Fixed Neuro Fuzzy Classification Technique For Intrusion Detection Systems

Dr A M Viswa Bharathy, Dr R Bhavani

Abstract: Over the years, design and development of intrusion detection systems have gone to new heights. A lot of algorithms and techniques have been developed and tested for the better security of our internetwork systems. Stand-alone efficient approaches, hybrid techniques and frameworks are given by many researchers and scientists towards the enhancement of intrusion detection andprevention systems. In this paper, we study various intrusion detection approaches with their pros and cons and conclude statistically with the proposed Fixed Neuro Fuzzy Classification (FNFC), a new technique for intrusion detection algorithm.

1 Introduction

In this section the various hybrid approaches in the literature are given in detail. As day by day the threats increase the usage of single technique to counter the intruders is not suffice. So the researchers found an intelligible way of thwarting the attacks through a more prominent approach. As a result, was born the process of combining two techniques as one to deal with evolutionary attacks. This is termed as the Hybrid Network Intrusion Detection System (H-NIDS). The hybrid approach can be divided into three classes namely Cascading Supervised Algorithms (CSA), Integrating Supervised and Unsupervised Algorithms (ISUA) and Fusing Learning Algorithms with Optimization Techniques (FLAOT). By the term hybrid it means either combination of Network-Host IDS (NH-IDS), Anomaly-Signature IDS (AS-IDS) or combination of two different Intrusion Detection Techniques (IDT). This work proposes to develop a Hybrid NIDS based on IDT.

1.1 General Framework

The common framework for the hybrid NIDS is given below in the figure 1.1 and the same is explained below.

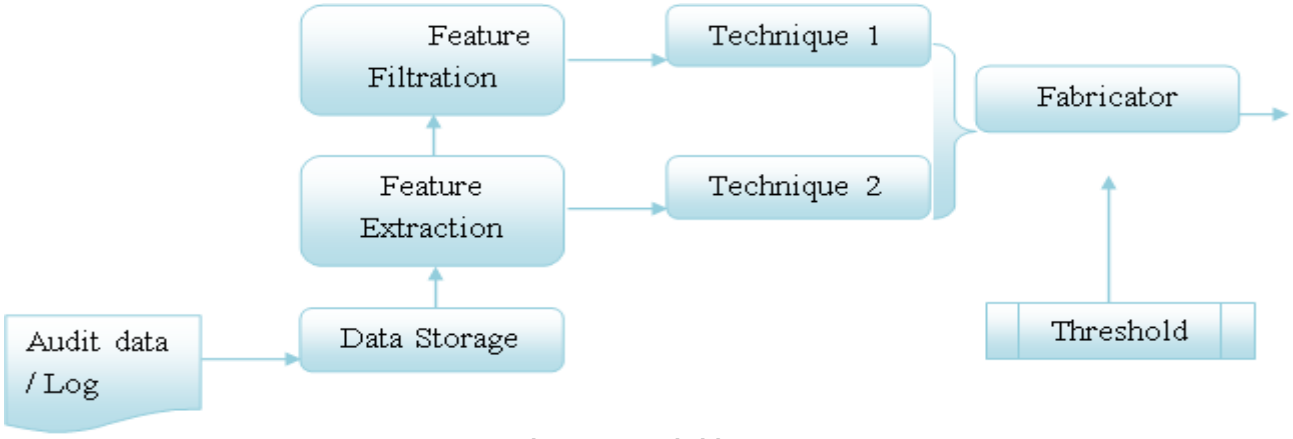


Figure 1.1 Hybrid NIDS

1.1.1 Audit Data

This log of data denotes the whole organised data set used for testing the system. Organised data is used so that the features are well selected and pruned. Usually the KDD Cup 99 data set is used for experimenting of intrusion detector.

1.1.2 Data Storage

The data fed into the system is initially stored in the local database prior to processing it. This is done to safe guard the data set in its original form before processing or tuning the data set.

1.1.3 Feature Extraction

The selected data set has many features. It is upto the designer to extract as many features as required by the system. The careful extraction of features plays a vital role in measuring the performance of the intrusion detector. In this phase as many features are extracted and this could be filtered in the next phase. The features are extracted enough to classify the data set into Normal, Probe, DoS, U2R and R2L. These features are used to calculate the similarity measure between data points.

1.1.4 Feature Filtration

In this stage, the features extracted during the previous stage undergo a careful selection and filtration process. The exact features needed for the system is filtered in this phase. The irrelevant and inappropriate features are removed from the template. Not only has the removal of unnecessary parameters help in reducing the computational

- *Dr A M ViswaBharathy, Assoc.Professor/CSE Veltech Multitech Dr Rangarajan Dr Sakunthala Engineering College, Tamil Nadu, India.*
- *Dr R Bhavani, Assoc.Professor/CSE Veltech Multitech Dr Rangarajan Dr Sakunthala Engineering College, Tamil Nadu, India.*

time and cost, but also aid in building a processed summarized set of attribute data set.

1.1.5 Technique 1 & 2

This could usually be either a supervised or unsupervised learning algorithms. In most cases it could be a classification or clustering technique. But the recent improvement has shown the use of optimization algorithms either in technique 1 or 2. The optimization technique is used to fine tune the parameters so that the classification accuracy is high.

1.1.6 Fabricator

In this phase the results of both the techniques are combined and a decision is made to utilise the best of classified data sets. This decision is influenced by the threshold value. This value is concluded based on the population of dataset and the technique used to classify the dataset. The output of the fabricator is the alarm to alert the system to take necessary counter action if it is an attack. All Hybrid NIDS (H-NIDS) approach follow the same framework described above by amending few changes to it.

1.2 Cascading Supervised Algorithms

Farid et al (2010) proposed a combination of Naive Bayes and Decision Tree (NB-DT). It had considerably low False Positive Rates (FPRs) for various network attacks. The disadvantages include higher FPRs for User-to-Root (U2R) and Remote-to-Local (R2L) data types. The method had convincing Detection Rates (DRs). Peddabachigari et al (2007) came up with the combination of Decision Tree and Support Vector Machine (DT-SVM). The dataset is processed by the DT for fine tuning the parameters and then passed to SVM for better classification. The method was tested on KDD Cup 99 data set and showed better results in terms of accuracy and DR compared to SVM.

1.3 Integrating Supervised and Unsupervised Algorithms

In the literature so far many hybrid approaches have been proposed by combining supervised and unsupervised algorithms. By this hybrid method the efficiency of supervised algorithms has been increased and the accuracy of unsupervised techniques has been improved. A combination of K-Means and ID-3 was used in Address Resolution Protocol (ARP) for classification of anomalous activities and an accuracy of 98% was achieved (Yasami&Mozaffari 2010). Similarly a combination of artificial neural networks and support vector machine was tested for network intrusion detection. The approach was experimented with KDD Cup 99 data set and achieved high classification rate especially with U2R and R2L attacks (Tang & Cao 2009). Agarwal& Mittal (2012) surveyed a number of data mining techniques for anomaly network intrusion detection. The literature survey concluded with a fact that combining one or more anomaly detection techniques yielded good results. The experimental results further proved that SVM when integrated with other prominent technique showed better results than SVM alone.

2 Literature Review

Ravale et al (2015) experimented their concept of hybrid anomaly detector built using K-means and Radial Basis-Kernel (RB-K) function. This RBF is a part of Support Vector Machine (SVM). The authors focussed on reducing the number of attributes associated with the data points. In this approach first the data points were clustered using K-Means based on their similarity and next the clustered groups were classified into various data points using the RBF kernel function of the SVM. The experiment used KDD Cup 99 data set along with its 41 attributes for evaluating the performance of the system. The results achieved better detection rate and accuracy when compared to the other methods. The paper did not measure the FAR of the proposed technique. Ghanem et al (2015) proposed a hybrid anomaly detector using Multi-Start Metaheuristic (MSM) technique with Genetic Algorithm. They have used negative selection based MSM for generation of anomaly detectors. The paper used K-Means for selecting a set of appropriate data points which reduces the time and space complexity of the system. After this using Genetic Algorithm the data points were optimized and unwanted detectors were reduced using the rule sets. The system was tested using NSL-KDD which is a modified version of regular KDD Cup 99 data set. The proposed method was compared with Bayes Network (BN), Bayesian Logistic Regression (BLR), Naive Bayes (NB), Multilayer Feed-Back Neural Network (MFBNN), Radial Basis Function Network (RBFN) and Decision Trees (J48). The parameters used to measure the performance of the system were computational time, accuracy and False Positive Rate (FPR). The method proposed by Ghanem et al showed better results than the existing methods. Sangeetha et al (2015) proposed an efficient anomaly detection technique designed using Genetic Algorithm and Bayesian Classifier (GA-BC). The authors have used GA for its probabilistic nature. A rule set generator was used and every time a new intrusion gets detected the rule set updates itself automatically. Each candidate in the rule set is tested for its fitness using a function. The system reported better detection rates and accuracy with acceptable false alarm rates. The running time of the system was bit high which was negotiable, compared to other techniques. A Hybrid Intrusion Detection System (H-IDS) with a combination of Multiple Criteria Linear Programming (MCLP) and Particle swarm optimization (PSO) (Bamakan et al 2015) was tested using the KDD Cup 99 data set. The MCLP was used to classify the data points into two classes namely normal and attack. The parameters and the data points were optimised using the PSO for fine tuning the system. The best tuned MCLP by PSO is applied to the data set. The method proved to be better in terms of DR, FAR and accuracy. The drawback of the system was it could not identify multiple data points. Ikram&Cherukuri (2016) proposed a NIDS model of Chi-Square for feature selection and Multi-Class SVM for five type classification of data set (CS-MCSVM). The authors have used one against all type of SVM for multi-classifying the data points based on their attributes. The proposed model by the authors had two levels. In the first level the Chi-Square separates high and low rank attributes and eliminates the lower ones and uses the optimal ranked attributes alone for the feature selection. In the second level, the data were divided into validation, training and test

data set. The attributes that pass the cross validation with high ranks were considered for the parameter selection. The system used 31 features of the available 41 features of the NSL-KDD Cup 99 data set. The experiments were done on MATLAB R2012A with libSVM package, as it supports SVM classification. The above model used rank based Chi-Square technique along with RBF kernel SVM. The method was tested and evaluated for DR, accuracy and FAR. The technique had convincing results in terms of training and testing time with better DR and accuracy. The lowest accuracy was recorded for the U2R data point. The work triggered the interestes in all developers with yet another unique technique called ranking based Chi-Square. Dhanachandra et al (2015) came up with their idea of using K-Means and Subtractive Clustering (SuC) technique for image segmentation. Before applying these techniques to improve the overall quality of the image partial stretching was used. This enhanced the vital as well as minor attributes of the image to a substantiable level. In this work instead of centroids being generated by the K-Means, it was done by the Subtarctive Clustering method. This Subtractive Clustering technique generates the centroids based on the potential value of the data points. These SC centroids were used by the K-Means for dividing the image into various partitions. The image partitions were fed into median filter to eliminate any redundant featuires and unwanted regions of the image. The authors used Peak to Signal Noise Ratio (PSNR) for evauating the output quality of the image and the results were better when compared to the other techniques. Cepheli et al (2016) proposed an architecture for Hybrid Intrusion Detection System (H-IDS). The framework by the authors consisted of six integrated components which work together for detecting the anomalous behaviour of the network. The H-IDS worked by combining the two techniques Expectation-Maximization Clustering (E-MC) and Information Distance Metrics (InfDM). Gaussian distributions were used in E-MC for effectively extracting the features of the data set, which would serve for better results. The authors used Snort tool to test and metrics used to test were TPR and FPR. The system was tested for both anomaly and signature based attack. DR and FAR was low for both the data sets. Soleimani&Kannan (2015) proposed a Hybrid-PSO (H-PSO) with GA for design of network in closed-loop supply chain. The authors used the PSO to fine tune the parameters of GA. The method was tested using the tool CPLEX and MATLAB. They tested with the case study of a furniture manufacturing company and the results were better compared to GA and PSO alone. Ahmad (2015) proposed a statistical method for feature selection. They used Principal Component Analysis (PCA) with PSO for data analysis and feature selection. As raw data sets are used for testing, FARs are increasing, so they used PCA for transforming raw features into primary features. False alarm rates were reduced drastically and detection rates increased linearly. Idris et al (2015) proposed a Combined Negative Selection Algorithm-PSO for email spam detection (CNSA-PSO). The features of the data sets were selected using threshold and distance value. Local Outlier Factor-LOF was used as a fitness function to calculate the reachable distance between non-spam space and the particle's LOF within the neighbourhood to get best features during detector generation. The experimental results and analysis showed that CNSA-PSO performed better than NSO model. De et al (2016) proposed a Particle Swarm Optimization-Composite Particle Algorithm (PSO-CPA) for ship routing and scheduling. They used Mixed Integer Non-Linear Programming (MINLP) to deal with Multiple Time Horizons (MTH), sustainability, and varying demand-supply at various ports. The Composite Particle Swarm Optimization (CPSO) was better than PSO and GA alone. The constraints considered were carbon emission, fuel cost and fuel consumption. A Combinatorial Particle Swarm Optimization (Combi-PSO) to solve Blocking Flowshop Scheduling Problem (Eddaly et al 2016) was proposed and tested. The objective of the authors was to minimize the makespan criterion using Hybrid Combinatorial Particle Swarm Optimization (HCPSO). They used Iterated Local Search Algorithm (ILSA) based on probabilistic perturbation. ILSA was sequentially and consistently applied to the PSO for improving the scope of solution. The computational results showed that the approach improved 76 among 120 best known existing techniques. Moustafa et al (2016) proposed a Two-Layer Particle Swarm Optimization for Protein Sequence Alignment (PSA). They focussed on the Multiple Sequence Alignment (MSA) issue. TL-PSO was used to align each fragment. The method succesfully dealt with unconstrained optimization problems and increased the diversity of particles. The method was tested on some Balibase benchmarks of different lengths. The numerical results were compared with CLUSTAL Omega, CLUSTAL W2, TCOFFEE, KALIGN, and DIALIGNPFAM. It showed better results in alignment compared to regular PSO. Bamakan et al (2016) proposed an Intrusion Detection Framework (IDF) using MCLP-SVM and Time-Varying Chaos Particle Swarm Optimization (TV-CPSO). The features used in MCLP-SVM for parameter and feature selection were time varying inertia weight and acceleration co-efficient. An improved MCLP called Penalized-MCLP (P-MCLP) was used to support unbalanced datasets. A Weighted Objective Function (WOF) is used to maximize the detection rate and minimize the False Alarm Rate. NSL-KDD data set was used for the experiment and it showed better results. A hybrid modified K-means with C4.5 classification in the multiagent system was proposed for splitting the large dataset into clusters (Al-Yaseen et al 2015). The dataset used for evaluating the system was the KDD Cup 1999 dataset. The detection accuracy was improved using this system but the processing time of IDS was reduced upto 70%. Eesa et al (2015) proposed a new alternative approach for feature extraction using Cuttle Fish Optimization (CFA) and classification using the Decision Tree (DT). The experimental results proved that CFA is efficient in extracting best features and eliminating redundant features. Basically this CFA works on the skin colour changing technique of the cuttle fish using light reflection principle. They stated that this fish has three layers namely Chromatophores, Iridophores and Leucophores. The subset combinations of these layers are responsible for the light reflection and skin colour change. The optimized data set by CFA were fed to DT which then classified smoothly with higher DR, FAR and accuraccy.

Table 2.1 Comparison of all Techniques

S.No	Proposed by	Methodology	Pros	Cons
1.	Ravale et al (2015)	K-means and Radial Basis-Kernel (RB-K)	➢ Redundancy reduced ➢ All 41 features used	➢ FAR not evaluatted
2.	Ghanem et al (2015)	Multi-Start Metaheuristic with Genetic Algorithm (MSM-GA)	➢ Irrelevant detectors reduced using rule sets	➢ Usage of extra rule sets in GA
3.	Sangeetha et al (2015)	Genetic Algorithm and Bayesian Classifier (GA-BC)	➢ Better DR and FAR	➢ Separat rule set used and running time is high
4.	Bamakan et al (2015)	Multiple Criteria Linear Programming-Particle swarm optimization (MCLP-PSO)	➢ Better FAR and accuracy	➢ Only dual classification is done
5.	Ikram&Cherukuri (2016)	Chi-Square-Multi-Class Support Vector Machine (CS-MCSVM).	➢ Separation of low and high rank attributes ➢ Good overall DR and FAR	➢ Only 31 features were used out of 41 ➢ Low accuracy for U2R
6.	Dhanachandra et al (2015)	K-Means and Subtractive Clustering (KM-SC)	➢ Partial stretching used to improve the quality of the image	➢ Dual clustering used for calculating centroid ➢ Too many image partitions
7.	Cepheli et al (2016)	Framework based on Expectation-Maximization Clustering and Information Distance Metrics (EMC-IDM)	➢ Best features were extracted using E-MC ➢ Tested for both anomaly and signature based attacks	➢ DR and FAR was very low
8.	Soleimani&Kannan (2015)	Hybrid PSO with GA	➢ Showed better results compared to normal PSO and GA	➢ Tested with a single case study ➢ Tested for closed loop alone
9.	Ahmad (2015)	PSO-PCA	➢ PCA used to transform data features	➢ DR increased and FAR decreased
10.	Idris et al (2015)	Combined Negative Selection Algorithm-PSO (CNSA-PSO)	➢ LOF was used as a fitness function to calculate the reachable distance between	➢ Performed better than PSO
11.	De et al (2016)	Particle Swarm Optimization-Composite Particle Algorithm (PSO-CPA)	➢ Used Mixed Integer Non-Linear Programming (MINLP) to deal with Multiple Time Horizons (MTH), sustainability, and demand-supply. ➢ Better than PSO and GA	➢ Consideredonly carbon emission, fuel cost and fuel consumption. ➢ Too many points to achieve global and local optima
12.	Eddaly et al (2016)	Hybrid Combinatorial Particle Swarm Optimization (HCPSO)	➢ ILSA based on probabilistic perturbation was used	➢ Computational time is very high
13.	Moustafa et al (2016)	Two-Layer Particle Swarm Optimization (TL-PSO)	➢ Improved and diversity and unconstrained optimization	➢ Better than regular PSO
14.	Bamakan et al (2016)	Multiple-Criteria Linear Programming- Support Vector Machine (MCLP-SVM) and Time-Varying Chaos Particle Swarm Optimization (TV-CPSO).	➢ Supports unbalanced data sets ➢ A Weighted Objective Function (WOF) used	➢ Time varying inertia weight and acceleration co-efficient not reliable
15.	Al-Yaseen et al (2015)	K-Means with C 4.5	➢ DR and accuracy improved ➢ Usage of multi agent system for centroidsin K-Means	➢ The computation time was only reduced by 70% ➢ Multi classification was not done
16.	Eesa et al (2015)	Cuttle Fish Optimization-Decision Tree (CFA-DT)	➢ CFA extracts best features and eliminates unwanted features	➢ Training time is bit high

3 Fixed Neuro Fuzzy Classification Technique

This FNFC is a selectively modified algorithm of existing more robust ANFIS classifier, which itself is a hybrid combo of fuzzy logic and neural networks. The FNFC model has 5 layers and the layer 1 and layer 4 parameters are fixed as per the best fit features of the dataset. In ANFIS the layer 1 and 4 would be adaptive.

Consider two nodes x1 and x2 as input and output is y
Each variable has two linguistic terms
M1 and M2 for x1
L1 and L2 for x2
R1 : if x1 is M1 and x2 is L1 then y = f1(x)
R2 : if x1 is M2 and x2 is L2 then y = f2(x)
f1(x) = p1x1 + q1x2 + r1
f2(x) = p2x1 + q2x2 + r2

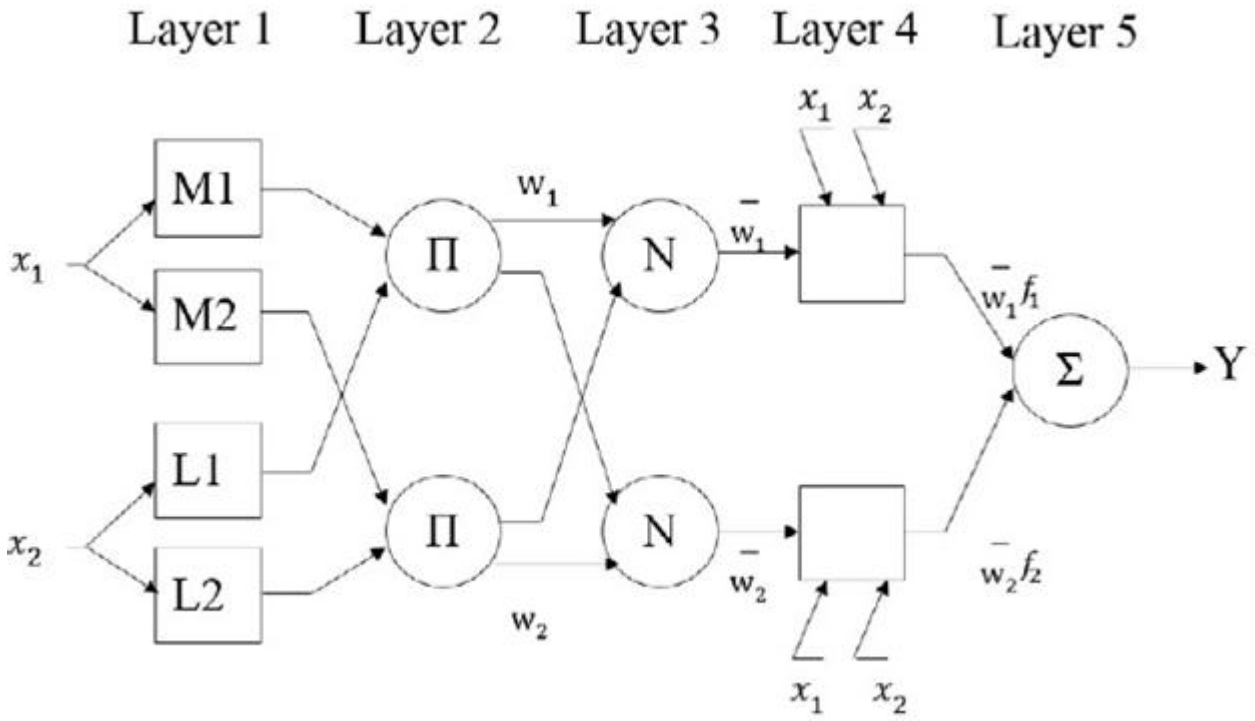


Figure 3.1 FNFC

4 Experimental Setup

The standard KDD Cup 99 data set has been used for the experiment purpose. The FNFC technique classifies the dataset into five types of clusters namely normal, probe, DoS, U2R and R2L. The dataset is classified based on the attributes associated with the lingusitic terms M and L. The features associated with the FNFC are given below in the table. A total of 5500 normal and 6034 attack dataset is chosen by random selection method.

Table 4.1 Attributes selected against each data type

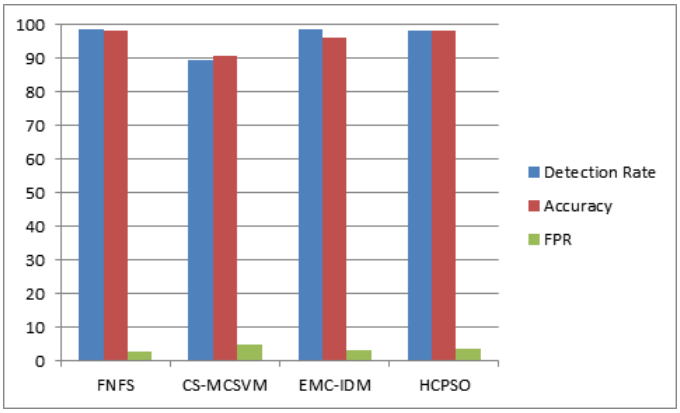
S.No	Attack	Attribute Type
1	Normal	1-41
2	Probe	1-3, 5, 6, 10, 12, 23-41
3	DoS	2-8, 10, 12, 13, 22-41
4	U2R	1-6, 10-14, 16-19, 23-30, 32-41
5	R2L	1-6, 9-19, 22-28, 31-41

5 Experimental Results and Analysis

In this section, the results of the experiment are presented in comparison with the various existing techniques in table 5.1.

Table 5.1 FNFC Comparison

S.No	Method	Detection Rate	Accuracy	FPR
1.	FNFC	0.9873	0.9826	0.02611
2.	CS-MCSVM	0.8952	0.9072	0.04731
3.	EMC-IDM	0.9847	0.9617	0.03242
4.	HCPSO	0.9823	0.9816	0.03612



Conclusion

The various IDS techniques have been compared with their pros and cons and tabulated well. The proposed FNFC is compared with its results and is proved to be performing well.

References

[1] Farid, DM, Harbi, N &Rahman, MZ 2010, 'Combining Naive Bayes and Decision Tree for Adaptive Intrusion Detection', International Journal of Network Security & its Applications, vol. 2, no. 2, pp. 12-25.

[2] Peddabachigari, S, Abraham, A, Grosan, C & Thomas, J 2007, 'Modeling Intrusion Detection System using Hybrid Intelligent Systems', Journal of Network and Computer Applications, vol. 30, no. 1, pp. 114-132.

[3] Yasami, Y &Mozaffari, SP 2010, 'A Novel Unsupervised Classification Approach for Network Anomaly Detection by K-Means Clustering and ID3 Decision Tree Learning Methods', The Journal of Supercomputing, vol. 53, no. 1, pp. 231-245.

[4] Tang, DH & Cao, Z 2009, 'Machine Learning-based Intrusion Detection Algorithms', Journal of Computational Information Systems, vol. 5, no. 6, pp. 1825-1831.

[5] Agarwal, B & Mittal, N 2012, 'Hybrid Approach for Detection of Anomaly Network Traffic using Data Mining Techniques', Procedia Technology, vol. 6, no. 1, pp. 996-1003.

[6] Ravale, U, Marathe, N &Padiya, P 2015, 'Feature Selection Based Hybrid Anomaly Intrusion Detection System Using K Means and RBF Kernel Function', Procedia Computer Science, vol. 45, no. 1, pp. 428 – 435.

[7] Ghanem, TF, Elkilani, WS & Abdul-Kader, HM 2014, 'A Hybrid Approach for Efficient Anomaly Detection using Metaheuristic Methods', Journal of Advanced Research, vol. 6, no. 1, pp. 609-619.

[8] Sangeetha, K, Periasamy, PS &Prakash, S 2015, 'Identification of Network Intrusion with Efficient Genetic Algorithm using Bayesian Classifier', Proceedings of the International Conference on Computer Communication and Informatics, pp. 1-4.

[9] Bamakan, SMH, Amiri, B & Shi, MMY 2015, 'A New Intrusion Detection Approach Using PSO based Multiple Criteria Linear Programming', Procedia Computer Science, vol. 55, no. 1, pp. 231-237.

[10] Ikram, ST &Cherukuri, AK 2016, 'Intrusion Detection Model using Fusion of Chi-Square Feature Selection and Multi Class SVM', Journal of King Saud University‐Computer and Information Sciences (in press).

[11] Dhanachandra, N, Manglem, K &Chanu, YJ 2015, 'Image Segmentation using K-means Clustering Algorithm and Subtractive Clustering Algorithm', Procedia Computer Science, vol. 54, no. 1, pp. 764-771.

[12] Cepheli, O, Buyukcorak, S & Kurt, GK 2016, 'Hybrid Intrusion Detection System for DDoS Attacks', Journal of Electrical and Computer Engineering, vol. 2016, Article ID 1075648.

[13] Ahmad, I 2015, 'Feature Selection Using Particle Swarm Optimization in Intrusion Detection', International Journal of Distributed Sensor Networks, vol. 11, no. 10, A. 806954.

[14] Soleimani, H &Kannan, G 2015, 'A Hybrid Particle Swarm Optimization and Genetic Algorithm for Closed-Loop Supply Chain Network Design in Large-Scale Networks', Applied Mathematical Modelling, vol. 39, no. 14, pp. 3990-4012.

[15] Idris, I, Selamat, A, Nguyen, NT, Omatu, S, Krejcar, O, Kuca, K &Penhaker, M 2015, 'A Combined Negative Selection Algorithm–Particle Swarm Optimization for an Email Spam Detection System', Engineering Applications of Artificial Intelligence, vol. 39, no. 1, pp. 33-44.

[16] De, A, Mamanduru, VKR, Gunasekaran, A, Subramanian, N &Tiwari, MK 2016, 'Composite Particle Algorithm for Sustainable Integrated Dynamic Ship Routing and Scheduling Optimization', Computers & Industrial Engineering, vol. 96, no. 1, pp. 201-215.

[17] Eddaly, M, Jarboui, B &Siarry, P 2016, 'Combinatorial Particle Swarm Optimization for Solving Blocking Flowshop Scheduling Problem', Journal of Computational Design and Engineering, vol. 3, no. 4, pp. 295–311.

[18] Moustafa, N, Elhosseini, M, Taha, TH & Salem, M 2016, 'Fragmented Protein Sequence Alignment using Two-Layer Particle Swarm Optimization (FTLPSO)', Journal of King Saud University-Science, (in press).

[19] Bamakan, SMH, Wang, H, Yingjie, T & Shi, Y 2016, 'An Effective Intrusion Detection Framework based on MCLP/SVM Optimized by Time-Varying Chaos Particle Swarm Optimization', Neurocomputing, vol. 199, no. C, pp. 90-102 .

[20] Al-Yaseen, WL, Othman, ZA &Nazri, MZA 2015, 'Hybrid Modified K-Means with C4.5 for Intrusion Detection Systems in Multiagent Systems', The Scientific World Journal, A. 294761.

[21] Eesa, AS, Orman, Z &Brifcani, AMA 2015, 'A Novel Feature-Selection Approach Based on the Cuttlefish Optimization Algorithm for Intrusion Detection Systems', Expert Systems with Applications, vol. 42, no. 1, pp. 2670-2679.

[22] ViswaBharathy, AM, Basha, AM 2017, 'A Multi-Class Classification MCLP Model with Particle Swarm Optimization for Network Intrusion Detection', Sadhana: Academy Proceedings in Engineering Science, vol. 42, no. 5, pp. 631-640.

[23] ViswaBharathy, AM, Basha, AM 2016, 'A Hybrid Intrusion Detection System Cascading Support Vector Machine and Fuzzy Logic', World Applied Sciences Journal, vol. 35, no. 1, pp. 104-109.

[24] ViswaBharathy, AM, Basha, AM 2016, 'A Hybrid Network Intrusion Detection Technique using Variable Multiplicative K-Means with Self-Organising PSO', Middle East Journal of Scientific research, vol. 24, no. 12, pp. 3812-3819.

[25] ViswaBharathy, AM, Basha, AM, 2016, 'A Detailed Review on Intrusion Detection Systems in Mobile Ad-Hoc Networks Based on Attack Classification and its Detection Technique' in International Journal of Innovative Research in Science and Technology, Vol. 2, no. 9, pp. 228-231.