ISSN: 0974-8571 Vol.13 No. 2 December, 2021

International Journal of Computational Intelligence in Control

DETECTION OF MALICIOUS NODE WITH FEATURE SELECTION METHOD IN WIRELESS SENSOR NETWORK

S. Saminathan, Research Scholar, PG & Research Department of Computer Science, Government Arts College (Autonomous) (Affiliated to Bharathidasan University, Tiruchirappalli), Karur, Tamilnadu, India.

Dr. A.Vinayagam, Assistant Professor, PG & Research Department of Computer Science, Government Arts College (Autonomous) (Affiliated to Bharathidasan University, Tiruchirappalli), Karur, Tamilnadu, India

Date of Submission:10th August 2021 Revised: 25th October 2021 Accepted: 13th December 2021

Abstract: As an important medium of information transmitting, Wireless Sensor Networks (WSN) is at risk of a series of malicious nodes. In view of the inefficiency of the existing malicious node detection methods in Wireless Sensor Networks, this paper proposed a malicious node detection model based on the Feature Selection methods and Classification techniques. A Novel Hybrid Feature Selection method mounts on Particle Swarm Optimization (PSO) and Information Gain analysis. The execution of the proposed Hybrid Feature Selection Method on KDD CUP dataset to decrease the volume of primary features and accurate by implementing better detection performance in the classification methods relating with other feature selectors. The relevant features and removing redundant features of KDD CUP dataset is Optimal Dataset. ANN with Multi-Layered Perceptron classification method was used to classify the nodes of WSN. The performance of the proposed malicious node detection method is compared with the various metrics like accuracy, error rates with their existing feature selection methods and classification techniques.

KEYWORDS: Wireless Sensor Networks, Malicious Node detection, Intrusion Detection, KDD CUP, Optimization, Feature Selection, Classification

1. INTRODUCTION

A Wireless Sensor Network (WSN) is defined as a highly distributed network formed by large number of small, lightweight sensor nodes where each node is equipped with a sensor to detect physical phenomena such as light, heat, pressure, etc. WSN consists of a base station, a sink and sensor nodes. The sensor nodes are mostly deployed in harsh environments and they have the facility to sense, process data and communicate with each other via a wireless connection. Sensory information collected by the sensor nodes is communicated to the base station which is the centralized point of control within the network through hop-by-hop transmissions. The data collected is aggregated at the aggregator node and only the aggregate values are forwarded to the base station. Using aggregation, the overall energy requirements of the network can be reduced by decreasing the amount of network traffic.

A Wireless Sensor Network (WSN) is an integral component of the broader term, The Internet of Things (IoT). According to [1], the WSN is described as a network of nodes that collaborate to sense data around its domain, and thereby controlling the surrounding environment. Due to the variety of its applications in military, healthcare, industrial control and monitoring and many more, WSNs have emerged as a dominant technology for the future. Wireless networks are vulnerable to security attacks due to the nature of the wireless broadcast medium. WSNs have additional vulnerabilities due to the resource limitations in the sensor nodes. Moreover, the sensor nodes can be deployed in an unattended environment, which makes them physically unsafe and can be captured by adversaries. The compromised sensors may not only be used for distribution of unwanted or false information, but can also degrade the performance of the entire network. Therefore, the security of WSNs becomes a major concern that attracts many researchers.

There are a number of attacks that exploit vulnerabilities of WSNs such as Denial of service (DoS) attack, HELLO flood attack, Sybil attack, Black hole attack, wormhole attack, selective forwarding attack, and sinkhole attack [2][3]. Most of the routing protocols in WSNs are not primarily designed with security considerations due to the resource limitations on the sensor nodes. This can make them vulnerable to various types of attacks [2]. Among such attacks against WSNs, a sinkhole attack has the ability to undermine the effectiveness of the network by attracting nearby nodes with false information and be able to launch further attacks. Sinkhole attack can result in dropping the sensed data packets or altering the data that pass through the compromised node [4]. Although many solutions were proposed in the literature to detect sinkhole attacks in WSNs, accuracy, and robustness of the detection of the true attacker remains a critical problem. Limitations of existing solutions require us to rethink novel and more effective solutions in terms of accuracy and speed of detection of the attack in WSNs. The capability of detection algorithms is highly dependent on the accuracy of attack detection [7][8][9][10][11][12][13][14].

2. FEATURE SELECTION TECHNIQUES

2.1 Chi-Square Analysis

Feature Selection via chi-square χ^2test [1] is another, very commonly applied method. CS attribute evaluation estimates the goodness of a feature bymeasuring the significance of the chi-squared statistic to the class. The firsthypothesis H_0 is the premise that the two features are irrelevant, and a chi-squared formula test it:

$$\chi^2 = \sum_{i=1}^{r}\sum_{j=1}^{c}\left(\frac{O_{ij}-E_{ij}}{E_{ij}}\right)^2 \quad (4.1)$$

where O_{ij} is the observed frequency, and E_{ij} is the expected (theoretical) frequency, affirmed by the null hypothesis [2]. The higher the value ofχ^2, the higher the proof upon the hypothesis H_0.

2.2 Symmetrical Uncertainty

The symmetrical uncertainty (SU) [3] between target concept and features are applied to obtain the best features for classification. The elements with higher SU values have the higher weight. SU measures the relationship among A, B variables based on the information theory. It was calculated as follows

$$SU\ (A,)\ B = 2\ \frac{I\ (A,B)}{H(B)A + H\ (B)}$$

Computing I(A, B) as the MI among A, B. H(..) as an entropy function for A, B features. The SU shows the normalized range value [0,1] as correction factor value is 2. If SU value is 1, then the information of one feature is predictable. If SU value is 0, then A, B are not associated.

2.3 Information Gain

Entropy is generally utilized in the information theory measure, which defines the purity of an absolute collection of examples. It is in the foundation of Gain Ratio, Information Gain and Similarity Uncertainty (SU) [3]. The entropy measure is considered a measure of the system's unpredictability. The entropy of Y is

$$H(Y) = \sum_{y\in Y} p(y)\log_2(p(y)) \quad (3.1)$$

Where *p(y)* is the marginal probability density function for the random variable *Y*. If the observed values of *Y* in the training data set *S* have partitioned according to the values of a second feature *X*, and the entropy of *Y* for the partitions induced by *X* is less than the entropy of *Y* before partitioning, then there is a relationship between features *Y* and *X*. The entropy of *Y* after observing *X* is then:

$$H(Y|X) = \sum_{x\in X} p(x)\sum_{y\in Y} p(y|x)\log_2\big(p(y|x)\big) \quad (3.2)$$

where *p(y |x)* is the conditional probability of *y* given *x*.

Given the entropy is a criterion of impurity in a training set *S*, we can define a measure reflecting additional information about *Y* provided by *X* that represents the amount by which the entropy of *Y* decreases. This measure is known as IG. It is given by

$$IG = H(Y) - H(Y|X) = H(X) - H(X|Y) \quad (3.3)$$

IG [4] is a symmetrical measure and it is given by equation (3.3). The information gained about *Y* after observing *X* is equal to the information gained about *X* after observing *Y*. Aweakness of the IG criterion is that it is biased in favour of features with more values even when they are not more informative.

3. PARTICLE SWARM OPTIMIZATION

PSO [4][5] was depend on the social behaviour connected with bird's assembling for the optimization problem. A social behaviour model of organisms that interact and live with big crowds is the motivation for PSO. The PSO is more accessible to put into action than Genetic Algorithm. It is for the motive that PSO does not

have a crossover or mutation operators and flow of particles has affected by using velocity function. In PSO, each particle changes its flying memory and its partner's flying inclusion following in mind the top goal of flying in the search space with velocity.

4. PROPOSED MALICIOIUS NODE CLASSIFICATION METHODOLOGY

In this framework, the next two phases are required to build the efficient malicious node identification method. KDD CUP dataset has utilized to analyse the behaviour of the malicious node.

Phase 1: Pre-Processing Phase: The importance of pre-processing is to decrease the dimension of the dataset. It is employed to remove the redundant and irrelevant features and to enhance the classification efficiency of the attacks in the networks. In this stage, a new hybrid feature selection method has proposed.

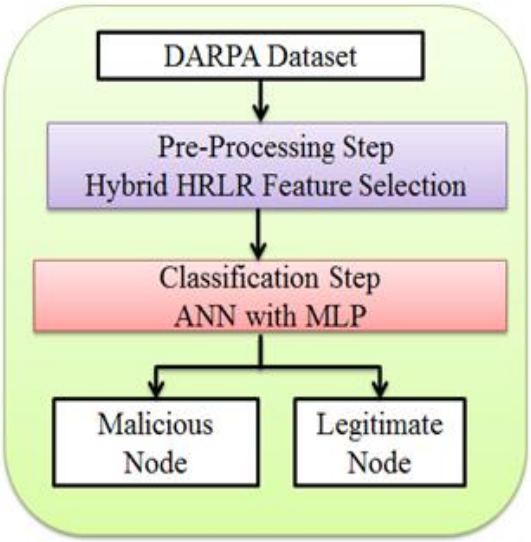

Figure 1: Proposed Framework for Classification of Malicious Node in WSN

This hybrid method combines the technique of Chi-Square analysis and Particle Swarm Optimization (PSO) technique. These two techniques are hybridized to give the most appropriate features and low redundant for the classification of a node in the network.

Phase 2: Classification phase: In this stage, the ANN classification method is applied to separate the node to their behaviour in the network. This method uses a MLP-NNfor classification.

4.1 Pre-Processing Step: Hybrid Feature Selection Method

This method has proposed with the combination PSO and IG analysis. Then the classification accuracy of the particle is examined with the Decision Feature. If the accuracy of the feature has a value prominent than the Decision Feature, then the feature is collected in T and passed to empty set R. Now, the R has an attribute with higher classification accuracy. Then the velocity is calculated and updated by applying the equation

$$U_{ud} = U_{ud} + C1i1(p_{jd} - y_{jd}) + C2i2(p_{gd} - y_{jd})$$

$$Y_{jd} = Y_{jd} + U_{ud}$$

This procedure iterated until the classification accuracy of the Similarity Uncertainty SU based on decision feature Df is equal to the classification accuracy of conditional feature based on Df. The final output is the optimal data set.

Table 1: Algorithm terms and its description

Term	Description
ω	Inertia
DeF	Decision Features
CoF	Conditional Feature
s&c	Social and Cognitive Components
SS	Swarm Size
DFV	Data Fitness Value
p_{best}	Particle Best Position
G_{best}	Global Best Position
R	Null Set
T	Feature Set
U_{ud}	A velocity of the Particle
y_{jd}	Individual Best position
r1 &r2	Random Values

The pseudo code for the Hybrid HRLR Feature Selection Method

Input: KDD CUP dataset
Output: Optimal Dataset
Step 1: *Initialize Conditional Features(CoF) and Decision Feature (DoF)by using IG analysis.*
Step 2: *Initialize SS = 20, s = 2.0, c=2.0, r1,r2=0.2 and .ω= 0.33*
Step 3: *For each particle r in SS do*
Step 3.1: Set R ←{ }
Step 3.2: Set T ← R

Step 3.3: Initialize $\forall x \in (CoF - R)$ *after storing the empty data set in T, the conditional features have checked with an empty set*

Step 3.4: Calculate Data Fitness Value using Griewangk function

Step 4: *If DFV >*P_{best}

Step 4.1: Set P_{best} *= DFV*

Step 5: *If* P_{best} $>G_{best}$

Step 5.1: Set P_{best} *=* G_{best}

Step 6:*if* $_{RU}(x) > \gamma_T(DoF)$

Step 6.1: Set $T \leftarrow R_U(X)$

Step 6.2: $R \leftarrow T$

Step 7: *Calculate and update the velocity by using the equation*

$$U_{ud} = U_{ud} + C1i1(p_{jd} - y_{jd}) + C2i2(p_{gd} - y_{jd})$$

$$Y_{jd} = Y_{jd} + U_{ud}$$

Step 8:*Repeat the process from step 3 until* $\gamma_R(DoF) == \gamma_C(DoF)$ *is satisfied.*

Step 8.1: If $\gamma_R(DoF) == \gamma_C(DoF)$

Step 8.2: Return R

4.2 Classification Step: Artificial Neural Network

ANN is an effective calculating system whose principal theme has acquired from the resemblance of biological NN. ANNs has also described as "Parallel Distributed Processing Systems." ANN obtains a massive number of units that are interrelated in some pattern to enable connection among the units. Those units also mentioned to as neurons or nodes are mere CPUs which operate in parallel. In this work, the ANN has adopted for classification of Intrusion Detection in the system. The following method depicts the steps of the MLP-NN training algorithm.

Step 1: *Initialize Bias, Learning rate* α*, weights, to begin the training of Multi-Layered Perceptron Neural Network. For simplicity and calculation, need to set weight =0 and bias* $\alpha = 1$.

Step 2: *Proceed step 3-8 at the terminating condition is true.*

Step 3: *Proceed step 4-6 for all training vector a.*

Step 4: *Initiate each input as follows:*

$$r_j = s_j \ (j = 1 \ to \ m)$$

Step 5: *Get the net input with the next relations*

$$s_{jn} = b + \sum_{j}^{m} r_j w_{jk}$$

Here bias is given as b, and the whole amount of input neuron is given by 'n'.

Step 6: *Apply the activation function to obtain the final output for each input*

unit k=1 to n

$$f(s_{jm}) = \begin{cases} 1 & if \ s_{jmk} > \theta \\ 0 \ if \ -\theta \le s_{jmk} \le \theta \\ -1 \ if \ s_{jmk} < -\theta \end{cases}$$

Step 7: *Adjust the weight and bias for r=1 to m and k=1 to n as follows:*

Step 7.1: Case 1: if $s_k \neq t_k$ *the m*

$$w_{jk}(new) = w_{jk}(old) + \propto t_k r_j$$

$$s_k(new) = s_k(old) + \propto t_k$$

Step 7.2: Case 2: if $s_k = t_k$ *then*

$$w_{jk}(new) = w_{jk}(old)$$

$$s_k(new) = s_k(old)$$

Here 's' is the exact output, and 't' is the desired/target output.

Step 8: *Testing for terminating condition, which will occur while there is no variation in weight.*

5. RESULT AND DISCUSSION

5.1 Number of Features obtained by proposed Feature Selection Method

Following table 2 provides the outcome attained by the proposed Hybrid Feature Selection method and current filter-based feature selection techniques like Information Gain and Particle Swarm Optimization. From table 2, Particle Swarm Optimization filters 31 features, Information Gain screens only 27 features, and the proposed Hybrid Feature Selection gives only 20 features. To assess the competence of the proposed Hybrid Feature Selection and other approaches by consuming classification techniques like Artificial Neural Network (ANN) and Support Vector Machine (SVM). The assessment of metrics is like Accuracy, True Positive Rate (TPR), Precision and Error rates like False Positive Rate (FPR), False Discovery Rate (FDR) and Miss Rate (MR).

Table 2: Number of Features obtained by using 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_rate
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	

Table 3 depicts the Classification Accuracy (in %) obtained by the proposed Hybrid Feature Selection Method, Information Gain and Particle Swarm Optimization methods processed datasets using Artificial Neural Network (ANN) and Support Vector Machine (SVM) classification techniques. From the table 3, it is clear that the proposed HFS method with ANN gives more accuracy than the SVM classification method.

Table 3: Classification Accuracy of Original Dataset, Information, PSO and Proposed Hybrid Feature Selection method using ANN, and SVM classification methods

Feature Selection Methods	Classification Methods (in %)	
	ANN	SVM
Original Dataset	69.333	64.111
Information Gain	89.667	74.471
Particle Swarm Optimization	91.25	69.667
Proposed HFS Method	93.67	82.778

Table 4 depicts the True Positive Rate (in %) obtained by the proposed Hybrid Feature Selection Method, Information Gain and Particle Swarm Optimization methods processed datasets using Artificial Neural Network (ANN) and Support Vector Machine (SVM) classification techniques. From the table 4, it is clear that the proposed HFS method with ANN gives more TPR than the SVM classification method.

Table 4: True Positive Rate (in %) of Original Dataset, Information, PSO and Proposed Hybrid Feature Selection method using ANN, and SVM classification methods

Feature Selection Methods	True Positive Rate (in %)	
	ANN	SVM
Original Dataset	69.3	64.2
Information Gain	84.7	66.4
Particle Swarm Optimization	86.58	70.4
Proposed HFS Method	92.79	81.6

Table 5 depicts the False Positive Rate (in %) obtained by the proposed Hybrid Feature Selection Method, Information Gain and Particle Swarm Optimization methods processed datasets using Artificial Neural Network (ANN) and Support Vector Machine (SVM) classification techniques. From the table 5, it is clear that the proposed HFS method with ANN reduces FPR than the SVM classification method.

Table 5: False Positive Rate (in %) of Original Dataset, Information, PSO and Proposed Hybrid Feature Selection method using ANN, and SVM classification methods

Feature Selection Methods	False Positive Rate (in %)	
	ANN	SVM
Original Dataset	35.5	45.1
Information Gain	30.7	38.1
Particle Swarm Optimization	29.4	32.2
Proposed HFS Method	15.21	21.2

Table 6 depicts the Precision (in %) obtained by the proposed Hybrid Feature Selection Method, Information Gain and Particle Swarm Optimization methods processed datasets using Artificial Neural Network (ANN) and Support Vector Machine (SVM) classification techniques. From the table 6, it is clear that the proposed HFS method with ANN gives more Precision than the SVM classification method.

Table 6: Precision (in %) of Original Dataset, Information, PSO and Proposed Hybrid Feature Selection method using ANN, and SVM classification methods

Feature Selection Methods	Precision (in %)	
	ANN	SVM
Original Dataset	55.3	49.4
Information Gain	84.3	74.7
Particle Swarm Optimization	85.3	75.89
Proposed HFS Method	92.37	86.56

Table 7 depicts the Specificity (in %) obtained by the proposed Hybrid Feature Selection Method, Information Gain and Particle Swarm Optimization methods processed datasets using Artificial Neural Network (ANN) and Support Vector Machine (SVM) classification techniques. From the table 7, it is clear that the proposed HFS method with ANN gives more Specificity than the SVM classification method.

Table 7: Specificity (in %) of Original Dataset, Information, PSO and Proposed Hybrid Feature Selection method using ANN, and SVM classification methods

Feature Selection Methods	Specificity (in %)	
	ANN	SVM
Original Dataset	64.5	54.9
Information Gain	69.3	61.9
Particle Swarm Optimization	70.6	67.8
Proposed HFS Method	84.79	78.8

Table 8 depicts the Miss Rate (in %) obtained by the proposed Hybrid Feature Selection Method, Information Gain and Particle Swarm Optimization methods processed datasets using Artificial Neural Network (ANN) and Support Vector Machine (SVM) classification techniques. From the table 8, it is clear that the proposed HFS method with ANN reduced the Miss Rate than the SVM classification method.

Table 8: Miss Rate (in %) of Original Dataset, Information, PSO and Proposed Hybrid Feature Selection method using ANN, and SVM classification methods

Feature Selection Methods	Miss Rate (in %)	
	ANN	SVM
Original Dataset	30.7	35.8
Information Gain	15.3	33.6
Particle Swarm Optimization	13.42	29.6
Proposed HFS Method	7.21	18.4

Table 9 depicts the False Discovery Rate (in %) obtained by the proposed Hybrid Feature Selection Method, Information Gain and Particle Swarm Optimization methods processed datasets using Artificial Neural Network (ANN) and Support Vector Machine (SVM) classification techniques. From the table 9, it is clear that the proposed HFS method with ANN reduced FDR than the SVM classification method.

Table 9: False Discovery Rate(in %) of Original Dataset, Information, PSO and Proposed Hybrid Feature Selection method using ANN, and SVM classification methods

Feature Selection Methods	False Discovery Rate(in %)	
	ANN	SVM
Original Dataset	44.7	50.6
Information Gain	15.7	25.3
Particle Swarm Optimization	14.7	24.11
Proposed HFS Method	7.63	13.44

6. CONCLUSION

Wireless sensor networks are randomly deployed and responsible for monitoring geographical area wide. In WSN, the aggregation of data is very complex because of its limited power and computing capabilities. Issue in data aggregation is that the data may be passed on malicious node. Through this research work, KDD CUP 99 data is considered to build a malicious node detection method with Feature Selection and Classification techniques. The feature selection methods like Information Gain (IG) and Particle Swarm Optimization (PSO) are hybridized to find the most relevant features for improving the accuracy of the malicious node detection. The classification of malicious node is obtained with the Artificial Neural Network (ANN) classification method. From the results obtained, it is clear that the proposed HFS method with ANN gives better result than the other feature selection methods with SVM classification method.

REFERENCES

[1] Thaseen I.S., Kumar C.A, "Intrusion Detection Model Using Chi-Square Feature Selection and Modified Naïve Bayes Classifier," Proceedings of the 3rd International Symposium on Big Data and Cloud Computing Challenges (ISBCC – 16').Smart Innovation, Systems and Technologies, Vol. 49.Springer, pp 81-91,2016.

[2] Abualigah, Laith Mohammad, and Ahamad Tajudin Khader. "Unsupervised text feature selection technique based on hybrid particle swarm optimization algorithm with genetic operators for the text clustering." *The Journal of Supercomputing* 73.11 (2017): 4773-4795.

[3] Satpute, Khushboo, and Rishik Kumar. "Optimization of Adaptive Resonance Theory Neural Network Using Particle Swarm Optimization Technique." *Advances in Machine Learning and Data Science*. Springer, Singapore, 2018. 1-7.

[4] Gu, Shenkai, Ran Cheng, and Yaochu Jin. "Feature selection for high-dimensional classification using a competitive swarm optimizer." *Soft Computing* 22.3 (2018): 811-822.

[5] Macia´-Pe´rez, F.: Network intrusion detection system embedded on a smart sensor, industrial electronics. IEEE Trans. 58(3), 722– 732 (2012).

[6] 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, 2002.

[7] 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).

[8] 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).

[9] 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).

[10] Subhashini, M., & Gopinath, R., Employee Attrition Prediction in Industry using Machine Learning

Techniques, International Journal of Advanced Research in Engineering and Technology, 11(12), 3329-3341 (2020).

[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).