. KNN is a supervised learning classifier that utilizes proximity to make predictions about the grouping of individual nodes. The clustered node is represented as C_m.

3.1.2. Generate transition probability matrix

Here, for computing the transition probability matrix C_{trans}, each clustered node's density $\gamma \in C_m$ and energy $T \in C_m$ are taken as the input. The matrix is expressed as,

$$C_{trans} = \gamma . T \tag{2}$$

3.1.3. Secure Cluster head selection

The nodes that have maximum probability are selected from the transition matrix C_{trans} to have a high level of energy since the energy loses in the current node. Thus, before the current node is attacked by the node outrage attack, the alternate cluster head is selected with high energy utilizing the BD-DMO algorithm. The system is made more secure from node attacks by the alternate selection. The DMO, which is inspired by animal behavior, is a swarm intelligence-based technique. It is utilized to find solutions for optimum global issues. In DMO, the parameter Ψ is distributed randomly. Thus, the updating criteria resulting in parameter estimation issues in the exploitation phase are modified to follow a binomial distribution that has the advantage of binomial numbers for making a quick estimation.

Population initialization

BD-DMO begins with the initialization of the population of mongoose (here, the maximum probability nodes are considered as the populations) and it is expressed as,

$$c_i = l + r * (u - l) \tag{3}$$

Here, $c_i \in C_{trans}$ and r signify i^{th} mongoose and random number, correspondingly, the search space's lower and upper bounds are indicated as l and u.

Alpha Group: Grounded on classification accuracy, the fitness of every single solution f_i is computed after initialization. Regarding this evaluation, the female alpha α was selected as,

$$\alpha = \frac{f_i}{\sum_{i=1}^{m} f_i} \tag{4}$$

α is associated with the number of babysitters B of the dominant female d. Usually, the babysitters are inferior group members that stay with the youngsters; also, for enabling the alpha female (mother) for conducting the rest of the squad on

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8
DOI: https://doi.org/10.17762/ijritcc.v11i8.7926
***Article Received**: 30 April 2023 **Revised**: 30 June 2023 **Accepted**: 20 July 2023*

daily hunting expeditions, they are cycled o a routine basis. Then, the solution is updated c_{i+1} as,

$$c_{i+1} = c_i + \Psi * d \tag{5}$$

$$\Psi = \binom{\xi}{\lambda} s^{\xi} r^{\lambda-\xi} \tag{6}$$

Here, Ψ epitomizes the output of vocalization utilizing the binomial distribution, λ signifies the number of vocals at a time ξ , s and r denote the success and failure of the vocal.

The sleeping mound s_i is computed for every repetition, which is denoted as,

$$s_i = \frac{f_{i+1} - f_i}{\max\{|f_{i+1}, f_i|\}} \tag{7}$$

The average of s_i is derived as,

$$\Omega^{s_i} = \frac{\sum_{i=1}^{M} s_i}{M} \tag{8}$$

When the next food supplier resting mound is considered, the algorithm advances to the scouting stage after the babysitting exchange criterion is fulfilled.

Scouting stage: Here, they will find a good sleeping mound if they forage quite far and it is expressed as,

$$c_{i+1} = \begin{cases} c_i - \Delta * \Psi * r\left[c_i - \vec{v}\right], & if\ \Omega_{i+1}^{s_i} > \Omega_i^{s_i} \\ c_i + \Delta * \Psi * r\left[c_i - \vec{v}\right], & otherwise \end{cases} \tag{9}$$

Wherein, $\vec{v}$ and Δ signify the movement vector and parameter for the movement ofa mongoose. And, both are computed as,

$$\Delta = \left(1 - \frac{I}{I_{\max}}\right)^{\left(2*\frac{I}{I_{\max}}\right)} \tag{10}$$

$$\vec{v} = \sum_{i=1}^{M} \frac{c_i * s_i}{c_i} \tag{11}$$

Here, I and $I_{\max}$ signify iteration and maximum iteration, correspondingly. Like the way of updating position for hunting, the cluster heads h_k are selected, which is expressed as,

$$h_k = \{h_1, h_2, h_3, \ldots\ldots h_K\} \tag{12}$$

3.2. Secure Routing

To deliver the data from one place to another, the secured routes are determined grounded on the obtained clustered head. The routing phase comprised four steps. They are explained further,

3.2.1. Generate Route

Here, the routes are generated utilizing clustered nodes for transferring data. It has a preferred contributing route, and this is used to forward the traffic even if there isn't a contributing route matching the data's destination. The routes $\Re_n$ are generated as,

$$\Re_N = \{\Re_1, \Re_2, \Re_3, \ldots\ldots \Re_N\} \tag{13}$$

3.2.2. Compute Pheromone

From the generated multiple routes, the best route is selected by the following steps,

Compute delta pheromone value Δp for all routes,

$$\Delta p = \frac{1}{\max(h_k) - \frac{\sum_{i=1}^{N} \Re_n}{n}} \tag{14}$$

Evaluate pheromone value p ,

$$p = \begin{cases} \varsigma_{\min} & if\ \varsigma < \varsigma_{\min} \\ \varsigma_{\max} & if\ \varsigma < \varsigma_{\max} \\ (1-\eta)p(t-1) + \sum_{k=1}^{K} p \end{cases} \tag{15}$$

Where, $\varsigma_{\min}$ and $\varsigma_{\max}$ epitomize minimum and maximum pheromone values, η symbolizes the density of node, t indicates time. From this pheromone value, the highest values are chosen as the optimal route for the data transaction.

3.2.3. High probability estimation

Here, optimal routes are selected to estimate high probability utilizing the IMF-KF in which energy, distance, and trusted values of the particular node are considered for secured routing. For estimating states grounded on the linear dynamical systems in the state space format, Kalman Filter (KF) is wielded. However, there is a biasing issue when there are unknown statistics in the estimation without considering its error variance; thus, it is modified to follow Identity Matrix Function (IMF).

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8
DOI: https://doi.org/10.17762/ijritcc.v11i8.7926
***Article Received**: 30 April 2023 **Revised**: 30 June 2023 **Accepted**: 20 July 2023*

The KF model assumes the true identity matrix $\aleph$ according to,

$$\aleph = \begin{bmatrix} -p_1^{\max} & -p_2^{\max} & \cdots & -p_{N-1}^{\max} & -p_N^{\max} \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{bmatrix} \quad (16)$$

Grounded on this modified matrix, the prior and posterior estimation vector is computed to get the linear combination betwixt the routes. The results are then given as a secure route from which the upcoming transmission will be switched.

3.3. Secure Data Transfer

The data is transferred through the routes following the secure routing. The transferred data D is taken as input to detect whether the data is attacked or non-attacked utilizing ML.

3.3.1. Pre-processing

Here, pre-processing is performed for extracting accurate and consistent information by reducing the redundant data, while the missing data is replaced with some substitute value. The pre-processed data is signified as D_φ .

3.3.2. Feature extraction

Subsequent to pre-processing, the features are extracted to make the classification very fast. Hence, the key features, namely Packet Protocol features, Login features, and Attack features are extracted, and it is expressed as,

$$F_\varphi = \{F_1, F_2, F_3, \ldots..F_J\} \quad where, j = 1,2,3,\ldots..J \quad (17)$$

Here, $F_\varphi \in D_\varphi$ refers to extracted features.

3.3.3. Classification

Here, the extracted features are inputted into the CSDSM-DNN classifier. A DNN has an output layer, an input layer, and at least one hidden layer in between. However, the learning time of the attack feature is relatively high in the conventional DNN. Thus, a modification has been made by adding a layer as learning layer for enhancing the learning time. However, in the prevailing learning layer, Sammon mapping has the limitation of not being easy to map hitherto unseen points since it assumes the metric to be in the Euclidean distance; thus, it is modified to follow cosine similarity distance for making it effective. Figure 3 depicts the structure of CSDSM-DNN,

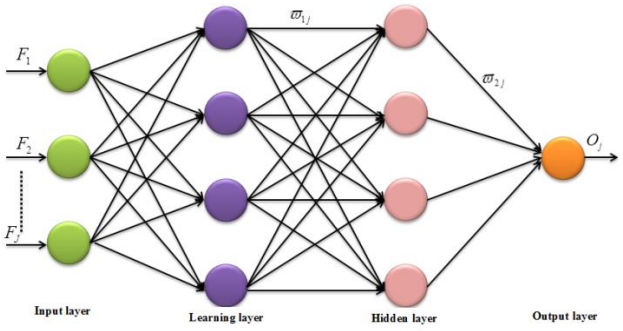


Figure 2: Structure of CSDSM-DNN

Step 1: Input the transferring data's extracted features.

Step 2: Compute the output of the learning layer F_j^{learn}, which learns the data as of the input layer and gives it to the hidden layer. It is computed as,

$$F_j^{learn} = \frac{l_j \bullet F_j}{\|l_j\| \|F_j\|} \quad (18)$$

Here, l_j signifies the j^{th} learning layer.

Step 3: Compute the output of the hidden layer utilizing equation (19),

$$h_{1i} = b_{1i} + \sum_{j=1}^{J} F_j^{learn} \varpi_{1i} \quad (19)$$

Step 4: Find the final output, the final hidden layer is multiplied by the weight of the same hidden layer's output, which is expressed as,

$$O_j = b_{2j} + \sum_{j=1}^{J} h_j \varpi_{2j} \quad (20)$$

Where, ϖ_{1i} and ϖ_{2j} represents the optimized weight, b_{2j} symbolizes the bias value of the final hidden layer's output, and O_j indicates the output unit that denotes whether the data has an attack or not. If the data is non-attacked, then it is securely stored in the cloud utilizing the Elliptical Curve Cryptography (ECC) algorithm. The pseudo-code of the proposed CSDSM-DNN is,

Input: Extracted features F_φ

Output: Classified Data O_j

Begin

Initialize $F_j^{learn}, b_{1i}, \varpi_{1i}$

For j^{th} neuron

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8
DOI: https://doi.org/10.17762/ijritcc.v11i8.7926
***Article Received**: 30 April 2023 **Revised**: 30 June 2023 **Accepted**: 20 July 2023*

Learn input features

$$F_j^{learn} = \frac{I_j \bullet F_j}{\|I_j\| \|F_j\|}$$

Update weight and bias for hidden layer

Compute hidden layer

$$h_{1i} = b_{1i} + \sum_{j=1}^{J} F_j^{learn} \varpi_{1i}$$

Update weight to output layer

Detect output

If non attacked data {

Store in the cloud

}else{

Process declined

}

End if

Return Classified Data

End

IV. RESULT AND DISCUSSION

Here, for assessing the proposed model's performance, numerous experiments are conducted. In the working platform of PYTHON, it is employed.

4.1 Dataset Description

A network intrusion detection dataset, which had been collected from publically available resources, is utilized by the proposed system. It comprises a broad variety of intrusions simulated in a military network environment. From this, 80% was utilized for training, and 20% was utilized for testing.

4.2. Performance analysis of cluster head selection

Here, with conventional techniques like the Whale Optimization Algorithm (WOA), Fish Swarm Optimization (FSO) Algorithm, Dwarf Mongoose Optimization (DMO), along with Crow Search Algorithm (CSA), the outcomes of the proposed BD-DMO are assessed and analogized.

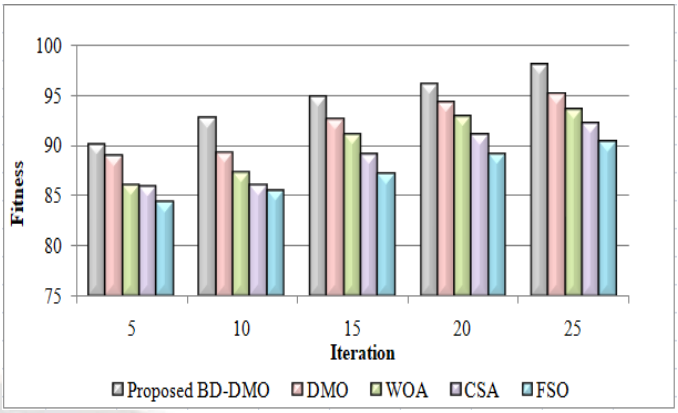


Figure 3: Performance analysis of proposed BD-DMO

Discussion: Figure 3 demonstrates that the proposed model's fitness value mounts when the number of iterations increases. For the proposed work, when the number of iterations is 5, the fitness value is 90.01%; for 10, it is 92.65%; lastly, for 25, it is 98%. However, for the prevailing DMO, fitness values are reduced to the order of 5 (88.9%), 10 (89.12%), and so on. This exposes that the proposed model outperforms other conventional techniques.

4.3. performance analysis of high probability estimation

Here, with the conventionalKFE, Maximum Likelihood Estimation (MLE), and Bayesian Recursive Estimation (BRE), the proposed system's performance is evaluated and analogizedgrounded on Mean Square Error (MSE) value.

Table: 1 Comparative analysis of proposed IMF-KF

Techniques	MSE
Proposed IMF-KF	0.01253
KFE	0.14872
MLE	0.08745
BRE	0.23756

Discussion: The proposed mechanism's efficacy is exhibited by the MSE value intable 1. The proposed model's better performance is attained by the lower value of the proposed model. Regarding MSE, the proposed technique achieves 0.0123, which is 0.13619 higher than existing KFEand 0.07492 higher than MLE. Thus, it proved that the proposed model displays higher efficiency.

4.4. Performance analysis for classification

Regarding True Negative (TN), True Positive (TP) accuracy, and F-Measure, the proposed model is evaluated and analogized with the prevailing frameworks like DNN, Recurrent Neural Networks (RNN), Convolutional Neural Networks (CNN), along with Support Vector Machine (SVM) for estimating the proposed model's superiority.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8
DOI: https://doi.org/10.17762/ijritcc.v11i8.7926
***Article Received**: 30 April 2023 **Revised**: 30 June 2023 **Accepted**: 20 July 2023*

Table 2: Performance of the CSDSM-DNN with the existing methods in terms of (a) TP (b) TN

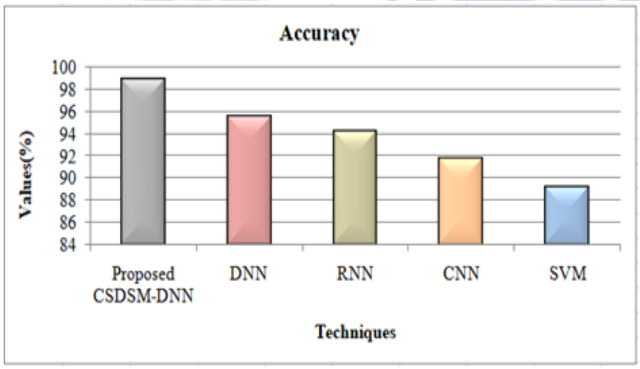
(a)

Techniques	TP
Proposed CSDSM-DNN	95.0
DNN	93.09
RNN	91.76
CNN	89.50
SVM	87.14

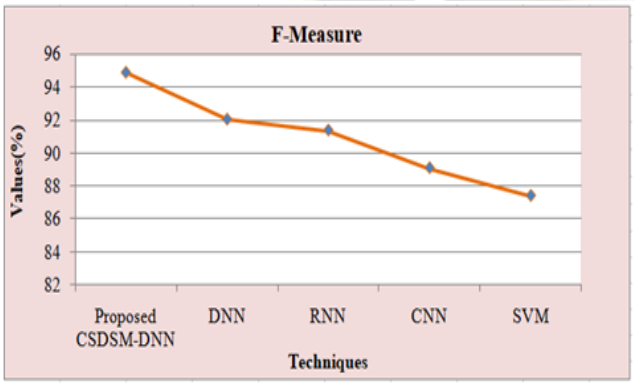
(b)

Techniques	TN
Proposed CSDSM-DNN	94.8
DNN	92.99
RNN	90.27
CNN	88.78
SVM	86.19

Discussion: The performance comparison of the proposed along with prevailing techniques is exhibited in table 2. The TN attained by the proposed technique is 95%, which is 1.91% more highly enhanced than the prevailing DNN. Similarly, the TN of the proposed technique is 94.8%, which is 1.81% higher than DNN and 4.53% higher than RNN. Thus, the proposed model outperforms.



(a)



(b)

Figure 4: Demonstrate the performance of the CSDSM-DNN with the existing methods in terms of (a) Accuracy, (b) F-Measure

Discussion: Better outcomes of the proposed CSDSM - DNN are displayed in figure 4. The prevailing techniques attain an accuracy of 95.49% for DNN, 94.25% for RNN, 91.68% for CNN, and 89.17% for SVM, whereas the proposed CSDSM - DNN attains 98.92% (accuracy). Likewise, the CSDSM –DNN attains the highest f-measure of 94.87%. Hence, the outcome displays a higher efficacy of the proposed method.

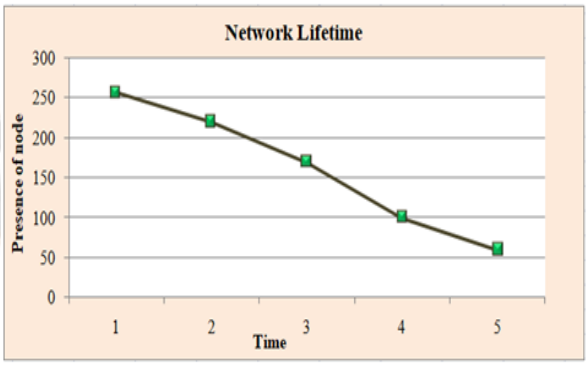


Figure 5: Network lifetime

Discussion: Figure 5 exhibits that within the minimum period of time; the network should be formed with the maximum number of nodes. Therefore, the proposed network kept 256 nodes while sending the data at 1sec, 219 nodes at 2sec, and 169 sec at 3sec. This analysis shows the higher life time of the proposed framework.

4.5. Performance analysis using the NSL-KDD dataset

Here, with DNN [8], SVM [14], and Weighted SVM (WSVM) [5], the detection rate of the proposed model is assessed and compared.

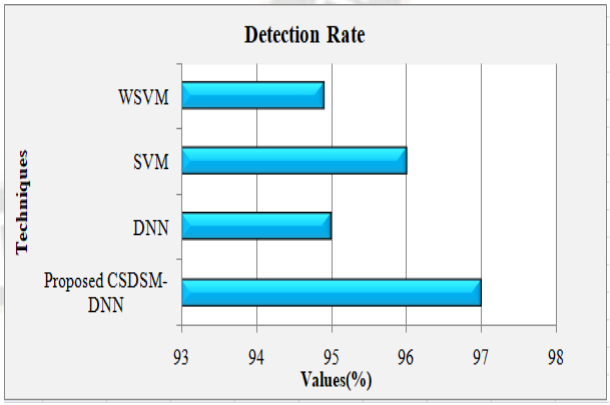


Figure 6: Performance analysis of proposed and conventional methods

Discussion: Grounded on the detection rate, the performance analysis is depicted in figure 6.When contrasted with the prevailing systems, the proposed technique attains a better detection rate (97%). However, the prevailing approaches like DNN and SVM attained 95% and 96%, correspondingly. Thus, the overall discussion demonstrates the proposed system's superior performance.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8
DOI: https://doi.org/10.17762/ijritcc.v11i8.7926
***Article Received**: 30 April 2023 **Revised**: 30 June 2023 **Accepted**: 20 July 2023*

V. CONCLUSION

To detect intrusion in WSN, this paper proposed a novel CSDSM-DNN approach. The model undergoes several operations like node clustering, cluster head selection, route generation, compute pheromone, high probability estimation, data pre-processing, feature extraction, and classification. The performance assessment takes place after executing all these steps. Here, regarding various metrics, the readings are noted and analogized with the prevailing systems. The proposed model could detect various uncertainties and recognizes the intrusion very correctly with an accuracy of 98.92%. Likewise, for several quality metrics like F-Measure, TN, TP, MSE, network lifetime, and detection rate, the proposed model achieves the best result. Thus, the outcomes revealed that when analogized with the prevailing techniques, the proposed system is highly efficient. For attacks mainly in the physical and network layer, this work provides three-level security. It can be developed in the future for preventing attacks from other layers also.

REFERENCES

[1] Almomani, I., & Alromi, A. (2020). Integrating software engineering processes in the development of efficient intrusion detection systems in wireless sensor networks. Sensors (Switzerland), 20(5), 1-28. https://doi.org/10.3390/s20051375

[2] Alruhaily, N., Alruhaily, N. M., & Ibrahim, D. M. (2021). A Multi-layer Machine Learning-based Intrusion Detection System for Wireless Sensor Networks.International Journal of Advanced Computer Science and Applications, 12(4), 281-287.

[3] Ashwini, B. A., & Manivannan, S. S. (2020). Supervised Machine Learning Classification Algorithmic Approach for Finding Anomaly Type of Intrusion Detection in Wireless Sensor Network. Optical Memory and Neural Networks (Information Optics), 29(3), 244–256. https://doi.org/10.3103/S1060992X20030029

[4] Batiha, T., & Krömer, P. (2021). Design and analysis of efficient neural intrusion detection for wireless sensor networks. Concurrency and Computation: Practice and Experience, 33(23), 1–12. https://doi.org/10.1002/cpe.6152

[5] Elsaid, S. A., & Albatati, N. S. (2020). An optimized collaborative intrusion detection system for wireless sensor networks. Soft Computing, 24(16), 12553–12567. https://doi.org/10.1007/s00500-020-04695-0

[6] Gavel, S., Raghuvanshi, A. S., & Tiwari, S. (2021). A novel density estimation based intrusion detection technique with Pearson's divergence for Wireless Sensor Networks. ISA Transactions, 111, 180–191. https://doi.org/10.1016/j.isatra.2020.11.016

[7] Gite, P., Chouhan, K., Murali Krishna, K., Kumar Nayak, C., Soni, M., & Shrivastava, A. (2021). ML Based Intrusion Detection Scheme for various types of attacks in a WSN using C4.5 and CART classifiers. Materials Today: Proceedings,1-9. https://doi.org/10.1016/j.matpr.2021.07.378

[8] Gowdhaman, V., & Dhanapal, R. (2021). An intrusion detection system for wireless sensor networks using deep neural network. Soft Computing,1-10. https://doi.org/10.1007/s00500-021-06473-y

[9] Sunanda, P. ., Janardhanan, K. A. ., Gupta, R. ., Tannady, H. ., Shrivastava, N. K. ., & Sharma, T. K. . (2023). Distributed Hashing Based Group Management Scheme for the Peer-to-Peer Trust Model. International Journal of Intelligent Systems and Applications in Engineering, 11(3s), 08–13. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/2525

[10] Jin, J. (2021). Intrusion Detection Algorithm and Simulation of Wireless Sensor Network under Internet Environment. Journal of Sensors,1-10. https://doi.org/10.1155/2021/9089370

[11] Liu, G., Zhao, H., Fan, F., Liu, G., Xu, Q., & Nazir, S. (2022). An Enhanced Intrusion Detection Model Based on Improved kNN in WSNs. Sensors, 22(4), 1–18. https://doi.org/10.3390/s22041407

[12] Liu, S., Wang, L., Qin, J., Guo, Y., & Zuo, H. (2018). An intrusion detection model based on IPSO-SVM algorithm in wireless sensor network. Journal of Internet Technology, 19(7), 2125–2134. https://doi.org/10.3966/160792642018121907015

[13] Maheswari, M., & Karthika, R. A. (2021). A Novel QoS Based Secure Unequal Clustering Protocol with Intrusion Detection System in Wireless Sensor Networks. Wireless Personal Communications, 118(2), 1535–1557. https://doi.org/10.1007/s11277-021-08101-2

[14] Dr. Avinash Pawar. (2020). Development and Verification of Material Plasma Exposure Concepts. International Journal of New Practices in Management and Engineering, 9(03), 11 - 14. https://doi.org/10.17762/ijnpme.v9i03.90

[15] Pan, J. S., Fan, F., Chu, S. C., Zhao, H. Q., & Liu, G. Y. (2021). A Lightweight Intelligent Intrusion Detection Model for Wireless Sensor Networks. Security and Communication Networks,1-15. https://doi.org/10.1155/2021/5540895

[16] Safaldin, M., Otair, M., & Abualigah, L. (2021). Improved binary gray wolf optimizer and SVM for intrusion detection system in wireless sensor networks. Journal of Ambient Intelligence and Humanized Computing, 12(2), 1559–1576. https://doi.org/10.1007/s12652-020-02228-z

[17] Singh, A., Amutha, J., Nagar, J., Sharma, S., & Lee, C. C. (2022). LT-FS-ID: Log-Transformed Feature Learning and Feature-Scaling-Based Machine Learning Algorithms to Predict the k-Barriers for Intrusion Detection Using Wireless Sensor Network. Sensors, 22(3).1-15. https://doi.org/10.3390/s22031070

[18] Singh, A., Nagar, J., Sharma, S., & Kotiyal, V. (2021). A Gaussian process regression approach to predict the k-barrier coverage probability for intrusion detection in wireless sensor networks. Expert Systems with Applications, 172, 1-11. https://doi.org/10.1016/j.eswa.2021.114603

[19] Christopher Davies, Matthew Martinez, Catalina Fernández, Ana Flores, Anders Pedersen. Using Machine Learning for Early Detection of Learning Disabilities. Kuwait Journal of Machine Learning, 2(1). Retrieved from http://kuwaitjournals.com/index.php/kjml/article/view/172

[20] Singh, G., & Khare, N. (2022). A survey of intrusion detection from the perspective of intrusion datasets and machine learning

techniques. International Journal of Computers and Applications, 44(7), 659–669. https://doi.org/10.1080/1206212X.2021.1885150

[21] Sinha, S., & Paul, A. (2020). Neuro-Fuzzy Based Intrusion Detection System for Wireless Sensor Network. Wireless Personal Communications, 114(1), 835–851. https://doi.org/10.1007/s11277-020-07395-y

[22] Ahmed Abdelaziz, Machine Learning Approaches for Predicting Stock Market Volatility , Machine Learning Applications Conference Proceedings, Vol 3 2023.

[23] Wen, W., Shang, C., Dong, Z., Keh, H. C., & Roy, D. S. (2021). An intrusion detection model using improved convolutional deep belief networks for wireless sensor networks. International Journal of Ad Hoc and Ubiquitous Computing, 36(1), 20–31. https://doi.org/10.1504/IJAHUC.2021.112980

[24] Zhao, R., Yin, J., Xue, Z., Gui, G., Adebisi, B., Ohtsuki, T., Gacanin, H., & Sari, H. (2021). An Efficient Intrusion Detection Method Based on Dynamic Autoencoder. IEEE Wireless Communications Letters, 10(8), 1707–1711. https://doi.org/10.1109/LWC.2021.3077946.