ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

MALICIOUS NODE FEATURE SELECTION USING SWARM INTELLIGENCE CLASSIFIER IN WIRELESS SENSOR NETWORK

*1VEMULA KESAVA KUMAR, 2P. SURESH VARMA

1, 2 Department of Computer Science and Engineering, Adikavi Nannaya University, Rajamahendravaram, India

Email: vemulakesav74@gmail.com

ABSTRACT

Rapid development and growth of technology Various real-time applications are used in wireless environments. Internet-enabled services are the most important in the world for the delivery of efficient services. There are a variety of quality factor issues and security attacks in wireless sensor network environments. Network efficiency is measured to find the attacks and malicious node functions. In this white paper, we propose efficient detection of malicious nodes and their function using deep learning. A novel swarm intelligence method is used to measure the features and apply a classification technique to measure the gain. In this document we used the dataset Knowledge Discovery Dataset UCI Repository to calculate the performance. The identifier is calculated using Tensorflow. The various functions evaluate the performance of accuracy, detection time, turnaround time, energy consumption and packet delivery ratio. The system accuracy proposed by us is to be calculated and the characteristics compared with existing methods.

Keywords: *Energy Efficiency, Malicious Attack, Swarm Intelligence, Tensorflow, Wireless Sensor Network.*

1. INTRODUCTION

Highly distributed wireless sensor network is formed based on sensor nodes, light weight process, and data optimization. In wireless sensor networks, there are several characteristics that can be measured using sink, sensor node values, base station factors, and Internet of Things (IoT) enabled services such as heat, water level, pressure, and other factors. Each sensory information is recorded in the base station and controls the network in each hop-by-hop [1]. Aggregation is another factor to find network lifetime and traffic characteristics. Many schemes have been proposed to mitigate these problems, but only a few can effectively and correctly detect the severity of the network. Many researchers analyzed various literatures in terms of network topology, attack capabilities, critical capabilities, limitations, endurance, and robustness levels. Efficiency is another factor in the WSN environment and provides a better way to detect attacks [2].

Various existing methods are available for measuring the WSN accuracy factor. Various network algorithms are also available to detect the attacks and malicious nodes. The accuracy and fast detection are the two main scenarios of the current IT and ITeS [3]. We need an efficient approach to measure attacks like sinkhole, snooping, phishing, etc. Therefore, we need to optimize the WSN environment using deep learning. Based on various characteristics, there is no strong detection algorithm to measure malicious node characteristics [4][5].

The Figure. 1 shows that various cluster of multiple nodes and access the service from base station. In each cluster we have a cluster head and a list of certificate authorities with access rights. Malicious node can be marked as malicious based on hop-by-hop transactions. Our goal is to measure the malicious node features by using swarm intelligence with deep learning features. In this method we aggregate the data from multiple features, base station-to-node routing, and topological structures. The estimate is measured by network lifetime [6] and triggers the malicious node [7]. The global decision can be obtained from attacking features.

The rest of this paper is organized as follows: In section 2, the literature review on different attacks and their detection algorithms. The proposed work is given in Section 3. The results are compared to

Journal of Theoretical and Applied Information Technology

31st October 2023. Vol.101. No 20

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

existing techniques and are provided in Section 4. The work concludes in Section 5 with conclusions and future research directions.

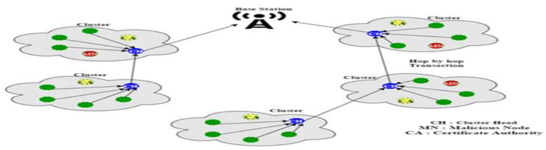


Figure1.Wireless Sensor Environment With Cluster And Malicious Node

2.RELATED WORKS

Routing is the major criteria while selecting nodes and making the transaction from one to another. In this case, various sensor node limitations are considered to allow us to justify the attack based on types and characteristics. Manikandan et al, Sinkhole is the attack and ability to calculate network lifetime efficiency [8]. Attacks can be launched anywhere based on vulnerable environment, access policies, packet transmission and characteristics of neighboring nodes. The attackers can attack the node at any cost, and multiple outcomes change the entire network environment. Wong et al. provide a compromised routing method that can be implemented in transit or at vulnerable stages [9][10].

Deep learning capabilities are currently available to measure network accuracy, score function, and robustness [11] of the network. Ghao Jio and Rugnga et al, captured packets are monitored and recorded in a centralized store-forward database and select the destination or hop node to send or receive packets based on availability [12]. Accounting [13] and auditing [14] are the two-factor guidelines in determining network attack loops and choosing network topologies. In each phase these characteristics are recorded to find the highly available critical characteristics [15]. Sinkhole attacks resulted and affected entire networks.

Limitations of existing methods are novelty, effective solution for measuring accuracy, quick detection of malicious attacks, and node index detection. The above property information is considered for selecting nodes and effective transmissions [16]. The effective algorithm is needed to select the features and find malicious nodes. Artificial intelligence is the technology to make effective decisions [17]. Chiago et al., The method of artificial bee colony is proposed for selecting bee groups, cluster groups and recommending attacks [18][19]. Table 1 below shows that various related investigations into attacks and optimization results have been performed.

Table 1 shows that different attacks and yearly comparison of detection algorithms were performed. Above all, the attacks are recognized based on specific data sets and optimized results [20]. From the results, we need an effective automated intelligent approach to detect the attack and record the malicious characteristics.

Table 1 Various Attacks And Detection Algorithms - Review

Year	Attack	Detection Algorithm	Simulators	Result
2017	Phishing Attack	Support Vector Machine	MATLAB	75-78%
2018	Sinkhole Attack	Decision Tree	MATLAB	78-81%
2019	Delay Systems	System Report	JS Script	81-83%
2020	Topo Stick	TopoGraph	NS3	78-80%
2021	Snooping	CNN Classifier	MATLAB	82-84%

3. WIRELESS SENSOR NETWORK COMMUNICATION AND METHODOLOGY

In this document, our proposed system consists of three phases such as Environment, Communication and Access Permissions. We chose a WSN-based cluster group, energy resources, less transmission delay, and increased energy efficiency. We designed a network with adaptive low-energy clustering and malicious node detection as shown in Figure. 2.

Journal of Theoretical and Applied Information Technology
31st October 2023. Vol.101. No 20

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

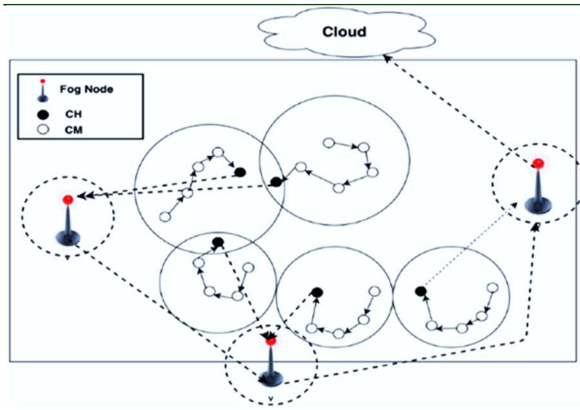


Figure2. Cluster Node Selection And Cluster Management Recording.

The multiphase consists of cluster head, communication session, node optimization and corresponding network functions. Each network capability is measured based on aggregate values, weight function, robust network characteristics and transmission. The thresholds are recorded based on results from communication media and malicious forgery of nodes.

The weight function can be measured using CH nodes and sinkhole attack characteristics. In this case the energy consumption, shortest routing, base station recommendations and packet dropping feature. We have selected all data and control packets from the base station and apply sinkhole functions to find malicious nodes. The following feature selection process is followed to monitor the attack and runs the features for multiple environments

Data Forwarding Process - In this case, we need to choose the base station, number packets can be sent and received, forward packets to the next hop or neighbour host, and find the network topology.

Acknowledgment selection - Each transmission acknowledgment of cluster head values, ACK messages, time factor is recorded. So, we can find the total network lifetime.

Packet delivery - The delivery factor is a measure of each packet transmission, waiting time, and the turnaround time of each packet. The time-to-live value is recorded to find the packet delivery and exceed the network index. Also, the CPU time can be tested at each stage and the malicious node can be found.

High energy threshold value - In each node, the energy consumption and the transmission factor are recorded for the selection of the cluster head. In this phase, each node transmission index is set for

malicious node selection and The variable value in symbol may be a very complex to solve.

The number of paths is unbounded and deciding whether a path is feasible or not an un-decidable problem in general case.

The number of execution may be more and it may fail test case even if one exit finally in case of infeasible path it will not terminate.

The problem of infeasible path can be eliminated only by considering an architecture which has no path selector phase.

The run time depends on characteristics of the problem instance in particular the problem

logging of CH node values. The threshold values are calculated as

$$Throshold_{(TE)} = (Energy \times Node_i) + Energy\_Index \tag{1}$$

Where

Energy is calculated as the energy consumption of each cluster head and

Node is the number of the node or packet transmitted over each cluster routing and

Energy_Index is the recorded value of the node-optimized result.

False route selection to detect malicious node characteristics in this case, each energy consumed results are recorded and apply shortest path from base station to cluster. Whereas cluster node distance measured as {X_i, Y_i, Distance_Index} and location can be stored for each base station index. Distance matrix is calculated and set each node malicious index. The values of each candidate malicious node are calculated as shown in Figure. 3 Flowchart

4.Swarm intelligence – Deep learning feature selection

Swarm intelligence is an optimization algorithm which is applied to measure the malicious node based on the waiting time for the resource and other computed features. It is a triggered approach used to monitor subsequent characteristics of each cluster head and apply global decision feature to select the attack simulations. The new node is selected using the fitness function and is chosen based on the current active node features. The probability value is re-coded and iterated based on the actual index. It is obtained based on attacker simulations

Journal of Theoretical and Applied Information Technology
31st October 2023. Vol.101. No 20

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

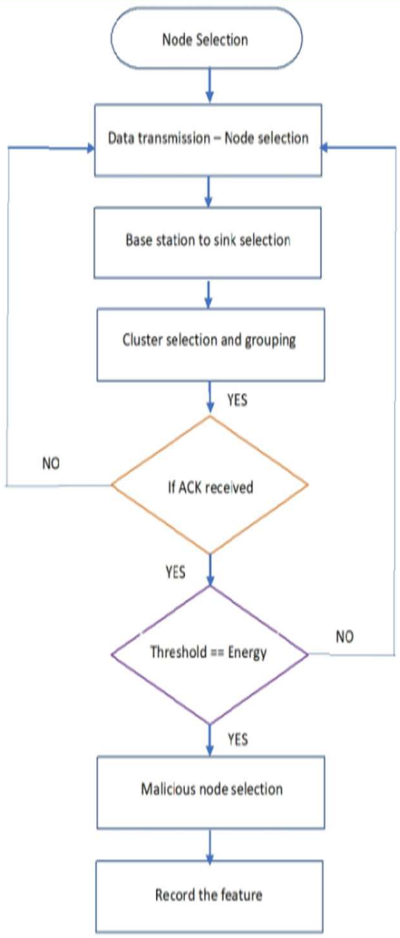


Figure3. Flow Chart For Selecting Malicious Feature And Methods

Pre-processing Phase – In this phase the selected dataset for evaluation and apply various classification techniques to filter the dataset. In this case Swarm Chi-square test is applied for removing redundant and irrelevant features using Eq (2). The selected features are recorded for evaluation.

$$Chi\_X^2 = \sum \frac{(A_{(ij)} - Energy_{(ij)})^2}{Index_{(ij)}} \quad (2)$$

Classification Phase - After phase I selected features are applied for behavioral analysis by using ANN Classifier. This stage each node values are tested for measuring accuracy index as shown in Eq (3). This is machine learning feature selection for node optimization.

$$Gain(I) = \sum x \in y, F_{(ij)} \log_2(energy_{(ij)})$$
(3)

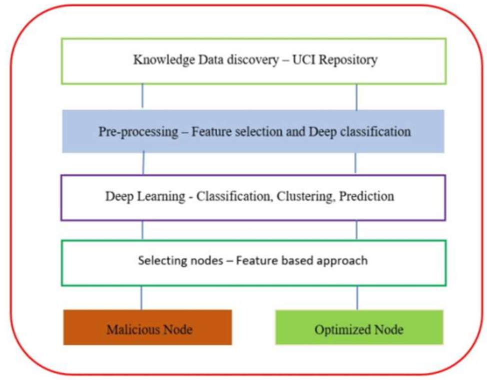


Figure 4 Selecting Node Using KDD Dataset And Deep

5. Learning process

The accuracy feature is calculated as swam intelligence decision feature which can be calculated by using multi stage objective functions with the Eq(4). Here the Empty set represented as R and time factor is set as T. So the classification index is obtained from below equation

$$Accuracy_{(Uij)} = U_{currentnode\_i} + U_{passednode\_i} + Optimization\_factor_{(Decision)} + N$$
(4)

Table 2 Description Of Various Indices For Selecting Features And Swarm Intelligence Process

Terms	Description
i	Iterations
DF	Decision Feature Index factor
Cf	Conditions
SWsize	Swarm Size
N	Nodes
CH	Cluster Heads
GPSset	Global Positioning set result based on current location specifications
R, L	Random Set, Null Set

Algorithm 1: Swarm Intelligence – Feature Selection

Input: KDD UCI Repository Dataset
Output: Deep Optimal Feature Selection

Step 1: Select the conditional feature Cf and Initialize the DF index
Step 2: Select index features R=0, L=1 and i=1
Step 3: Apply the iteration of each node values
Set R(i) <- T(i) and Df(N)

Step 4: Select ∀ X F(CF – R(i) then sort the node with respect to time (Tt),

Checked result are stored to find fitness function.

Step 5: G(f) <-DF(R X N) / SWsize so the each values are measured to find utilization index

Step 6: if CH >=Threshold

Set X = G(F)

Else

Repeat Step 3

Step 7: If Gpset >=R(jj) && SWSize(Node)

Set Feature ==Decision_Result

Else

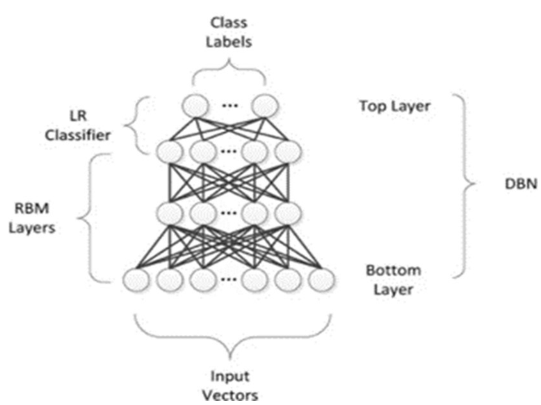
Return 0

Step 8: Feature Result as obtained

$\text{Accuray}_{(Uij)} = U_{currentnode\_i} + U_{passednode\_i} + \text{Optimization\_factor}_{(Decision)} + N$

Step 9: Update the features

From the above representation feature selection is obtained from decision tree and deep neural network prepared by using deep learning as shown in Figure 5.



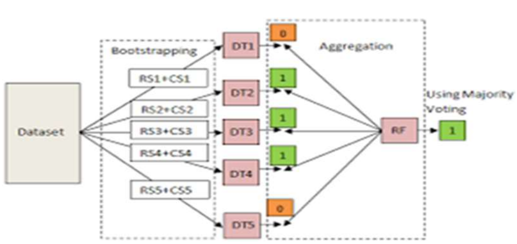


Figure 5Selection Of Malicious Feature With Respect To Classifier Results

Do not begin a new section directly at the bottom of the page, instead, move the heading to the top of the next page.

6. EXPERIMENTAL SETUP AND PERFORMANCE EVALUATION

For the experiments and simulation environment, we used the Tensorflow tool to simulate the system. The experiments are performed using GPU computing devices with multitasking operating systems. Table 3 below shows grid optimization input for our proposed systems

Table 3: Network Simulation Parameters

Simulations Input	Values and Count
Deep Network Size	100 X 100 X 3 Layer
Base Station feature	{50,50}
Sensor Node count	10 – 500
Cluster head index percentage	10-20%
Range	0.05 to 0.50
Energy Index	0.5
Packet Size	100 bytes
Data Rate	64 – 512 bytes
Protocol	ANN Classifier
Sinkhole Nodes	10

Based on the values of the above table, we generate a deep belief network based on the inputs of the swarm intelligence function by adjusting the simulation parameter index as shown in Table 4 and measure the accuracy using the Eq (5).

Table 4 Simulation parameters of swarm intelligence feature

Simulation Index	Values
Decision Variable	100 -1000 neuron
Hop Count	100 - 500
Swarm Size	10,50,100,500
Iteration	5,10,15,20

$$Accuracy(Index) = \frac{1}{N}\sum(Weight_i - Decisio_i) \quad (5)$$

From the inputs above, we calculated the actual sinkhole attacker stats as follows:

The below functions which shown in the Figure 6 are applied to Tensorflow, and a deep belief network is generated using swarm functions. The following Figure 7 shows the result of the Tensorflow simulator from different nodes and swarm functions. In this case, multi-hop routing features are recorded, and all nodes are classified based on feature selection capabilities. Based on this representation, we tested the environment and conducted experiments.

Information Gain, Particle Swarm Optimization and Proposed Hybrid Feature Selection Method

Sl.No	Information Gain	Particle Swarm Optimization	Proposed Hybrid Feature Selection Method
1	num_failed_32s	urgent	Protocol_type
2	srv_diff_host_rate	Wrong_fragment	diff_srv_rate
3	hot	num_compromised	rerror_rate
4	srv_serror_rate	same_srv_rate	srv_serror_rate
5	dst_host_srv_diff_host_rate	diff_srv_rate	srv_rerror_rate
6	same_srv_rate	count	Service
7	rerror_rate	dst_host_srv_diff_host_rate	dst_host_diff_srv_rate
8	logged_in	srv_count	dst_host_count
9	dst_host_srv_serror_rate	dst_host_same_src_port_rate	dst_host_srv_rerror_rate
10	count	dst_host_diff_srv_rate	dst_host_serror_rate
11	dst_host_srv_rerror_rate	dst_host_count	Src_bytes
12	Service	dst_host_rerror_rate	dst_host_srv_count
13	Dst_bytes	dst_host_srv_count	srv_diff_host_rate
14	Src_bytes	dst_host_serror_rate	srv_diff_host_rate
15	dst_host_same_srv_rate	dst_host_srv_serror_rate	dst_host_srv_diff_host_rate
16	dst_host_same_srv_rate	logged_in	serror_rate
17	dst_host_diff_srv_rate	is_guest_32	dst_host_same_src_port_rat e
18	srv_Count	Dst_bytes	srv_Count
19	dst_host_serror_rate	Src_bytes	dst_host_srv_serror_rate
20	dst_host_same_src_port_rate	dst_host_same_srv_rate	Dst_bytes
21	dst_host_count	dst_host_srv_rerror_rate	
22	srv_rerror_rate	Service	
23	diff_srv_rate	hot	
24	serror_rate	srv_rerror_rate	
25	is_guest_32	Flag	
26	Protocol_type	rerror_count	
27	num_compromised	srv_serror_rate	
28		serror_rate	
29		Protocol_type	
30		srv_diff_host_rate	
31		num_failed_32s	
32		land	

Figure 6Selected Features Based On Input Dataset Using Swarm Intelligence

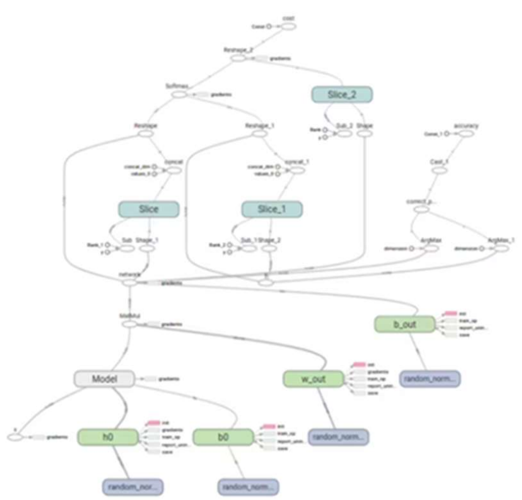


Figure 7 Tensorflow Result Of Swam Feature Classification.

The representations are appropriately accepted for evaluation and simulations are carried out. Based on this, Table 5 shows the result of the swarm characteristics

Table 5 Simulation Result Of Kdd Uci Repository – Decision Rate And Accuracy

Swarm Size	Nodes	Packet Size	Hop Count	Decision Rate	Accuracy in %
10	5	64,128,512	100 - 500	0.97,0.96,0.96	96,94,96
	10	64,128,512	100 - 500	0.95,0.97,0.94	96,94,96
	15	64,128,512	100 - 500	0.95,0.95,0.96	95,96,94
	20	64,128,512	100 - 500	0.97,0.98,0.96	94,95,94
50	5	64,128,512	100 - 500	0.97,0.96,0.96	95,96,97
	10	64,128,512	100 - 500	0.95,0.97,0.94	96,94,96
	15	64,128,512	100 - 500	0.95,0.95,0.96	96,94,96
	20	64,128,512	100 - 500	0.97,0.98,0.96	95,96,94
100	5	64,128,512	100 - 500	0.95,0.97,0.94	94,95,94
	10	64,128,512	100 - 500	0.95,0.95,0.96	95,96,97
	15	64,128,512	100 - 500	0.97,0.98,0.96	96,94,96

The result of the table above has measured the decision rate and accuracy index of malicious node results. Based on this number, a malicious node can be identified using the execution of each process. From the above results, Table 6 shows the processing time, turnaround time and malicious node classifications. In this case, the total number of nodes can be set to 20 and the burst time for each process is recorded as 0.50 ms.

Table 6 Malicious Node Results Using Execution Of Decision Rate.

Swarm Size	Hop Count	No.of Active Nodes	Waiting Time	Turn Around Time	Malicious Node Count
10	100 - 500	18	0.65	0.32	2
50	100 - 500	16	0.68	0.33	4
100	100 - 500	17	0.71	0.32	3
500	100 - 500	18	0.71	0.32	2

From the above results, there is an average accuracy index of 95% and an optimization component of 45%. So, the number of nodes can be increased and iterated, which means that the sinkhole attackers' results will show up as negative. From this plot, the average true positive result is shown in Figure 8 below. The chart below shows the average number of positive or active node counts and swarm optimization results.

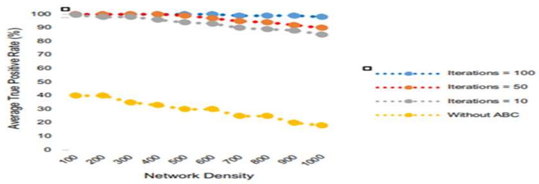


***Figure 8** Result Of Average Positive Node Count And Network Density With Respect Swarm Optimizer.*

Multiple iterations can be performed to measure the average convergence speed, which can be calculated since the processing time of each process can be executed. Figure 9 below shows the average cycle time and network density values based on number of iterations. The following chart result shows that the average throughput time is measured using the swarm classifier intelligence approach

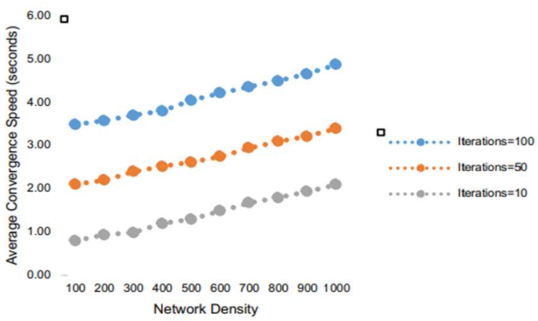


Figure 9 Result Of Average Cycle Time And Network Density With Respect Swarm Optimizer

Our proposed swarm intelligence classifier gave a good accuracy result. We can choose deep learning method to measure accuracy, precision, and score function. The result is compared to existing methodologies and is shown in the Figure 10

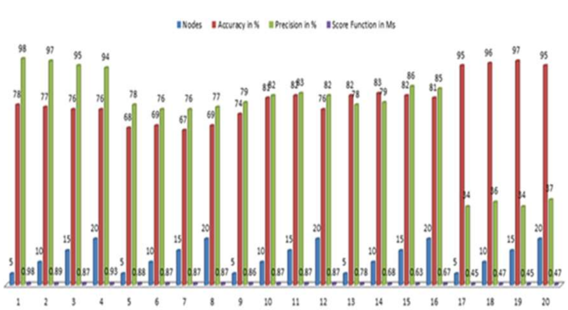


Figure 10 Result Of Accuracy, Precision, And Score Function.

Our proposed method is compared to existing methods such as Support Vector Machine, Toposearch, Residue Index and CNN Classification and the results are tabulated in Table 7. Compared to these results, our proposed method offers a better accuracy index, better precision, and malicious node detection

Table 7 Comparison Of Proposed Method With Existing Methodologies

Approach	Nodes	Hop count	A*	P*	S*	M*
Support Vector Machine	5	100 - 500	78	98	0.98	25-40
	10	100 - 500	77	97	0.89	25-60
	15	100 - 500	76	95	0.87	30-60
	20	100 - 500	76	94	0.93	35-70
TopoSearch	5	100 - 500	68	78	0.88	27-67
	10	100 - 500	69	76	0.87	29-48
	15	100 - 500	67	76	0.87	29-60
	20	100 - 500	69	77	0.87	32-59
Residue Index	5	100 - 500	74	79	0.86	45-76
	10	100 - 500	81	82	0.87	45-87
	15	100 - 500	82	83	0.87	50-89
	20	100 - 500	76	82	0.87	52-88
CNN Classification	5	100 - 500	82	78	0.78	63-105
	10	100 - 500	83	79	0.68	68-110
	15	100 - 500	82	86	0.63	72-98
	20	100 - 500	81	85	0.67	75-125
Swarm Intelligence	5	100 - 500	95	34	0.45	100-200
	10	100 - 500	96	36	0.47	125-205
	15	100 - 500	97	34	0.45	150-300
	20	100 - 500	95	37	0.47	200-400

where
A* is Accuracy in %
P* is Precision in %
S* is Score Function
M* is Malicious Node Count

7. CONCLUSION:

Deep learning is the approach to effective decision making. In our work, we proposed a swarm intelligence method to detect malicious nodes in wireless sensor networks. Detecting malicious nodes using an intelligent approach is a recent trend, and various researchers suggest finding only the active nodes of the network lifetime. We applied classification, regression, and clustering process selection functions. The selected features are applied for swarm intelligence selection and the TensorFlow simulator is used to simulate the network and measurement accuracy. The KDD UCI repository dataset is used for evaluation and for applying deep learning techniques to simulations.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Based on execution, our suggested system accuracy index averages 95% and compares the result to existing methods. From the result, our proposed system gives better results. In the future, swarm intelligence methods can be applied to real-time IT and ITeS datasets.

REFERENCES

[1] S. D. Roy, S. A. Singh, S. Choudhury and N. C. Debnath, "Countering sinkhole and black hole attacks on sensor networks using Dynamic Trust Management," 2021 IEEE Symposium on Computers and Communications, Marrakech, 2021, pp. 537-542.

[2] C. Blum, and X. Li, "Swarm intelligence in optimization," Swarm Intelligence . Springer, Berlin, Heidelberg. pp. 43-85, 2018.

[3] S. Manikandan, K. S. R. Radhika, M. P. Thiruvenkatasuresh and G. Sivakumar, "Deepq: Residue analysis of localization images in large scale solid state physical environments"AIP Conference Proceedings 2393, 020078 (2022)

[4] D. Karaboga, "An idea based on honey bee swarm for numerical Optimization," Erciyes university, engineering faculty, computer engineering department. 2015.

[5] J. Singh, R. kumar and A. K. Mishra, "Clustering algorithms for wireless sensor networks: A review," 2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, 2015, pp. 637-642.

[6] Y. H. Lee, J. H. Kang, and S. J. Lee, "A specification-based intrusion detection mechanism for leach protocol," The Journal of Korean Institute of Communications and Information Sciences, pp. 138-147, 2019

[7] S. Manikandan, P. Dhanalakshmi, K. C. Rajeswari and A. Delphin Carolina Rani, "Deep sentiment learning for measuring similarity recommendations in twitter data," Intelligent Automation & Soft Computing, vol. 34, no.1, pp. 183–192, 2022

[8] S. Manikandan and M. Chinnadurai, "Evaluation of Students' Performance in Educational Sciences and Prediction of Future Development using TensorFlow",International Journal of Engineering Education Vol. 36, No. 6, pp. 1783–1790, 2020, 0949-149X/91, TEMPUS Publications

[9] F. Ishmanov, and Y. Bin Zikria, "Trust Mechanisms to Secure Routing in Wireless Sensor Networks: Current State of the Research and Open Research Issues," Journal of Sensors, 2020.

[10] Manikandan, S & Chinnadurai, M 2019, 'Intelligent and Deep Learning Approach OT Measure E-Learning Content in Online Distance Education', The Online Journal of Distance Education and e-Learning, vol.7, issue 3, July 2019, ISSN: 2147-6454

[11] Rethinavalli, S., & Gopinath, R., Classification Approach based Sybil Node Detection in Mobile Ad Hoc Networks, International Journal of Advanced Research in Engineering and Technology, 11(12), 3348- 3356 (2020).

[12] Rethinavalli, S., & Gopinath, R., Botnet Attack Detection in Internet of Things using Optimization Techniques, International Journal of Electrical Engineering and Technology, 11(10), 412-420 (2020).

[13] Priyadharshini, D., Poornappriya, T.S., & Gopinath, R.,A fuzzy MCDM approach for measuring the business impact of employee selection, International Journal of Management (IJM), 11(7), 1769-1775 (2020).

[14] Poornappriya, T.S., Gopinath, R., Application of Machine Learning Techniques for Improving Learning Disabilities, International Journal of Electrical Engineering and Technology (IJEET), 11(10), 392-402 (2020).

[15] Benjie Chen, Kyle Jamieson, Hari Balakrishnan And Robert Morris" An Energy-Efficient Coordination Algorithm for Topology Maintenance in Ad Hoc Wireless Networks," in Proceedings of the wireless network, 2019.

[16] Subhashini, M., & Gopinath, R., Mapreduce Methodology for Elliptical Curve Discrete Logarithmic Problems – Securing Telecom Networks, International Journal of Electrical Engineering and Technology, 11(9), 261-273 (2020).

[17] Upendran, V., & Gopinath, R., Feature Selection based on Multicriteria Decision Making for Intrusion Detection System, International Journal of Electrical

Engineering and Technology, 11(5), 217-226 (2020).

[18] Upendran, V., & Gopinath, R., Optimization based Classification Technique for Intrusion Detection System, International Journal of Advanced Research in Engineering and Technology, 11(9), 1255- 1262 (2020).

[19] S.Manikandan, M.Chinnadurai, D.Maria Manuel Vianny and D.Sivabalaselvamani, "Real Time Traffic Flow Prediction and Intelligent Traffic Control from Remote Location for Large-Scale Heterogeneous Networking using TensorFlow", International Journal of Future Generation Communication and Networking, ISSN: 2233-7857, Vol.13, No.1, (2020), pp.1006-1012.

[20] Manikandan S, Chinnadurai M, Thiruvenkatasuresh M.P, Sivakumar M. (2020). "Prediction of Human Motion Detection in Video Surveillance Environment Using Tensor Flow", International Journal of Advanced Science and Technology, 29(05), 2791 - 2798.