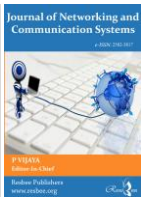
Resbee Publishers

Journal of Networking and Communication Systems

Received 7 July, Revised 4 September, Accepted 7 October



Intrusion Detection System for Wireless Mesh Networks via Improved Whale Optimization

Dr. Sesham Anand
Professor of CSE
Maturi Venkata Subba Rao Engineering College, Hyderabad
seshamanand282015@gmail.com

Abstract: Wireless Mesh networks (WMNs) suffers from abundant security issues because of its dynamic and open communication channels. It is thus risky to formulate an Intrusion Detection System (IDS) that could make out diverse unidentified attacks in the network. This paper intends to propose an Improved Selection of Encircling and Spiral updating position of WO (ISESW) based model for detecting the attacks in WMN systems. The adopted scheme includes two phase's namely, Feature Selection and Classification. Initially, the features (informative features) from the given data are selected using Principal Component Analysis (PCA) model. The selected informative features are then subjected to classification process using Neural Network (NN), where the presence of attacks is classified. To make the detection more accurate, the weights of NN are fine-tuned using the ISESW algorithm, which is the improved version of WOA model. Finally, the superiority of adopted scheme is evaluated over traditional models in terms of varied measures.

Keywords: Intrusion Detection; Mesh networks; ; PCA Framework; Neural network; Whale Algorithm.

Nomenclature

Abbreviation	Description
CNN	Convolutional Neural Network
ELM	Extreme learning machine
FPR	False Positive Rate
FNR	False Negative Rate
ISESW	Improved Selection of Encircling and Spiral updating position of Whale
KBIDS	Knowledge-Based Intrusion Detection Strategy
MSCA	Mean Shift Clustering Algorithm
NN	Neural Network
NIDS	Network Intrusion Detection System
PDR	Packet Delivery Ratio
PCA	Principal Component Analysis
RFA	Recursive Feature Addition
RBM	Restricted Boltzmann Machine
SD	Standard Deviation
SVM	Support Vector Machine
WSN	Wireless Sensor Networks
WMNs	Wireless Mesh Networks

1. Introduction

In WMNs, security has a very important significance. In recent times, it has been emerging as a advanced communication mechanism and it is suited for many appliances in military and grids [1] [2]. However, due to the multi-hop nature, the WMNs suffer from diverse attacks that include DoS attacks, forwarding attacks, hijack attacks and tampering attacks. It is not feasible to find a solution using prevention-oriented equipment for solving entire security problems; thus, detection approaches were developed that offers an effective solution to the security challenges [3].

Intrusion detection is defined as "the process of monitoring the events occurring in a computer system or network and analyzing them for signs of intrusions, defined as attempts to compromise the confidentiality, integrity, availability, or to bypass the security mechanisms of a computer or network"

https://doi.org/10.46253/jnacs.v3i4.a2

[4]. IDSs are software or hardware systems, which monitors the event occurring in a network and analyzes them for security threats. As attacks in WSN have enlarged for the past few years, IDS have turn out to be a essential part of the majority of organizations for their secure communication [5].

Network-oriented IDSs are composed of a set of single-purpose hosts or sensors positioned at different spots in a network. These sensors monitor the traffic of network, perform local analysis of the traffic and inform the attacks to a central management system. Since the sensors included certain limitations to run the IDS, they could be highly secured against attacks. Numerous sensors are modelled to run in "stealth mode", which makes it trickier for an attacker to find out their location and presence [14].

The arrangement of the work is as follows. Section II discusses the reviews done on WMN systems. Section III describes the proposed intrusion detection framework for WMN and section IV portrays the PCA based feature selection and optimized NN based classification. Moreover, section V portrays the results and section VI concludes the paper.

2. Literature Review

2.1 Related Works

In 2018, C. Wang *et al.* [1] have developed ELM based model for detecting the intrusions in WSN. Moreover, an incremental approach was adopted that derived the optimum count of hidden neurons. In addition, a binary search based optimization was developed that raised the count of hidden neurons. At last, the simulation results have shown the better performance of the adopted model with high learning speed and best attack detection rates.

In 2018, Baykara and Resul [2] have suggested a scheme for minimizing the cost of maintenance and configuration of networks. The introduced scheme was capable of demonstrating the network congestion on servers in real-time. Thus, it offered system information without difficulty. At last, the introduced arrangement identified zero-day attack owing to the modelling of ID that offered better performance over other IDSs.

In 2018, Aldwairi et al. [3] have illustrated the usage of RBM approach for evaluating anomalous and normal Net Flow traffic. Here, the introduced technique was evaluated on the well-known "ISCX dataset" and the outcomes pointed out that the adopted model categorized anomalous and normal traffic flow effectively. Moreover, a balanced set was utilized that decreased the biases, which appeared throughout the training of RBM.

In 2018, Qu et al. [4] have established a KBIDS model for linking the gap between balancing. Here, initially, MSCA differentiated the abnormal patterns that imitated the atypical behaviour of a WSN from a usual context. Subsequently, the SVM model was employed for increasing the margin among normal and abnormal characteristics and thus, the classification error was reduced.

In 2018, Tarfa et al. [5] have adopted a NIDS that was dependent on two schemes, namely, RFA and bigram method. Accordingly, the bigram method was suggested for encoding payload string characteristics into a constructive model, which could be exploited in feature selection. Furthermore, a novel assessment measure was considered that evaluated the diverse systems and it chooses the most excellent between them. Finally, the enhancement of the presented scheme was validated in terms of diverse measures.

3. Proposed Intrusion Detection Framework for Wireless Mesh Networks

3.1 Proposed Architecture

In this paper, a new intrusion detection model is proposed with two major phase's viz. Feature Selection and Classification, which is illustrated in Fig.1. Initially, the input data is subjected to feature selection process, where the informative features are selected using PCA framework. The selected features are then subjected to NN classifier for classification purpose. The output attained from NN demonstrates either "belongs to the attack category" or "does not belong to the attack category". Further, in order to make the WMN system more precise, the weights of NN are fine-tuned using the ISESW algorithm.

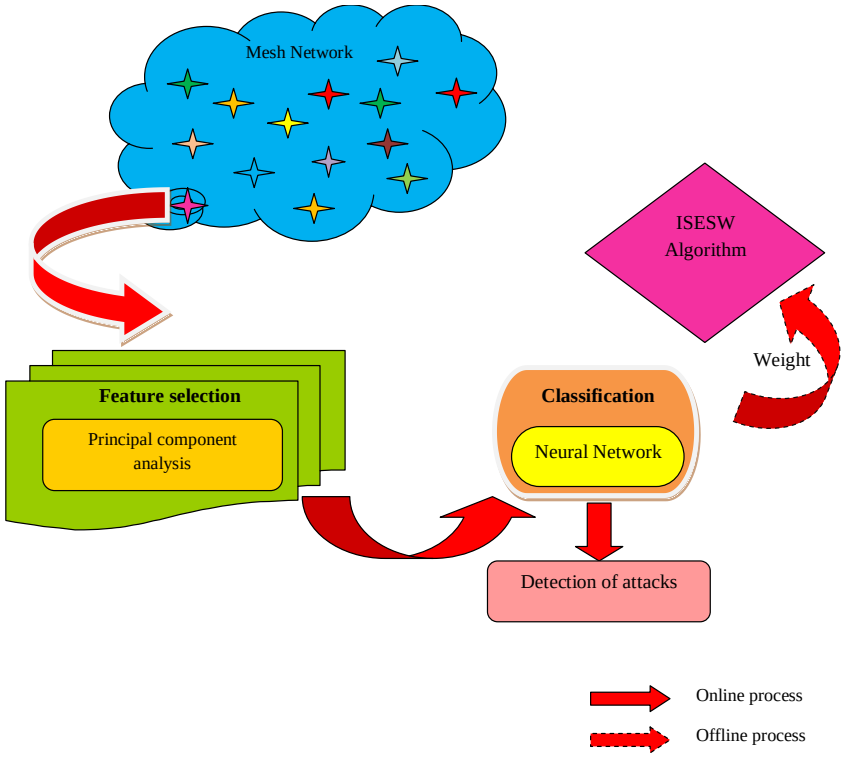


Fig. 1. *Block diagram of Proposed IDS Framework*

4. PCA Based Feature Selection and Optimized NN based Classification

In the presented work, PCA framework is exploited for selecting the informative features present in each category of attacks. In fact, PCA [6] is one among the well-known dimensionality reduction techniques, which minimizes the size of the data sets without any changes in the original variability of the data. The numerical configuration of PCA is given below.

(a)Mean: It is "the average of the values of the variables throughout the distribution". It is also called as the central tendency. Eq. (1) specifies the mean value for the random variable in which $D_k = D_1, D_2, \cdots D_l$ represents the random variables and k indicates the size for the random variables for l count of samples.

$$\text{Mean}(\overline{D}) = \frac{1}{l}\sum_{k=1}^{l} D_k \tag{1}$$

(b) SD: It is "used to determine the degree of scatter". The average distance between the mean and the point at which the data is set is available are evaluated and they are squared with aspire of calculating the spreading of data. Moreover, Eq. (2) manifests the mathematical equation for SD in which the mean is denoted as $\overline{D}$

$$\text{SD} = \sqrt{\frac{1}{l}\sum_{k=1}^{l}\left(D_k - \overline{D}\right)^2} \tag{2}$$

(c) Covariance: The covariance is calculated between two dimensions. This measurement also helps in determining the amount of the variations in dimension from the mean. The mathematical equation for covariance is portrayed in Eq. (3).

$$\text{Cov}(D,H) = \frac{\sum_{k=1}^{l}\left(H_k - \overline{D}\right)\left(H_k - \overline{H}\right)}{l} \tag{3}$$

(d) Eigen values of a matrix: A matrix is rectangular array of numbers, symbols, or expressions and each of the individual items enclosed within the rectangular array of matrixis referred as elements. Moreover, the term B is a $_{l\times l}$ matrix and the mathematical equation corresponding to the eigen value of B is represented in Eq. (4). The scalar parameter in Eq. (4) is indicated as λ.

$$[B][D] = \lambda[D] \tag{4}$$

The features selected by PCA framework are referred as fe, which are then provided as input to NN for classification purpose.

4.1 Optimized Neural Network

The selected features denoted by fe are subjected to NN for classification. NN [8] considers the features fe_{nu} as input specified by Eq. (5), where *nu* signifies the total count of features.

$$fe = \{fe_1, fe_2, ...fe_{nu}\} \tag{5}$$

The model includes input, output, and hidden layers. The output of the hidden layer $e^{(H)}$ is defined as in Eq. (6), where F refers to the "activation function", $\hat{i}$ and j refers to the neurons of hidden and input layers correspondingly, $W_{(B\hat{i})}^{(H)}$ denotes bias weight to $\hat{i}^{th}$ hidden neuron, $n_{\hat{i}}$ symbolizes count of input neurons and $W_{(j\hat{i})}^{(H)}$ denotes the weight from j^{th} input neuron to $\hat{i}^{th}$ hidden neuron. The output of the network $\hat{G}_{\hat{o}}$ is determined as in Eq. (7), where $\hat{o}$ refers to the output neurons, n_h indicates the number of hidden neurons $W_{(B\hat{o})}^{(G)}$ denotes output bias weight to the $\hat{o}^{th}$ output layer, and $W_{(\hat{i}\hat{o})}^{(G)}$ specifies the weight from $\hat{i}^{th}$ hidden layer to $\hat{o}^{th}$ output layer. Consequently, the error amongst the predicted and actual values is computed as per Eq. (8) that should be reduced. In Eq. (8), n_G symbolizes the output neuron count, $G_{\hat{o}}$ and $\hat{G}_{\hat{o}}$ refers to the actual and predicted output respectively.

$$e^{(H)} = F\left(W_{(B\hat{i})}^{(H)} + \sum_{j=1}^{n_i} W_{(j\hat{i})}^{(H)} fe \right) \tag{6}$$

$$\hat{G}_{\hat{o}} = F\left(W_{(B\hat{o})}^{(G)} + \sum_{i=1}^{n_h} W_{(\hat{i}\hat{o})}^{(G)} e^{(H)} \right) \tag{7}$$

$$Er^* = \underset{\left\{W_{(B\hat{i})}^{(H)}, W_{(j\hat{i})}^{(H)}, W_{(B\hat{o})}^{(G)}, W_{(\hat{i}\hat{o})}^{(G)}\right\}}{\arg\min} \sum_{=1}^{n_G} \left| G_{\hat{o}} - \hat{G}_{\hat{o}} \right| \tag{8}$$

As mentioned above, the training of NN model is carried out using a new ISESW algorithm via optimizing the weights $W = W_{(B\hat{i})}^{(H)}, W_{(j\hat{i})}^{(H)}$, $W_{(B\hat{o})}^{(G)}$ and $W_{(\hat{i}\hat{o})}^{(G)}$. Thus, the category of attack is attained as output. The objective function OF of the presented work is defined in Eq. (9)

$$OF = \text{Min}(Er^*) \tag{9}$$

4.2 ISESW Algorithm

For improving the performance of existing WOA [7], it is planned to make some improvements in the algorithm. Self-improvement is proven to be promising in traditional optimization algorithms [9] [10] [11] [12] [13]. The mathematical modelling of proposed model is briefly explained here.

(i) Encircling Prey: The humpback whales have the capability to identify the locality of prey and encircle them. The encircling activities of humpback whales are given in Eq. (10) and Eq. (11), where $\vec{A}$ and $\vec{U}$ are the coefficient vectors and current iteration is represented as t.

$$\vec{Y} = \left| \vec{U}.\vec{R}_p(t) - \vec{R}(t) \right| \tag{10}$$

$$\vec{R}(t+1) = \vec{R}_p(t) - \vec{A}.\vec{Y} \tag{11}$$

In addition, $\vec{R}$ is the position vector and $\vec{R}_p$ is the best position acquired so far. Moreover, $\vec{A}$ and $\vec{U}$ are calculated by Eq. (12) and Eq. (13). In Eq. (12), the component $\vec{a}$ is lessened from 2 to 0 for varied iterations. The random vectors ra_1 and ra_2 resides lies among [0, 1].

$$\vec{A} = 2\hat{a}.ra_1 - \vec{a} \tag{12}$$

$$\vec{U} = 2ra_2 \tag{13}$$

(ii) Exploitation Phase:

This phase is modelled based on the "Shrinking encircling mechanism and Spiral updating position".

(a)"Shrinking encircling mechanism": It is accomplished by lessening the $\vec{a}$ value in Eq. (12).

(b) Spiral update Evaluation: A spiral formula is formed among the whale position and prey as represented in Eq. (14), in which $\vec{Y}$ indicates the distance of i^{th} whale to prey and b is a variable that denotes logarithmic spiral shape and l is an arbitrary integer that lies between $[-1,1]$. The arithmetical formula for $\vec{Y}$ is given in Eq. (15).

$$R(t+1) = \vec{Y}' e^{bl}.\text{Cos}(2\pi l) + \vec{R}_p(t) \quad (14)$$

$$\vec{Y}' = \left|\vec{R}_p(t) - \vec{R}(t)\right| \quad (15)$$

During optimization, the position of whales is shown numerically in Eq. (16), in which ϕ is a random integer in the range [0, 1]. Traditionally, the random parameter p is chosen in a random manner. However, in the adopted model, p is selected on the basis of Eq. (17), in which df is computed as per Eq. (18). In Eq. (18), $f(t-1)$ points out the fitness of prior iteration and $f(t)$ denotes the fitness of present iteration.

$$R(t+1) = \begin{cases} \vec{R}_p(t) - \vec{A}.\vec{Y} & \text{if} \quad \phi < 0.5 \\ \vec{Y}'.e^{bl}.\text{Cos}(2\pi l) + \vec{R}_p(t) & \text{if} \quad \phi \geq 0.5 \end{cases} \quad (16)$$

$$p = df \times \text{rand} \quad (17)$$

$$df = f(t-1) - f(t) \quad (18)$$

Exploration phase: This is evaluated as shown in Eq. (19) and Eq. (20). The arbitrary position vector elected from the present population is indicated by $X_{(rand)}$.

$$\vec{Y} = \left|\vec{U}\vec{R}_{(rand)} - \vec{R}\right| \quad (19)$$

$$\vec{R}(t+1) = \vec{X}_{(rand)} - \vec{A}.\vec{Y} \quad (20)$$

5. Results and discussion

5.1 Simulation Procedure

The developed IDS model in WMN using ISESW-NN was implemented in Matlab and the resultants were observed. The analysis was carried out using ADFA Linux dataset. The proposed ISESW model was compared with conventional classifiers such as SVM [14] and CNN [15] and the outcomes were attained in terms of accuracy, precision, FNR, FPR and specificity. Here analysis was carried out for message size of 512 bits, 1024 bits and moreover, analysis was done by combining both the sizes.

5.2 Overall Performance Analysis

The performance of adopted ISESW-NN model over the conventional models with respect to positive and negative measures for is represented in Fig. 2. On noticing the outcomes, the presented ISESW model has accomplished better accuracy when compared over the existing models. Here, from Fig. 2(a), the presented method has achieved a higher accuracy of 0.9985, which is 0.91% better than existing SVM and CNN models. Also, the presented method has achieved a minimal FPR of 0.009, which is 78.05% improved than existing SVM and CNN models. This shows the enhancement of the presented ISESW-NN framework over the existing models.

5.3 Performance Evaluation by Varying Data Size

The resultants acquired by ISESW-NN model in terms of positive and negative measures for 512 bit size, 1024 bit size and combined bit sizes are shown in Table II, Table III and Table IV respectively. In this work, analysis is carried out for varied types of attacks such as Data flooding, Jamming, Black hole, Hello flooding and Grey hole. From the Tables, it is observed that the proposed model attains better accuracy, precision, specificity and sensitivity for all types of attacks. In addition, on observing the negative measures like FNR and FPR, the adopted scheme has revealed minimal values, thus guarantying the enhanced attack detection rate. Thus, the betterment of the developed is proved from the results.

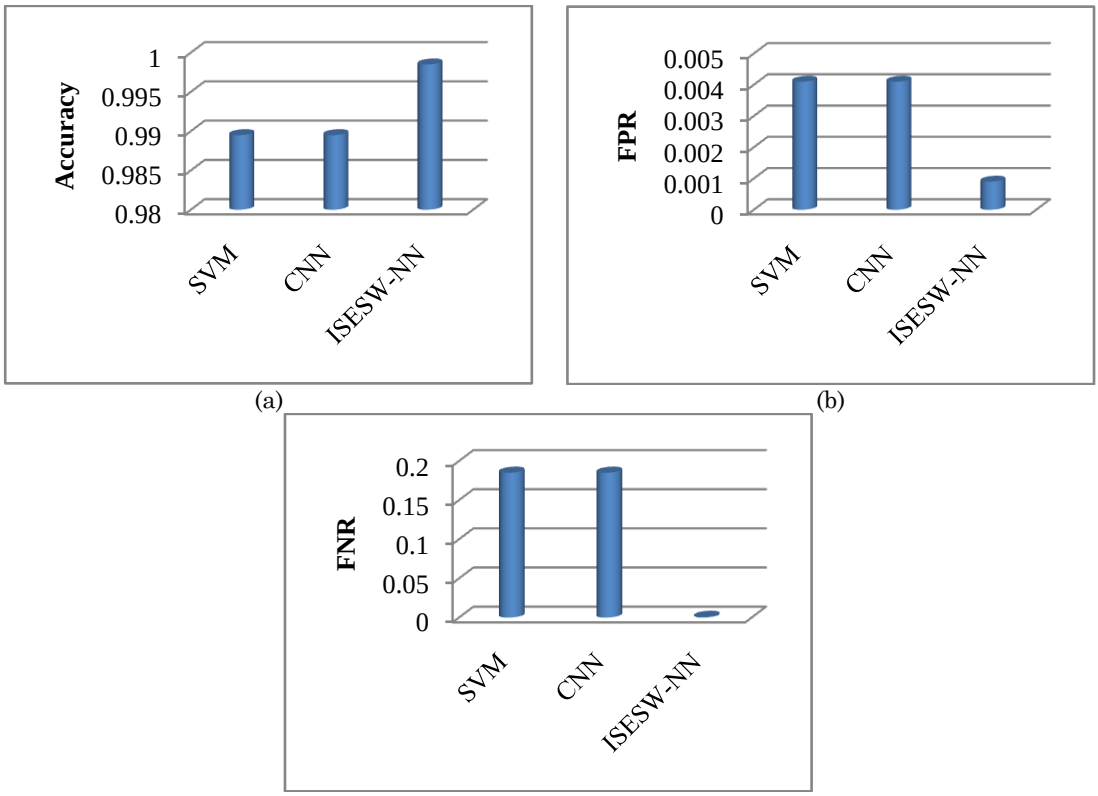


Fig. 2. *Performance evaluation of the proposed work over the existing work with respect to (a) Accuracy (b) FPR and (c) FNR*

Table 1: *Experimental Analysis of proposed model over conventional models on 512 bit dataset*

Attacks	Data size	Precision	Accuracy	Specificity	Sensitivity	FNR	FPR
Normal	99	0.9574	0.9589	0.9389	0.9729	0.027	0.061
Data flooding	14	0.9565	0.9968	0.9966	1	0	0.003
Jamming	26	0.8542	0.9494	0.9734	0.8723	0.127	0.027
Black hole	11	0.9375	0.9968	0.9967	1	0	0.003
Hello flooding	15	0.9091	0.9905	0.9932	0.9524	0.05	0.007
Grey hole	33	1	1	1	1	0	0

Table 2: *Experimental Analysis of proposed model over conventional models on 1024 bit dataset*

Attacks	Data size	Precision	Accuracy	Specificity	Sensitivity	FNR	FPR
Normal	188	0.9492	0.9430	0.9688	0.9032	0.097	0.031
Data flooding	23	0.9286	0.9684	0.9929	0.7647	0.24	0.007
Jamming	48	0.6923	0.9051	0.9398	0.7200	0.28	0.06
Black hole	16	1	0.9557	1	0.6111	0.39	0
Hello flooding	22	0.6667	0.9430	0.9653	0.7143	0.29	0.034
Grey hole	19	1	0.9241	1	0.7333	0.29	0

Table 3: *Experimental Analysis of proposed model with respect to different type of attacks on combined dataset*

Attacks	Data size	Precision	Accuracy	Specificity	Sensitivity	FNR	FPR
Normal	247	0.9551	0.9281	0.9491	0.9105	0.089	0.051
Data flooding	74	0.9459	0.9937	0.9954	0.9722	0.028	0.005
Jamming	37	0.7867	0.9238	0.9594	0.7468	0.25	0.041
Black hole	37	0.9629	0.9852	0.9977	0.8125	0.19	0.002
Hello flooding	27	0.8947	0.9471	0.9904	0.6182	0.38	0.009
Grey hole	52	0.9608	0.9640	0.9951	0.7656	0.23	0.004

5.4 Analysis on Training and Testing Time

Table IV demonstrates the training as well as testing time attained by the presented ISESW-NN model for varied types of attacks such as Data flooding, Jamming, Black hole, Hello flooding and Grey hole. On

observing the outcomes, it could be known that the implemented model consumes minimal testing time for all types of attacks.

Table 4: *Training Time and testing time Analysis of proposed model with respect to different attacks*

Attack type	Testing time	Training time
Normal	0.0022	0.6084
Jamming	0.0025	0.5618
Data flooding	0.0025	0.5928
Hello flooding	0.0026	0.4836
Black hole	0.0022	0.4836
Worm hole	0.0019	0.5616

6. Conclusion

This paper had developed a technique for IDS in WMN systems that included two stages such as, feature Selection and classification. At first, the informative features from the given data were chosen via PCA model. The selected informative features were classified using NN, which detects the presence of attacks. Moreover, to attain a precise detection, the weights of NN were fine-tuned using the new ISESW algorithm. Finally, a precise analysis was made for validating the enhancement of presented model over traditional schemes in terms of varied measures. Particularly, a higher accuracy of 0.9985 was achieved by the presented method, which was 0.91% better than existing SVM and CNN models. Also, the presented method has achieved a minimal FPR of 0.009, which was 78.05% improved than existing SVM and CNN models. Thus, the superiority of the developed model has been verified successfully.

Compliance with Ethical Standards

Conflicts of interest: Authors declared that they have no conflict of interest.

Human participants: The conducted research follows the ethical standards and the authors ensured that they have not conducted any studies with human participants or animals.

References

[1] Cheng-Ru Wang, Rong-Fang Xu, Shie-Jue Lee, Chie-Hong Lee, "Network intrusion detection using equality constrained-optimization-based extreme learning machines" Knowledge-Based Systems, vol. 147, pp. 68-801, May 2018.

[2] Muhammet Baykara, Resul Das, “A novel honeypot based security approach for real-time intrusion detection and prevention systems”, Journal of Information Security and Applications, vol. 41, pp. 103-116, August 2018.

[3] Tamer Aldwairi, Dilina Perera, Mark A. Novotny, “An evaluation of the performance of Restricted Boltzmann Machines as a model for anomaly network intrusion detection”, Computer Networks, vol. 144, pp. 111-119, 24 October 2018.

[4] Hongchun Qu, Zeliang Qiu, Xiaoming Tang, Min Xiang, Ping Wang, “Incorporating unsupervised learning into intrusion detection for wireless sensor networks with structural co-evolvability”, Applied Soft Computing, vol. 71, pp. 939-951, October 2018.

[5] Tarfa Hamed, Rozita Dara, Stefan C. Kremer, “Network intrusion detection system based on recursive feature addition and bigram technique”, Computers & Security, vol. 73, pp. 137-155, March 2018.

[6] Pravendra Kumar, Sanjeev Kumar Singh Yadav,"Multi-objective optimization of electrical discharge drilling (EDD) process using PCA based grey relational analysis",Materials Today: Proceedings, vol.26,2020.

[7] Seyedali Mirjalili,Andrew Lewisa,"The Whale Optimization Algorithm",Advances in Engineering Software,vol.95,pp.51-67,May 2016.

[8] Yogeswaran Mohan, Sia Seng Chee, Donica Kan Pei Xin and Lee Poh Foong, "Artificial Neural Network for Classification of Depressive and Normal in EEG", 2016 IEEE EMBS Conference on Biomedical Engineering and Sciences (IECBES), 2016.

[9] B. R. Rajakumar, "Impact of Static and Adaptive Mutation Techniques on Genetic Algorithm", International Journal of Hybrid Intelligent Systems, vol. 10, no. 1, pp.11-22, 2013.

[10] B. R. Rajakumar, "Static and Adaptive Mutation Techniques for Genetic algorithm: A Systematic Comparative Analysis", International Journal of Computational Science and Engineering, Vol. 8, No. 2, pages: 180-193, 2013.

[11] S. M. Swamy, B. R. Rajakumar and I. R. Valarmathi, “Design of Hybrid Wind and Photovoltaic Power System using Opposition-based Genetic Algorithm with Cauchy Mutation”, IET, Chennai, India, Dec. 2013, DOI: 10.1049/ic.2013.0361

[12] Aloysius George and B. R. Rajakumar, "APOGA: An Adaptive Population Pool Size based Genetic Algorithm", AASRI Procedia - 2013 AASRI Conference on Intelligent Systems and Control (ISC 2013), Vol. 4, pages: 288-296, 2013.
[13] B. R. Rajakumar and Aloysius George, "A New Adaptive Mutation Technique for Genetic Algorithm", In proceedings of IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), pages: 1-7, December 18-20, Coimbatore, India, 2012, DOI: 10.1109/ICCIC.2012.6510293.
[14] Erfan A. Shams, Ahmet Rizaner, Ali Hakan Ulusoy, "Trust aware support vector machine intrusion detection and prevention system in vehicular ad hoc networks", Computers & Security, vol. 78, pp. 245-254, September 2018.
[15] Y. LeCun, K. Kavukvuoglu, and C. Farabet, "Convolutional networks and applications in vision", In Circuits and Systems, International Symposium on, pages 253–256, 2010.