International Journal of Advanced Research and Development
ISSN: 2455-4030
Impact Factor: RJIF 5.24
www.advancedjournal.com
Volume 2; Issue 6; November 2017; Page No. 644-650

Improved intrusion detection system based on optimized SVM using M-FOA

Farha Haneef, Shailendra Singh
Senior Member, IEEE, NITTTR, Bhopal, Madhya Pradesh, India

Abstract
Intrusion detection system (IDS) is an essential tool to ensure security in cyber space. It is meant for detecting deviations in the normal behaviour of the system. An intrusion detection model is used to correctly classify the incoming data as normal or attack. The main objective is to minimize the false positives and enhance the detection rate and classification accuracy. In this paper, an IDS model has been proposed using optimized SVM. The SVM kernel parameters C and γ are optimized using Modified Fruit Fly optimization Algorithm, (M-FOA)in order to increase the detection rate, lower the false alarm rate and improve classification accuracy. The validity of proposed model has been compared with certain state-of-the–art models using KDD CUP'99 dataset. The result shows better performance than the other SVM classifier models in terms of accuracy, detection rate and false alarm rate.

Keywords: intrusion detection system, classification, parameter optimization, support vector machine, fruitfly optimization algorithm

1. Introduction
Intrusion Detection today is a major field of research owing to extreme digital advancements. With improvements in digital technology, its widespread presence, easy access and high speed internet, security digital systems either in a network or standalone has become an issue of great concern. Recent cyber-attacks like ransomware wanna cry which affected users worldwide, by locking access to their systems until an amount of ransom is paid to the hackers or mirai botnet malware which affected 2.5 million IoT devices brings forward the current situations of extreme vulnerabilities to cyber crimes. Cyber crimes or attacks pose direct harm to the confidentiality, integrity and availability of a system or a network of systems [1]. Due to this severity of challenges, it became most important to find out robust methods to mitigate or at least minimize the malicious intrusions into ones system. For this very reason, Intrusion Detection System (IDS) has remained an all time favourite and ever evolving topic of research for researchers. The works done in this field endeavour towards making it a more computationally effective and accurate model, so that it can work efficiently in real time scenario.
Intrusion detection system (IDS) can be in the form of software or hardware component present in a system or a network of systems to detect any effort for unauthorized access or an attack to on the system. An IDS does the analysis and monitoring of activities by user and system, does the auditing of configuration of systems and their vulnerabilities [2]. The major work of IDS is to classify the incoming data traffic as normal or attack type and alert the administrators in case of any anomaly being detected. The major issue countered in the development of IDS is its misclassification rate.
Many designs of IDS are prone to generate a high rate of incorrect classifications normally called the false alarm rate. It refers to detecting a normal type data packet as an attack type or vice-versa. False detection done by an IDS can be thousands in number which can hugely hamper the performance of security cover promised by an IDS model. Thus, the study of IDS so far, has provided an insight into the fact, that major issue to be dealt with the designing of IDS model is reduce its false or incorrect detection rate. And hence, this itself becomes the basis of this proposed work, which tries to design such a classifier for IDS, which not only minimizes the rate of false detection by it, but also improves its accuracy and detection.
The rest of the paper has been designed as follows- section II deals with the related previous researches on IDS, section III deals with the proposed method for classification and section IV gives the experimental results. The paper is then concluded.

2. Related Work
An IDS model is basically developed in two phases feature selection and classification. Many authors use different combinations of data mining, machine learning, statistics and metaheuristic methods to achieve an efficient model. Some of them are discussed as follows-
The concept of detection of anomalous or intrusive activities was introduced by James Anderson in his report [3], for the very first time by studying the system or network activity patterns. Sannasi Ganapathy *et al*. in [4] present the fact that various computationally intelligent techniques for efficient IDS models are being designed in present times. These include neural network based systems, intelligent agent based systems, systems involving concepts of fuzzy sets, rough sets and soft computing, Particle Swarm Optimization(PSO), Genetic Algorithms etc. They also proposed an IDS model wherein IGR(Information Gain Ratio) was used for feature selection which was able to reduce 41 features of KDD CUP'99 dataset to 19 features by the use of agent based attribute selection algorithm. For Classification IREMSVM

algorithm was used which generated a high detection accuracy of 99.78 and 99.79 for probe and DoS class respectively.

Rung-Ching Chen *et al*. in [5] proposes a model for network intrusion detection based on Rough Set Theory(RST) and SVM. Rough Set Theory in this model was used for feature selection which was able to reduce 41 features of KDD CUP'99 dataset to 29 features. SVM was used as classifier and the classification accuracy achieved with this model was 89.13%. The false positive rate was reduced with this method.

Safaa O. Al-mamory *et al*. in [6] presented a novel concept of two grains levels network intrusion detection system. This model was developed using a very fast decision tree algorithm. This feature set having 41 features was reduced to a set of 20 which resulted in a high detection rate and low processing time. Information gain or gini index was used for feature selection process. The evaluation method was embedded in the VFDT algorithm itself. The concept of Hoeffding Trees was used for classification which was able to generate an accuracy of around 93.825%.

Mohammed A. Ambusaidi *et al*. in [7] presented a filter approach for feature selection based on mutual information. This approach could deal with features which were either linearly or non-linearly dependent. Least Square Support Vector Machine(LSSVM) is used in the form of classifier. The feature selection method is named Flexible Mutual Information Based Feature Selection(FMIFS). The model was able to reduce the KDD dataset to 19 features with high accuracy and detection rate. The accuracy achieved with (FMIFS+LSSVM) model was 99.79%.

Cheng-Lung Huang *et al*. in [8] proposed a Genetic Algorithm(GA) based method to optimize the feature subset and parameters of SVM classifier to improve its classification accuracy for any pattern classification problem. The parameters optimized were the penalty parameter (C) and the kernel function parameter gamma (γ) for the radial basis function. Three criteria were used to design the fitness function including classification accuracy, feature cost and number of features selected. They performed experiments using various real world datasets obtained from UCI repository.

B. M. Aslahi-Shahri *et al*. in [9] have presented a hybrid model for IDS combining Genetic Algorithm(GA) and SVM. The size of optimal feature subset achieved by this model was considerably reduced to 10. This work divided the features selected into three priorities as first, second and third. The first priority was the most important priority having 4 features and the third was the least important having 2 features. The second had 4 features involved. The detection rates achieved as the classification result of SVM for some chromosome was used as a fitness value by GA to generate original components was. The results attained showed a false-positive value of 0.017 and a true positive value of 0.973.

Mehdi Hosseinzadeh Aghdam *et al*. in [10] used the concepts of Ant Colony Optimization(ACO) and K-NN classifier to form a wrapper method. ACO was used for candidate feature subset selection and the classifier's performance was used to evaluate the goodness of subset selected. The reduction in features obtained was a minimum of 3 for R2L class and a maximum of 8 for Probe class. The model was able to decrease detection error by around 24%. The accuracy achieved was 98.9%.

S.Singh *et al*. in [11] proposed a model for IDS combining the concepts of Intelligent Water Drops (IWD) with SVM. The evolutionary algorithm IWD was used to select candidate optimal feature subsets whose worthiness was evaluated by the fitness value of SVM. The feature subset achieved with the help of the hybrid approach consisted of 9 features out 41 features of KDD CUP'99 dataset. The accuracy achieved was 99.0915.

3. Proposed Work

The classification process for IDS model being proposed in this work uses SVM whose optimization is done with M-FOA. Other than function parameters such as the gamma (γ) for the kernel and the penalty parameter C. Designing an SVM, includes choosing a kernel function set, the kernel parameters and a soft margin constant C (penalty parameter).The overall proposed model for IDS is as shown in figure 1.

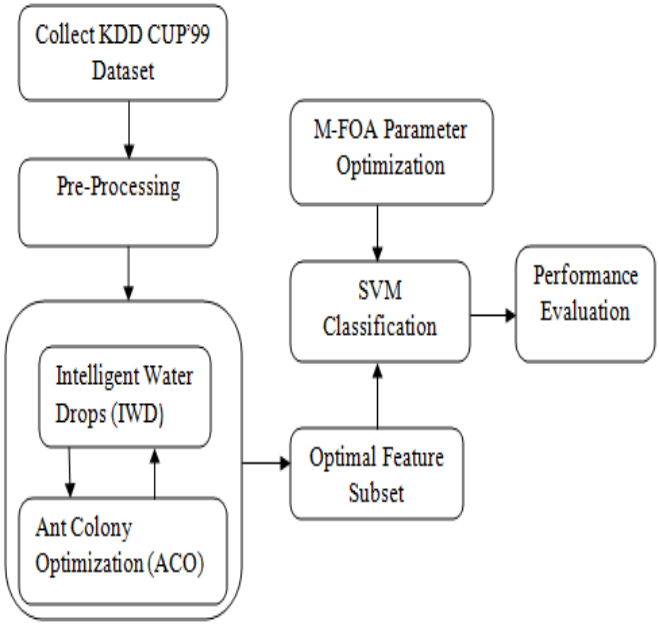

Fig 1: Proposed IDS Model

The design model involves two processes- feature selection and classification. The KDD CUP'99 dataset has been used as the training and testing dataset. After undergoing pre-processing, the dataset is fed to the hybrid feature selection method (IWD+ACO). This method returns the most optimal feature subset required for classification. For the purpose of classification, Support Vector Machine whose parameters are optimized by M-FOA algorithm has been proposed. The procedure unfolds as follows-

1. Pre-Processing- KDD CUP‟99 database has 41 features such as dst_bytes, src_bytes etc. We will prefer only numerical data for testing and training, so text features are needed to be converted into numerical values. Therefore, we have assumed some numerical values for different text features, like protocol_type feature tcp as 3 udp as 7, and „icmp as 9 etc.
2. In this work, IWD & ACO algorithm based approach is proposed to select the optimal features from the overall 41 features. The selected features discriminate in

predicting class during classification for anomaly and misuse. Total 7 features were selected out of 41. In this method IWD algorithm is used to find partial solutions or candidate solutions, from among which ACO algorithm finds the iterations best solution. Thus, ACO refines the choice of a subset for IWD.

3. Classification with SVM

Support Vector Machine (SVM) is one of the most widely used classification algorithms. Its usage has been beneficial in a large scale of applications. Support vector machines are a concept in machine learning that is mainly used for classification and regression purposes [14]. It is basically a supervised learning model. In a given problem, if a set of training data items are given with the knowledge of the class or category to which they belong, an SVM training algorithm builds a model that will assign new data items to one class or the other. A support vector machine is used to develop a hyperplane or a set of hyperplanes in a high-dimensional space, for classification, regression, or other tasks. A good separation is said to have been achieved by the hyperplane which is most distant to the nearest training-data point belonging to any class. The more the distance of the margin, the lower will be the generalization error of the classifier. Assuming we have N training data samples{(x1, y1), (x2, y2).....(xn, yn)}. Here xi ϵ R_n is a set of feature vectors and yi ϵ{+1,-1} is the class label [11]. A binary classification problem is expressed as a Minimization problem as depicted below:

$$\frac{1}{2}\|w\|_2^2 + C\sum_{i=1}^{n}\xi_i \qquad (1)$$

Subjected to: $y_i(w^*x_i) + b >= 1 - \xi_i$, $\xi_i >= 0$, i=1……n

Where C is the regularization parameter, ξ_i is the penalizing relaxation variable.

A non linear classifier in an input space can be depicted as follows-

$$f(x) = sign\left(\sum_i (i=1)^{n} [\alpha^* \times y_i \times K(x_i, y_i) + b^*]\right) \qquad (2)$$

Where, b* is the bias calculated by the Karush-Kuhn-Tucker (KKT)

f(x) is the decision function and $K(x_i,y_i)$ is the kernel function which results in the inner product for the feature space.

Here $K(x_i, y_i)$ is the kernel function Eq. (3). The kernel function used for this work is the RBF Kernel function which is equal to

$$K(x_i, y_j)=\exp(-\gamma\|x_i-y_i\|^2) \qquad (3)$$

The problem of research lies mainly in the field of optimization of the regularization parameter C and the kernel parameter γ of the SVM. Our work tries to identify the best optimizing method for this purpose. The algorithm proposed for the optimization of SVM parameters is M-FOA (Modified Fruit Fly Optimization Algorithm.)

Parameter optimization with M-FOA

Fruit fly optimization algorithm also abbreviated as FOA is one of the latest evolutionary computation method brought to light by Wenchao Pan in his work [13]. FOA is a new entrant in the field of swarm intelligence which is based on the foraging of fruit fly. Fruit flies have strong senses of vision and smelling. They are able to locate food resources far wide in the environment due to their great smelling ability. They approach the food's location, by being directed to their sense vision and the location confirmed by partner.

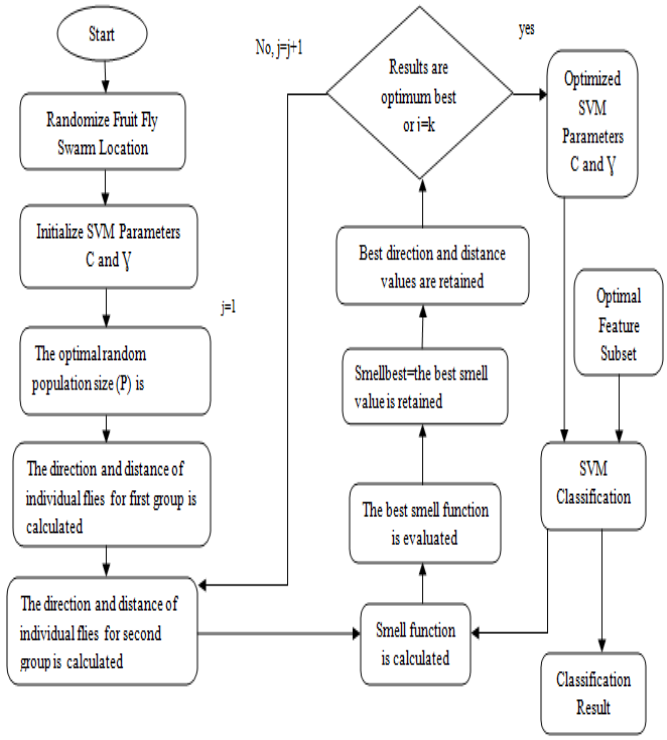

Fig 2: Flow- Chart of M-FOA for parameter optimization of SVM

The M-FOA or the Modified- Fruit Fly Optimization Algorithm is a modified version for existing FOA method. The modification has been done by including random search of two groups of swarm and self-adaptive population size feature into the conventional FOA. The advantages of the MFOA over the FOA are ease of large search range, implementation, less processing time, and reduced memory requirement.

M-FOA, develops two groups from the population size. The work of first group is to look for a new search space with a wide area, and that of second group is to achieve nearby optimum space. Thus, this procedure is able to achieve a wider search space. A set of swarm will follow an optimum solution which another swarm has already achieved. The FOA is modified to have more search space and discontinuous function such as SVM parameter Optimization problems which is referred to as "modified FOA or M-FOA."

As MFOA, separates the population size into two groups, the work of first group is to find a new search space with a wide area, while that of second group is to find nearby optimum space. This procedure can achieve a wider search space. FOA also shows some limitations in its incapability in estimating

the negative value of searching parameters, where they assign the random value of (sign(ε)) on point (−1, 1) at the smell function (Si = sign(ε)/Dist$i$).
The pseudo code of M-FOA for SVM parameter optimization is as shown bellow is as shown below-

begin
fori = 1 tosizepop
Set the SVM parameter with initialized distance reciprocal;
Calculate the individual fitness;
Improve the SVM model with the distance reciprocal and performance assessment
results into the smell array;

end

Initialize No of iterations K;
Set the optimal random population size (P)
Set initial location of fruit fly parameters randomly as X-axis, Y-axis

for j=1 to j<2,
Direction and Distance for all population (P) is generated as
For group 1,
X_i = random value, Y_i = random value
For group 2,
X_i = X-axis + random value, Y_i =Y-axis +random value.
The distance and the smell concentration are calculated as:

$$\text{Dist}_i = \sqrt[2]{x_i^2 + y_i^2}$$

S_i = sign (ε) /Dist$_i$

$\text{Smell}_i = \text{fitness}\ (S_i)$;
Set the SVM parameter with S_i evaluate the initial parameter;
RBF Kernel function for kernel set;
Probability of smell function computation; P(Si|x);
Negative likelihood minimisation;
Decision function for new object classification;

[bestSmell, bestIndex] = max(Smell); Smellbest = bestSmell

best C = S_i(bestIndex);

best$Y$ = S_i(bestIndex);

end

for j=2 till j<=K

Optimal random population size is determined.
Direction and distance for all population size is randomly assigned as:
For group 1,
X_i = random value, Y_i = random value.
For group 2,
X_i = X-axis + random value, Y_i = Y-axis + random value.

The best values for direction and distance X_i and Y_i are utilized from the previous iteration.

Estimate Dist$_i$ = $\sqrt[2]{x_i^2 + y_i^2}$ and S_i = sign(ε)/Dist$i$.

$\text{Smell}_i = \text{fitness}(S_i)$

[bestSmell, bestIndex] = max(Smell);

ifbestSmell > $Smellbest$

Smellbest=bestSmell

else

Smellbest retains the value of previous iteration

best C = S_i(bestIndex);

best$Y$ =S_i(bestIndex);

end for

j=j+1;
return best C, best$Y$;

end

To implement our proposed approach, this research used the RBF kernel function for the SVM classifier because it can analyse higher-dimensional data and requires that only two parameters, C and γ be defined. When the RBF kernel is selected, the parameters (C and γ) are used as input attributes which is optimized using M-FOA algorithm.
The working of M-FOA can be divided in to several steps as follows: First the parameters of SVM which are C and γ, are initialized for optimization. Numbers of iterations are declared then. For the first iteration, for all the individual flies in the population of group 1 and 2, their initial value of x and y are initialized. The main step after population calculates the distance of the optimal food location to the origin distance (D).Then, the smell value(S) is calculated, which represents the reciprocal of the distance of the food location to the origin. Replace the smell value (S) with the smell function S_i which is a fitness function. Establish the fruit fly with the maximal smell or best fitness function absorption and the reciprocal location among the fruit fly swarm contain the maximal smell value and coordinates x and y, which are the optimal points for best fitness function.
The first iteration ends here. Then a loop starting from second iteration to the number of iterations is generated, in which same steps are followed as in first iteration with just a difference that, the best values for the direction and distance are taken from the previous iteration. When the best smell is calculated, it is checked whether it is better than the result of the previous iteration, if so then the overall best value that is Smellbest is made to store its value and indices, otherwise it

Smellbest holds the best value from the previous iteration itself. This refers to the fact that, the fruit fly swarm flies towards the location with the maximal smell value.
The circulation ends when the smell concentration is no longer superior to the early iterative smell concentration or when the iterative number approaches the maximal iterative number.

Fitness Function
The smell value (S) is replaced with the smell function Si which is a fitness function. The fitness function is evaluated using the formula

$$Fitness = f1 * Acc + f2 * DR + f3 * \frac{1}{FAR} \quad (4)$$

Where, Acc is Accuracy of the prediction, DR is Detection Rate of the prediction and FAR is false alarm rate. The fitness function helps the algorithm to find out the best possible value of smell, i.e. location of highest probability for food, ones which increase the accuracy and the detection rate of the classification and lower the rate of false predictions(hence, the inverse value of the false alarm rate). Here f1, f2 and f3 are weights defined by user.

IV Experimental Setup
We have established a framework implementation using java technique where we use JDK 8.0 with Net beans IDE and considered Oracle XE 10G as a best available database to store the KDD parameters and its value to further process.

Dataset
The KDD Cup 99 dataset has been used for implementation of our proposed algorithms. KDD Cup 99 dataset are based on the 1998 DARPA initiative which provide a benchmark for evaluating IDS. In 1998, DARPA Intrusion Detection Evaluation Program was set up and managed by MIT Lincoln Laboratory at MIT. The objective of evaluation program was to evaluate research in the field of intrusion detection.

V Result Analysis
In this section we compare the existing and proposed technique through some parameters such as False Alarm Rate, Precision, and Detection rate, Accuracy, Precision, Detection Rate and F1-Score.

1. **Confusion Matrix:** A confusion matrix also known as an error matrix is generally used to evaluate the performance of the classifier's being implemented. A confusion matrix gives information about the four quantities- true positive, true negative, false positive and false negative.

1. True Positive(TP)- Tells about the true classification i.e Detection of an attack when it is actually an attack.
2. False Positive(FP)- Denotes the misclassification i.e attack detected when it is originally normal.
3. True Negative(TN)- Refers to the accurate detection of the negative class i.e normal detected when it is truly normal.
4. False Negative(FN)- Gives the amount of incorrect detection of the negative class i.e normal detected when it is truly attack

Table 1: Confusion matrix for proposed model

CLASS	Predicted Negative Class	Predicted Positive Class
Actual Negative Class	14118	198
Actual Positive Class	126	31000

2. SVM Parameter Optimization
We have defined the values of the SVM parameters C and γ as the dimensions of the fruit fly in the search space. A two dimensional vectors is the representation of the position of a particle. The lower bound of these dimensions is set to [2^{-15}, 2^{10}] and the upper bound to [2^{-5}, 2^{15}].C=1.0 and gamma= 0.100000000000000001 values were achieved with accuracy of 99.287%.

3. Evaluation Metrics
The various parameters of comparison are as follows-

a. Accuracy- It is a ratio of true or accurate detection to the total detection evaluated. It is represented by the following formula-

$$ACCURACY = \frac{TN + TP}{TN + TP + FN + FP} \quad (5)$$

Accuracy for the proposed work IWD+ACO with GA was 99.287%.

b. Detection Rate- Also known as sensitivity or recall. It is a ratio of total number of true detection out of actual positive detection. The formula is given as follows

$$DETECTION\ RATE(DR) = \frac{TP}{TP + FN} \quad (6)$$

The Detection Rate achieved for the proposed model is 99.595%

c. False Alarm Rate- It is the rate of misclassification. i.e when a data input being actually a negative class is classified as a positive class.

$$FALSE\ ALARM\ RATE(FAR) = \frac{FP}{FP + TN} \quad (7)$$

False Alarm Rate for the model was as low as 1.383%

Table 2: Various Evaluation Metrics for different classifiers

Metrics Classifier	Detection Rate(DR) %	False Alarm Rate(FAR)%	Accuracy (ACC)%
RST+SVM [5]	86.72	13.27	89.13
DSSVM [12]	92.0646	1.5959	93.2997
K-NN [12]	91.0963	1.7048	92.4988
ACO+KNN [10]	98.20	2.59	98.9
GA+SVM [9]	97.3	1.70	n/r
IWD+SVM [11]	99.4075	1.405	99.0915
IWD+ACO +SVM+ MFOA (proposed)	99.595	1.383	99.287

The comparison of the results achieved by the proposed work with previous works done on the IDS models has been shown in the table 2. The results are closely comparable to the IWD+SVM [11] method and GA+SVM [9] method, while varying differences exist with other models. The detection rate of IWD+ACO with GA is 99.595%. The nearest to these values are that of IWD+SVM's 99.4075% and ACO+KNN's 98.20%. While that of RST+SVM and DSSVM lie too far to 86.72% and 92.0646%. The other important metric is that of accuracy which 99.287% for the proposed model is. The only near about results are that of IWD+SVM and ACO+KNN [10] with 99.0915% and 98.9% respectively. The other important metric is that of false alarm rate. The proposed model produces the FAR as low as 1.383 which is only comparable to IWD+SVM's 1.405 and DSSVM's 1.5959. The FAR's of GA+SVM and K-NN are comparable to each other with values 1.70 and 1.7048

Given below are the graphical comparison of all the three parameters of the classifier performance of the proposed method IWD+ACO+SVM+M-FOA with other existing approaches. Figure 3 shows the comparative analysis of the detection rate of various methods, which shows that the proposed work gives highest detection rate with 99.595%. The only comparable result is that of IWD+SVM with 99.4075%. The other closest are that of ACO+K-NN with 98.20% and GA+SVM with 97.3%. The result shows that use of metaheuristic optimization techniques have tremendously improved the detection rates to near perfect solutions.

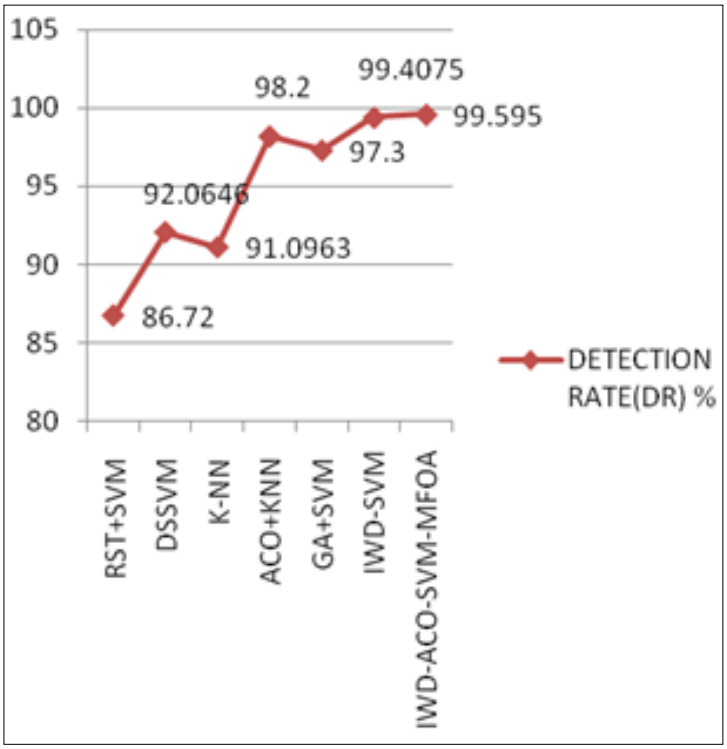

Fig 3: Detection Rate Comparison for all methods

Graphical comparison of False Alarm rates in figure 4 show a very high value of FAR of 13.27 with RST+SVM model which is sharply reduced by DSSVM method with 1.595 FAR. The false Alarm Rates are further reduced with the help of optimization algorithms. This is evident from the result shown as 1.7 for GA-SVM, 1.405 for IWD-SVM and 1.383 for IWD-ACO-SVM-MFOA.

Figure 5 shows a graphical comparison for accuracies of different models. The lowest value of accuracy was achieved by RST+SVM with a value of 89.13% and the highest value achieved was with that of the proposed work with that of 99.287%. While DSSVM and K-NN achieved moderately good accuracies of 93.2997 and 92.4988 respectively. The near optimal accuracies were achieved by new metaheuristic optimization algorithms ACO+KNN and IWD+SVM methods as 98.9% and 99.0915% respectively.

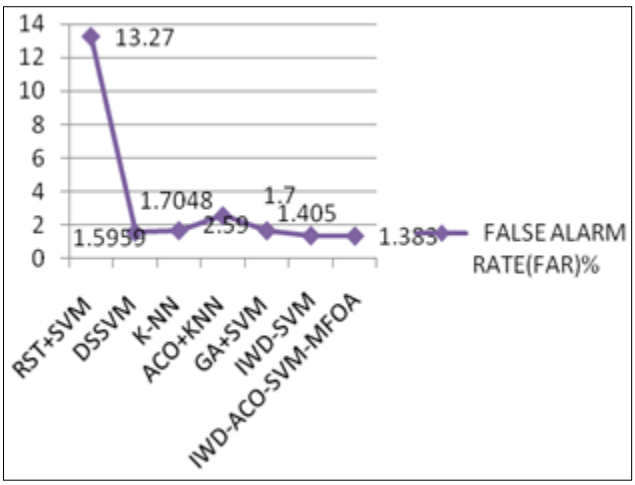

Fig 4: False Alarm Rates Comparison for all methods

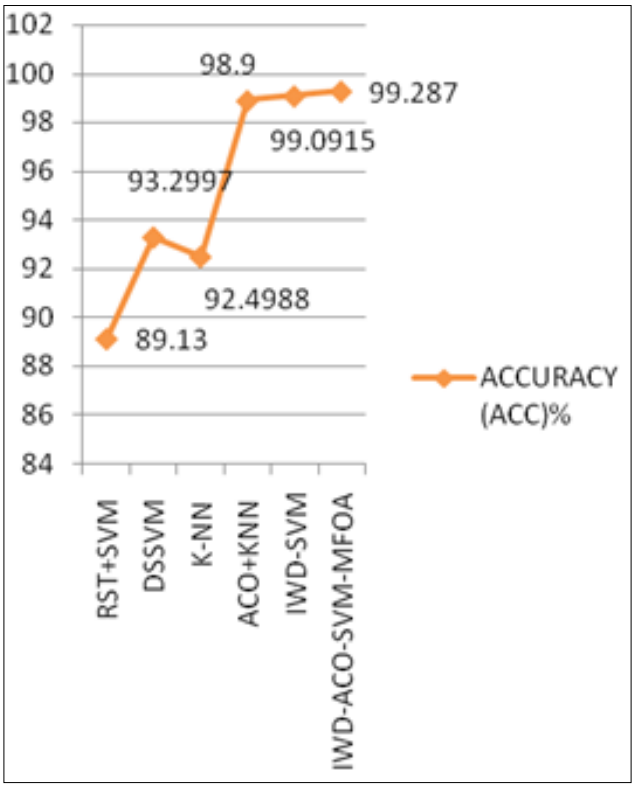

Fig 5: Accuracy Comparison for all methods

4. Conclusion

SVM has proven to be an excellent classier as per the literatures available. In recent researches, the efficiency of SVM classifier has greatly been enhanced by optimizing kernel parameters. In this paper, SVM parameters optimization has been performed by using Modified- Fruit Fly Optimization (M-FOA). The tuning of parameters with the M-FOA algorithm yields better results than existing SVM based classification approaches for intrusion detection. As M-FOA being swarm optimization technique provides ease in implementation, reduces processing time and memory requirement. Contrary to other swarm optimization techniques with self-adaptive population size M-FOA performs random search by deploying two groups of swarms hence it covers larger search space. Result shows that values of C=1.0 and γ = 0.100000000000000001 have achieved with accuracy of 99.287%.The optimized SVM has noticeably reduced false alarm rate to 1.383%,and enhanced detection rate to 99.595%. Further work may include intrusion detection with real time dataset over a real time application.

5. References

1. Singh, Shailendra, Sanjay Silakari. A survey of cyber-attack detection systems. International Journal of Computer Science and Network Security. 2009; 9(5):1-10.
2. Iglesias, Félix, Tanja Zseby. Analysis of network traffic features for anomaly detection. Machine Learning. 2015; 101(1-3):59-84.
3. Anderson, James P. Computer security threat monitoring and surveillance. Technical report, James P. Anderson Company, Fort Washington, Pennsylvania. 1980, 17.
4. Ganapathy, Sannasi *et al*. Intelligent feature selection and classification techniques for intrusion detection in networks: a survey. EURASIP Journal on Wireless Communications and Networking. 2013; 1:271.
5. Chen, Rung-Ching *et al*. Using rough set and support vector machine for network intrusion detection system. Intelligent Information and Database Systems, 2009. ACIIDS 2009. First Asian Conference on. IEEE. 2009.
6. Al-mamory, Safaa O, Firas Jassim S. On the designing of two grains levels network intrusion detection system. Karbala International Journal of Modern Science. 2015; 1(1):15-25.
7. Ambusaidi, Mohammed A *et al*. Building an intrusion detection system using a filter-based feature selection algorithm. IEEE transactions on computers. 2016; 65(10):2986-2998.
8. Braga, Petrônio L, Adriano Oliveira LI, Silvio Meira RL. A GA-based feature selection and parameters optimization for support vector regression applied to software effort estimation. Proceedings of the 2008 ACM symposium on Applied computing. ACM. 2008.
9. Aslahi-Shahri BM. *et al*. A hybrid method consisting of GA and SVM for intrusion detection system. Neural Computing and Applications. 2016; 27(6):1669-1676.
10. Aghdam, Mehdi Hosseinzadeh, Peyman Kabiri. Feature Selection for Intrusion Detection System Using Ant Colony Optimization. IJ Network Security. 2016; 18(3):420-432.
11. Acharya, Neha, Shailendra Singh. An IWD-based feature selection method for intrusion detection system. Soft Computing. 2017, 1-10.
12. Guo, Chun *et al*. A distance sum-based hybrid method for intrusion detection. Applied intelligence. 2014; 40(1):178-188.
13. Pan, Wen-Tsao. A new fruit fly optimization algorithm: taking the financial distress model as an example. Knowledge-Based Systems. 2012; 26:69-74.
14. Cortes, Corinna, Vladimir Vapnik. Support-vector networks. Machine learning. 1995; 20(3):273-297