International Journal of Security and Its Applications
Vol. 11, No. 9 (2017), pp.59-72
http://dx.doi.org/10.14257/ijsia.2017.11.9.05

Improved Detecting Host Based Intrusions Based On Hybrid SVM Using Grey Wolf Optimizer

Vidhya Sathish[1*] and P. Sheik Abdul Khader[2]

[1]*Research Scholar, Department of Computer Applications, B.S.Abdur Rahman University, Chennai-48, India*
[2]*Professor & Director Data Centre, Department of Computer Applications, B.S.Abdur Rahman University, Chennai-48, India*
**Author for Correspondence: vidhyasathish83@gmail.com*

Abstract

The blooming of intrusion instance trace notified as grim threat as per internet industry is concerned. To overcome, detection methodologies are designed by adopting an extensive intense research in the internet industry. Based on the consideration of challenging task and performance existence of contemporary computational methodologies, the objective of this Proposed Research has developed the enhanced hybrid strategy by combining the Support Vector Machine approach from classifier-based techniques and the Grey Wolf Optimizer from evolutionary techniques to optimize the support vector machine parameter towards the accurate classification of Host based intrusions with high detection accuracy and minimal false leads.

Keywords*: Support Vector Machine, Grey Wolf Optimizer, Attribute Classification, High Detection accuracy*

1. Introduction

The blooming of intrusion instance trace notified as grim threat as per internet industry is concerned. The reason is that they may reside over Host end points from neither inside nor outside the organization [1-2]. In common, there are four types of intrusion turned as a root cause for disrupting the Host service. They are known to be Type 1: Denial-Of-Service attacks, Type 2 : User-To-Root attacks, Type 3 : Remote-To-Local attacks and Type 4 : Probing attacks. The 'Type 1' is the class of attacks making the system resources idle. Based on this, 'back', 'smurf', 'teardrop' and 'land' attacks are evolved. The 'Type 2' attacks make the unauthorized access gain authorized privileges from the user's account. The 'Type 3' attacks make the unauthorized access from the remote machine. Based on this, 'Guess Passwd', and 'imap' attacks are evolved. The 'Type 4' attacks bloom based on the port scanning of network. For example, 'nmap', 'portsweep', and 'satan' attacks are evolved. To overcome these intrusions, detection methodologies[3-5] are designed by adopting two common processes during training and testing phases. First, the profile of normal behavior is built during the training phase and second, the current traffic is compared with the profile created in the training phase during the testing phase.

Generally, Signature-based Detection methodologies and Anomaly-based Detection Methodologies are developed as the broad categories of Intrusion Detection Systems. The Signature-based detection methodologies are, in specific, for detecting 'known' pattern *i.e.*, already trained by the system. The Anomaly-based Detection methodologies are, in specific, for detecting unknown anomalies in the current traffic. Most of the detection

Received (January 18, 2017), Review Result (August 16, 2017), Accepted (September 8, 2017)

ISSN: 1738-9976 IJSIA

methodologies are highly framed by Classifier-based and Evolutionary techniques. The Classifier-based techniques are composed of Data Mining and Machine Learning approaches. The exact difference is, Data Mining-based approaches are found on predicting unknown patterns and knowledge discovery of Databases, whereas, Machine Learning-based approaches are found on predicting 'known' patterns and also represent a Pre-Process step with an intent to improve the learner efficiency. Later, Evolutionary Detection methodologies [6] are developed based on real behavior of mammals, insects and species hunting the prey. For example, the prompt of Ant Colony Optimization algorithm was designed based on the real attitude of ants moving towards the prey. Likewise, Particle Swarm Optimization algorithm and Bees Colony Optimization algorithm were developed.

In recent days, Hybrid approach of Classifier-based and Evolutionary techniques have been developed as contemporary computational methodologies with an intent to improve its generalization outcome of detection rate and minimize its false leads over intrusions. Some of the contemporary methodologies showed better accuracy in detecting the intrusion when compared to earlier and later techniques. But the pitfall of these methodologies is the rate of false alarm that seems to be high and clustering over constraints (attack and normal pattern analysis) and needs to be improved. Therefore, the requirements of designing the efficient intrusion detection system in providing the high detection accuracy of and minimal false leads for the classification and characterization of intrusions.

At present, an extensive intense research is going on in the internet industry to attain these challenging requirements. Based on the consideration of challenging task and performance existence of contemporary computational methodologies, the objective of this Proposed Research has developed the enhanced hybrid strategy by combining the support vector machine approach from classifier-based techniques and the grey wolf optimizer from evolutionary techniques to optimize the support vector machine [7] parameter towards the accurate classification of Host based intrusions with high detection accuracy and minimal false leads.

2. Literature Survey

The specification of scrutinizing the accurate classification and characterizing the network traffic instances are discerned as one of the challenging task. This chapter propagandize the comprehensive analysis over diversified detection methodologies[8-10] which intricate with the scheming of detection accuracy acquired from Host-based network traffic. As per literature concerned, utilizing the support vector machine from classifier based techniques and optimization algorithm from evolutionary techniques in designing the intrusion detection systems makes the researchers widely impressive to design the diversified setups as neither single nor hybrid approaches. Based on this, literature analyses are reviewed into three forms. They are known to be Support Vector Machine-based Detection approaches; Optimization algorithm-based Detection approaches and Hybrid approaches of classifier and evolutionary techniques.

(i) Support Vector Machine-based Detection approaches :

Author & Year	Name of the Journal	Methodology	Dataset Utilization	Detection Accuracy	False Positives Obtained
Bahareh, 2014	Journal of Advances in Computer Research	Library Function of Support Vector Machine	KDDCUP99	**99.36%**	**0.64%**
Ambusaidi, 2014	IEEE ICCTSPCC	Least Square Support Vector Machine	KDDCUP99	**99.47%**	**0.52%**
Ravinder, 2014	International Journal of Computer Applications	Support Vector Machine	KDDCUP99	**99.73%**	**2.318%**
Vidhya Sathish, 2014	International Journal of Applied Engineering Research	Study of Library Function of Support Vector Machine	KDDCUP99	**99.78%**	**0.21%**

(ii) Optimization based Detection approaches :

Author & Year	Name of the Journal	Methodology	Dataset Utilization	Detection Accuracy	False Positives Obtained
Huy, 2008	Springer	Sequential Minimal Optimization performance analysis	KDDCUP99	**91.65%**	**0.8%**
Abadeh, 2007	Engineering Applications & Artificial Intelligence	Parallel Genetic Local Search Algorithm	KDDCUP99	**96.3%**	**0.29%**
Benaicha, 2014	IEEE Science and Information Conference	Genetic Algorithm	NSL-KDD	**99%**	**3%**
Aghadam, 2016	International Journal of Network Security	Ant Colony Optimization	KDDCUP99	**98.9%**	**2.59%**

Gomez, 2002	IEEE Proceedings on Information Assurance	Fuzzy Logic	KDDCUP99	**98.95%**	**7%**
Pooja, 2015	International Journal of Engineering Science and Research Technology	Sequential Support Vector Machine Classifier	KDDCUP99	**97%**	**3.94%**
Vidhya Sathish, 2016	Asian Journal of Applied Sciences	Study of Sequential Minimal Optimization for Support Vector Machine	KDDCUP99	**99.85%**	**0.14%**

(iii) Hybrid Approach of Classifier-based and Evolutionary techniques :

Author & Year	**Name of the Journal**	**Methodology**	**Dataset Utilization**	**Detection Accuracy**	**False Positives Obtained**
Chen, 2009	International Journal of Network Security and its applications	Rough Set Theory and Support Vector Machine	KDDCUP99	**89.13%**	**13.27%**
Muda, 2011	International Conference on Information Assurance and Security	One-R and K-Means Clustering	KDDCUP99	**99.26 - 99.33%**	**2.73%**
Mostaque, 2013	International Journal of Innovative Research in Computer and Communication Engineering	Genetic Algorithm and Fuzzy Logic	KDDCUP99	**86.10%**	**0.45%**
Atefi, 2013	International Conference on Computing and Informatics	Support Vector Machine and Genetic Algorithm	KDDCUP99	**99.49%**	**1.78%**
Ghanam, 2015	Journal of Advanced Research	Multi Start meta heuristics method and Genetic Algorithm	NSL-KDD	**96.1%**	**0.03%**

Wang Hai, 2011	Wuhan University Journal of Natural Sciences	Improved Support Vector Machine by Principle Component Analysis and Particle Swarm Optimization	KDDCUP99	**97.75%**	**N/A**
Wang J, 2009	Proceedings of the International Workshop on Information Security and Applications	Support Vector Machine and Binary Particle Swarm Optimization	KDDCUP99	**99.84%**	**N/A**

3. Overall System Architecture

The overall system structure has been designated with five key steps such as Pre-Process, Attribute Selection, Proposed Classifier/Clusterer, Evaluation and Classification Result based on detection accuracy and false alarm rate obtained as shown in Figure 1.

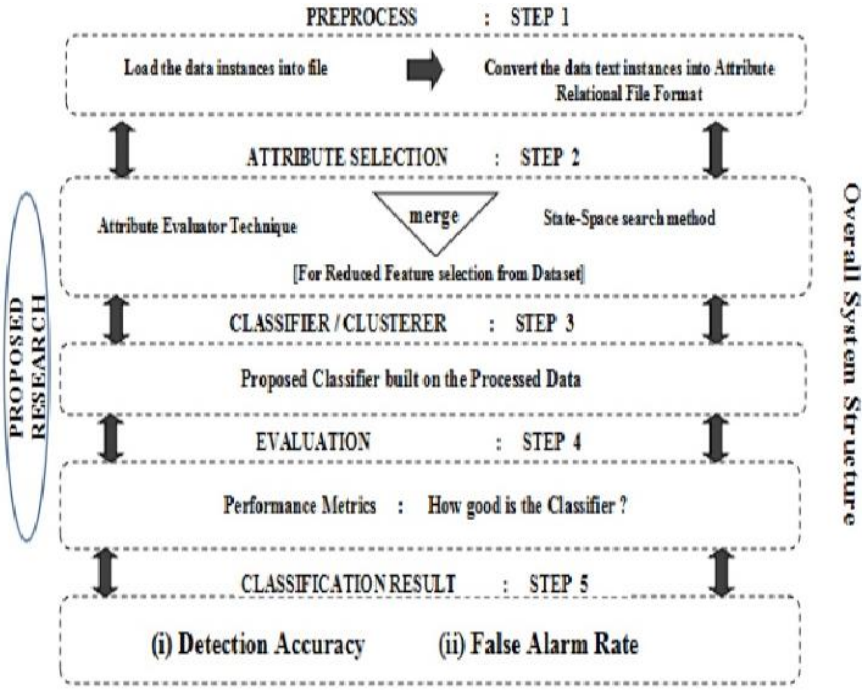

Figure 1. The Overall System Architecture

Description :

In Step 1,

Initially load the data text instances in the file as Comma Separated Value (CSV) format. Before applying the algorithm to selected data instances, convert CSV format into Attribute Relational File format as 'filename .arff' extension. Herewith, each attribute is assigned with a specified number to avoid irrelevance between them.

In Step 2,

Feature Selection (or) attribute selection is the process which automatically searches for the best subset of attributes through 'state-space search method'. Herewith, the performance is improved by locating the best or good enough combinations from overall selecting attributes.

In Step 3,

Own algorithm built and applied directly to the processed data is taken into account by coupling the above-mentioned steps (1 & 2) to classifier approaches. Three keen observations are deployed from the step 3, such as (i) reduced over fitting, which gives opportunity to make decisions over noise, (ii) improved modeling accuracy and (iii) reduced training time, which makes classifier train faster.

In Step 4,

Evaluation is attained based on the cross validation performance metrics to protect over fitting in the predictive model. Herewith, performance metrics expounds with relevant exemplification from the collection of random dataset instances which proclaimed to 'confusion matrix' illustrate for classification of 'normal' and 'attack' pattern instances. The confusion matrix table is assigned with four deviant measures. They are known to be True Positives, True Negatives are the proportion of correctly identified instances, False Positives that are the misleads of True Negatives and False Negatives that are the misleads of True Positives.

In Step 5,

To get the better of congruence results during training the Support Vector Machine classifier at every stage i.e from the study of existing Library Function of Support Vector Machine and Sequential Minimal Optimization till the combined approach of Grey Wolf Optimizer. Sequential Minimal Optimization algorithm provides the elaborate analysis in evaluating the every class instance trace. The main characteristic of this Proposed Research paved a way for proving the High Detection accuracy at a rate and False Positives attained low at a rate in a minimal learning time.

4. Support Vector Machine

Support Vector Machine(SVM) [11-13] is known to be well-known supervised machine-learning classifier from the principle of structured risk minimization. This paved a way to create hyperplane with an intent to extract non-risk and risk factors by minimizing the vector space. The study of SVM is experimented by Sequential Minimal Optimization(SMO) algorithm which is notified as iterative algorithm in process of breaking large data into subspecies of program and can be solved analytically while training the SVM classifier. The expression of SVM can be represented in the form of,

$$\max_{\alpha} \sum_{i=1}^{n} \alpha_i - 1/2 \sum_{i=1}^{n} \sum_{j=1}^{n} y_i y_j k(x_i x_j) \alpha_i \alpha_j$$

Subject to,

$$0 \leq \alpha_i \leq C, \text{ for } i = 1, 2, \ldots n$$

$$\sum_{i=1}^{n} y_i \alpha_i = 0$$

Where 'C' is hyper parameter notified as parameter of prior distribution used, to distinguish between positives and negatives for the underlying system pattern analysis.

$k(x_i\ x_j)$ - Kernel Function
α_i - Lagrange multipliers notified as a strategy of finding local maxima and minima of the function subject to equality constraint.
n - number of training examples.
x_i - i^{th} training example

SVM is the hyperplane that separates the set of positive examples from the set of negative examples with maximum margin. Herewith ' y_i' represents the correct output of SVM [the value of ' y_i' is '+1' for positive class; the value of ' y_i' is '-1' for negative class]. Based on this, the SMO is structured in the form of,

$$0 \leq \alpha_1\ \alpha_2 \leq C \longrightarrow \text{Eq. Step 1}$$
$$y_1\ \alpha_1 + y_2\ \alpha_2 = k \longrightarrow \text{Eq. Step 2}$$

In Eq. Step 1,

initialize the Lagrange multiplier α_i is initialized to distinguish the parameter as prior distribution .

In Eq. Step 2,

based on kernel(SMO binary classification), the optimal Lagrange multiplier is fitted as ' α_1' and then the pair of Lagrange multipliers is optimized as $\alpha_1;\alpha_2$. The process will be progressed until convergence made [when two or more things come together to form a whole].

Structure of SMO kernel function :
(i) Kernel relies on the dot product of inner loop.

(ii) If input is the sparse vector, then it can be stored as 'sparse array'[an array in which most of the elements have a default value as 'null' or 'zero']. The occurrence of large number of zero elements makes the computation and storage inefficient.

(iii) The dot product make repeated use of computational procedure over 'non-zero' inputs.

(iv) In case, input is 'sparse binary vector', then position of 'one's can be stored as input, followed by summing the weights corresponding to the position of 'one's placed.

5. Grey Wolf Optimizer

Grey Wolf Optimizer(GWO) algorithm [14, 7] is designated as evolutionary techniques based new meta-heuristics algorithm. It is derived from real behavior of western wolf which pretends as 'candid wildness' in nature. Two major components are required for any meta-heuristics approach. They are known to be exploration and exploitation. The exploitation describes the investigation by generating diversified solutions in order for the search space in global scale. The exploration focuses the search in local regions. There should be a healthy balance between these two approaches in improving the convergence of algorithm.

The major difference between GWO and other evolutionary approaches are known as GWO notified to be heterogeneous i.e. an enclosure of diversified set of elements makes the experiments to high-level instructional practices when compared to homogeneous families of Ant Colony, Particle Swarm Optimization etc. The GWO moves relatively huge together which seems to be live in the pack. It also remains resilient to execute its stealthy operation while hunting the prey when compared to other evolutionary computational methods. The other difference is pheromone behavior of Ants; Particle

Swarm to contact with their subordinates find duration exceeding to search over the plane. Whereas, 'Grey Wolf algorithm breaks this kind of pheromone attitude by shortening the run time of search.

Structure of GWO :

As per mathematical procedure, GWO can be expressed in terms of :

$$\vec{D} = \vec{C} . \vec{X_p}(t) - \vec{X}.(t)$$

$$\vec{X}(t+1) = \vec{X_p}(t) - \vec{A} . \vec{D}$$

where 't' - indicates the current iteration
xp - Position of prey
x - Position of search agent (Grey Wolves)
c - Distance between prey and Grey Wolves
A - makes the Grey Wolf search globally
t+1 - updates the Grey Wolf positions randomly around the prey.

To find the best optimum, GWO is guided by three search agents such as alpha, beta and delta. The alpha search agent is notified as a decision maker while the other two subordinates help the 'alpha search agent' to find the fittest optimum. The hunting behavior of Grey Wolves can be expressed in terms of:

$$\overrightarrow{D_\alpha} = |\vec{C_1}.\overrightarrow{X_\alpha} - \vec{X}|, \overrightarrow{D_\beta} = |\vec{C_2}.\overrightarrow{X_\beta} - \vec{X}|, \overrightarrow{D_\delta} = |\overrightarrow{C_3}.\overrightarrow{X_\delta} - \vec{X}|$$

$$\overrightarrow{X_1} = \overrightarrow{X_\alpha} - \vec{A_1}.(\overrightarrow{D_\alpha}), \overrightarrow{X_2} = \overrightarrow{X_\beta} - \overrightarrow{A_2}.(\overrightarrow{D_\beta}), \overrightarrow{X_3} = \overrightarrow{X_\delta} - \overrightarrow{A_3}.(\overrightarrow{D_\delta})$$

$$\vec{X}(t+1) = \frac{\overrightarrow{X_1} + \overrightarrow{X_2} + \overrightarrow{X_3}}{3}$$

It is observed that the make the GWO delivers the random behavior throughout the optimization of the search agents. Over repeated times from the global search of candidates, the search agents would estimate the position of prey. The random value of global search lies between [-1,+1]. For instance, Grey Wolf global search moves nearby towards the prey when $|\vec{A}| < 1$ and far by (diverge) from the prey when $|\vec{A}| > 1$.

6. Hybrid SVM With Grey Wolf Optimizer

Utilizing the benefits of SVM from classifier-based technique and GWO from evolutionary technique, the objective of Proposed Research is to develop the enhanced hybrid strategy towards features classification of intrusion instances with high detection accuracy and minimal false leads.

Structure of Hybrid SVM with GWO :

1. Initialize
the population 'n' size; number of search agents; maximum number of iterations; stopping criterion.
Initialize

the parameters such as a, C, A, r1, r2.
Compute the random population and store it as [filename . arff extension]

2. # Generate SVM object with new parameters
$svm = new algorithm : : svm(Type 1; Kernel; C)
Type 1 = $\max_{\alpha} \sum^{n}_{i=1} \alpha_i - 1/2 \sum^{n}_{i=1} \sum^{n}_{j=1} y_i\, y_j\, k(x_i\, x_j)\, \alpha_i\, \alpha_j$

Subject to,

$0 \leq \alpha 1\ \alpha 2 \leq C$ (1)

$y1\ \alpha 1 + y2\ \alpha 2 = k$ (2)

3. # Retrained SVM parameters to calculate the fitness of each search agent

X_α ; X_β ; X_δ

$svm = for (each search agent) in

Current iteration t,

Update the position of current search

agent by equation

Calculate the fitness of each search

agent

if (t+1)

$y_i \varepsilon \{-1 , +1\} =$ A < 1 # move towards fittest optimal

update $X(t+1) = \frac{X_1+X_2+X_3}{3}$

return X_α fitness # optimal value returns

else

Global search A > 1 # diverge from optimal

end if

4. # Procedure to train new SVMmodel for cross validation.
$ svmmodel = fitcsvm (X ,Y , 'kernel function', ' ', 'Standardize', 'true', Class Names', {'neg class', 'pos class'});

$ CVSVMModel = crossval(SVMModel, 'k fold', 10)
$ FirstModel = CVSVMModel . Trained{1}
for i = 1 : k
confusionmat = cell(1,1)
testindex = (CVSVMModel = = i);
trainindex = ~testindex;
SVMModel = fitcsvm (data (train, :), labels(train));
Y= CVSVMModel . Predict (data (test, :));
errormat (i) = sum (index) / length (y);
end for

5. # Classification of attribute output delivers.

True Positives	False Positives
False Negatives	True Negatives

#True Positives & True Negatives = overall accuracy of correctly classified instances

False Negatives & False Positives / False Alarm Rate = overall accuracy of incorrectly classified instances

7. Results & Discussion

The requirements of 'Hybrid SVM' were structured to be notified as 'Improved Anomaly-based Intrusion Detection System', in a real environment. The hardware pre-requisite was originated from Intel(R) Core(TM) i3-2330MCPU processor with 6GB Ram; 500GB Hard Disk and 64-bit operating system along with core software installation performed by Windows 7 operating system background. The software pre-requisite performed by installing the Java Development Kit, 'version 6.0' to run WEKA 'version 3.6.2' in safe mode. Herewith, the random collection of KDDCUP99 dataset was considered for this empirical study.

The experimentation was executed in two varied forms. First, the overall detection accuracy of 'Hybrid SVM with GWO' and its false leads were evaluated from random dataset instances. The results of this strong prospect (as shown in Figure 2. & .3.) were compared with 'Framework of Proposed Efficient Data-Adapted Decision Tree Algorithm[EDADT, 15]'*. The nativity of this existing technique is to change the SVM parameters by applying Radial Basis Function as kernel function and generate the model for each tuning process . (Fig 2.&3) shows Comparison of Techniques in attaining overall high detection accuracy and low false alarm rate. Herewith, Hybrid SVM with GWO achieves 99.98% high detection rate and false alarm rate low at 0.01% when compared to Existing EDADT, 98.12% and false alarm rate 0.18%. Second, to check the integrity of this Proposed Research in reduced feature set using class-wise attributes represented with fifteen different combinations. The results of this strong prospect (as shown in Tabular form.1.)were compared with 'Random tree algorithm'*, used as binary classifier for simulation on WEKA that classifies the instances as 'attack' or 'normal'[16].

RESULT 1

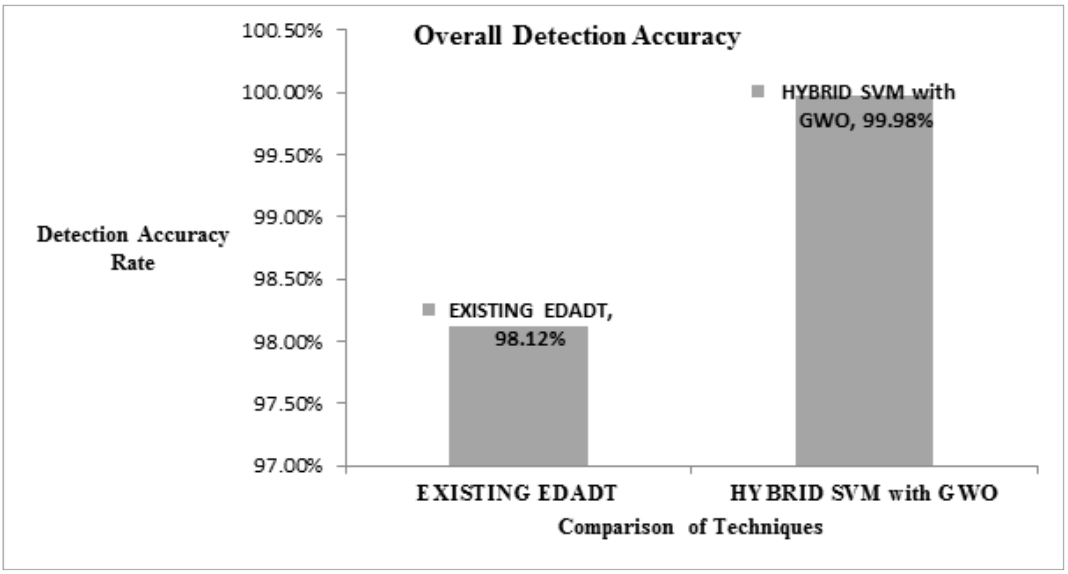

Figure 2. Comparative Study of Techniques Attained in Overall Detection Accuracy

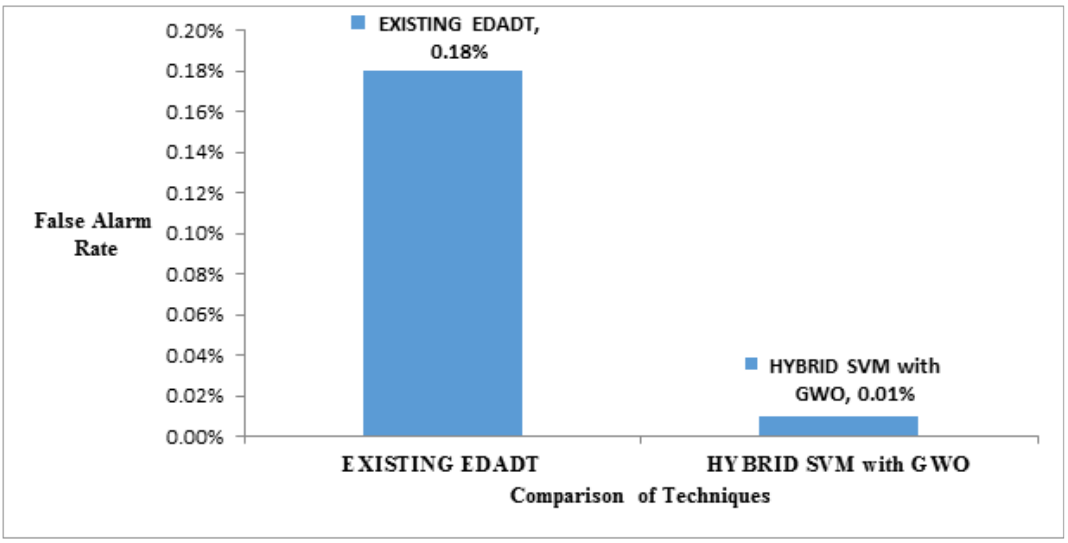

Figure 3. Comparative Study of Techniques Attained in Accuracy of False Alarm Rate

RESULT 2

To validate the integrity of Proposed Hybrid SVM with GWO, in reduced feature set using class-wise attributes that represent with different fifteen combinations from the approximation of twenty five thousand instances from the Tab.1. below. With respect to KDDCUP99 dataset, four different class labels are organized, and based on these labels, data attributes can be categorized from the total of forty two attributes. The four different labels are Basic Features (B), Content Features (C), Traffic Features (T) and Host Features (H). Each class label[16] has unique characteristics and been known that as Basic Features 'B' are acknowledged for individual TCP connection, the Content Features 'C' for suspicious behavior, the Traffic Features 'T' acknowledged for time-based computation and the Host Features 'H' for occurrence of attack instances.

Table 1. Comparative Study of Techniques in Class-wise Attributes for Feature Reduction

Class-wise Attributes	Random Forest Technique		**Hybrid SVM with GWO**	
	Detection Accuracy	False Alarm Rate	Detection Accuracy	False Alarm Rate
1. BCTH	76.54%	8.53%	**99.9805%**	**0.0195%**
2. BCT	78.59%	8.49%	**99.8866%**	**0.1134%**
3. BCH	72.71%	3.47%	**99.9844%**	**0.0156%**
4. BTH	68.61%	3.22%	**99.9531%**	**0.0469%**
5. CTH	61.04%	6.76%	**99.8436%**	**0.1564%**
6. BC	76.19%	8.92%	**99.7967%**	**0.2033%**
7. BT	72.39%	7.55%	**99.8905%**	**0.1095%**
8. BH	71.16%	5.66%	**99.9453%**	**0.0547%**
9. CT	60.91%	7.03%	**99.3862%**	**0.6138%**
10. CH	63.96%	7.12%	**99.7029%**	**0.2971%**
11. TH	61.56%	7.52%	**99.828%**	**0.172%**
12. B	80.78%	6.62%	**99.8006%**	**0.1994%**
13. C	79.42%	24.34%	**81.7826%**	**18.2174%**
14. T	52.59%	6.32%	**99.3823%**	**0.6177%**
15. H	61.12%	7.95%	**99.6873%**	**0.3127%**

RESULT 3

Figure 4. below illustrates a comparative study of the projection of detection accuracy and false positives obtained by DARPA1999 dataset and KDDCUP99 dataset from the varied mode of instances. Herewith, the Detection Accuracy data obtained by DARPA1999 are 99.8582%, 99.8624% and 99.9376% and False Positives are 0.0870%, 0.1376% and 0.0624% respectively. Whereas, KDDCUP99 dataset represents the detection rate as 99.8504%, 99.8740%, and 99.9805% , and False Positives as 0.001% that approximately remains the same for all varied modes of instances. The outcome herewith attained by KDDCUP99 dataset is found to be more accurate for Enhanced Hybrid Strategy than DARPA1999 dataset.

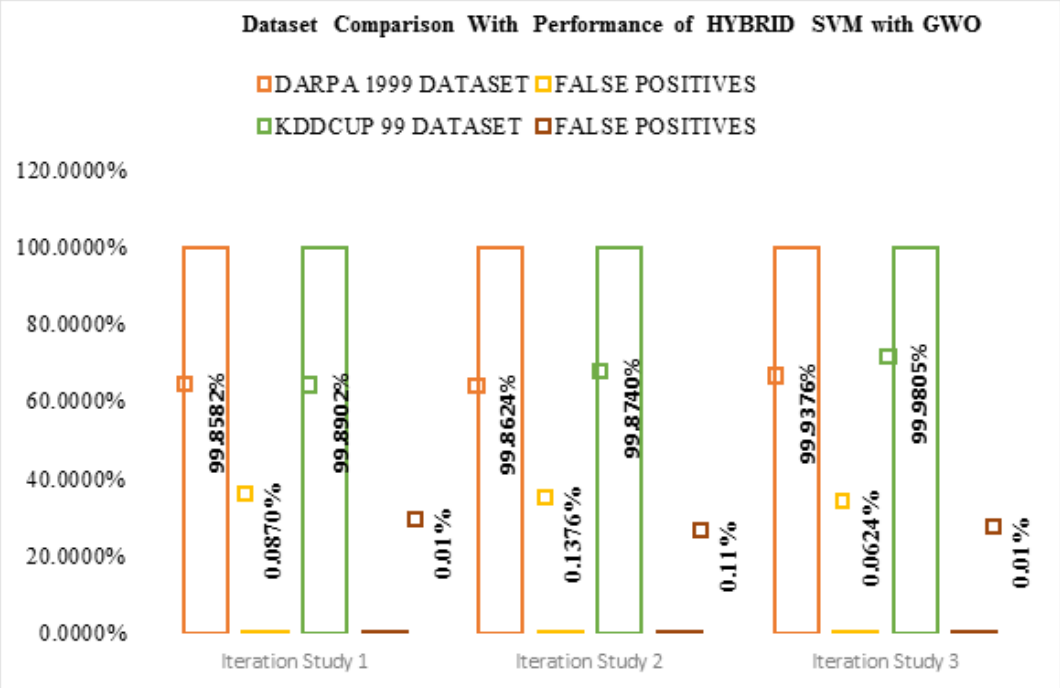

Figure 4. Dataset Comparative Study with Performance of 'Hybrid SVM with GWO' Approach

8. Conclusion

From the congruent results during training the combined approach of Support Vector Machine with Grey Wolf Optimizer algorithm. This work became exalted in evaluating every classification of instance trace. The main characteristic of this Research work paved a way for crafting the well-organized detection system by the proven High Detection Accuracy at a rate of 99.9805% and false positives attained low at a rate of 0.001% in a minimal learning time.

As a future scope of betterment, other classifier approaches such as Extreme Learning Machine and Relevance Vector Machine (equivalent to Support Vector Machine fulfillment viewpoint) approaches will be performed as improved Hybrid Approach with Grey Wolf Optimizer in escalating the justification of extending the research work.

References

[1] H. J. Liao, C. R. Lin, Y. C. Lin and K. Y. Tung, "Intrusion Detection System : A Comprehensive Review", Journal of Network and Computer Applications, vol. 36, **(2013)**, pp. 16-24.
[2] S. K. Jonnalagadda and I. R. P. Reddy, "A Literature Survey and Comprehensive Study of Intrusion Detection", International Journal of Computer Applications, vol. 81, **(2013)**, pp. 40-47.
[3] A. Bijalwan, M. Thapaliyal, E. S. Pilli and R. C. Joshi, "Survey and Research Challenges of Botnet Forensics", Internatioanl Journal of Computer Applications, vol. 75, **(2013)**, pp. 43-50.
[4] P. Sapate and S. A. Raut, "Survey on Classification Techniques for Intrusion Detection", Proceedings of the Fourth International Conference on Advances in Computing & Information Technology (ACITY 2014), **(2014)**, pp. 223-231.
[5] S. Vidhya and P. S. A. Khader, "Deployment of Proposed Botnet Monitoring Platform Using Online Malware Analysis for Distributed Environment", Indian Journal of Science and Technology, vol. 7, no. 8, **(2014)**, pp. 1087-1093.
[6] C. Kolias, G. Kombourakis and M. Maragoudakis, "Swarm Intelligence in Intrusion Detection : A Survey", Computers & Security, vol. 30, **(2011)**, pp. 625-642.
[7] S. Vidhya and P. S. A. Khader, "Enhanced Hybrid Model of Support Vector-grey Wolf Optimizer Technique to Improve the Classifier's Detection Accuracy in Designing the Efficient Intrusion Detection model", Asian Journal of Applied Sciences, vol. 4, **(2016)**, pp. 135-148.
[8] N. S. Chandolikar and V. D. Nandavadekar, "Selection of Relevant Feature for Intrusion Attack

Classification by Analyzing KDDCUP99", MIT International Journal of Computer Science and Information Technology, vol. 2, **(2012)**, pp. 85-90.
[9] M. S. Iftikhar and M. R. Fraz, "A Survey on Application of Swarm Intelligence in Network Security", Transactions on Machine Learning and Artificial Intelligence, vol. 1, **(2013)**, pp. 01-15.
[10] J. Singh and M. J. Nene, "A Survey on Machine Learning Techniques for Intrusion Detection Systems", International Journal of Advanced Research in Computer and Communication Engineering, vol. 2, no. 11, **(2013)**, pp.4349-4355.
[11] N. Maharaj and P. Khanna, "A Comparative Analysis of Different Classification Techniques for Intrusion Detection System", International Journal of Computer Applications, vol. 95, **(2014)**, pp. 22-26.
[12] J. Jyashree and R. Leena, "Intrusion Detection System Using Support Vector Machine", International Journal of Applied Information Systems, vol. 3, **(2013)**, pp.25-30.
[13] M. Arora and L. Bhambhu, "Role of Scaling in Data Classification Using SVM", International Journal of Advanced Research in Computer Science and Software Engineering, vol. 4, **(2014)**, pp. 271-273.
[14] S. Mirjalili, S. M. Mirjalili and A. Lewis, "Grey Wolf Optimizer", Advances in Engineering Software, vol. 69, **(2014)**, pp. 46-61.
[15] G. V. Nadiammai and M. Hemalatha, "Effective Approach Toward Intrusion Detection System Using Data Mining Techniques", Egyptian Informatics Journal, vol. 15, **(2014)**, pp. 37-50.
[16] A. Preetil and S. K. Sharma, "Analysis of KDD Dataset Attributes - classwise for Intrusion Detection", Elsevier Procedia Computer Science, vol. 57, **(2015)**, pp. 842 - 851.
[17] B. Liu, M. Cai and J. Yu, "Swarm Intelligence and Applications in Abnormal Data Detection", Informatica, vol. 39, **(2015)**, pp. 63-69.
[18] G. P. Spathoulas and S. K. Katsikas, "Methods for Post-processing of Alerts in Intrusion Detection: A Survey", International Journal of Information Security Science, vol. 2, **(2013)**, pp. 64-80.
[19] S. Taruna and S. Hiranwal, "Enhnaced Naïve Bayes Algorithm for Intrusion Detection in Data Mining", International Journal of Computer Science and Information Technologies, vol. 4, **(2013)**, pp. 960-962.
[20] S. Vidhya and P. S. A. Khader**,** "Implementation of Automated Detection in Response to Increasing Recognition of Dangers Posed by Insider Threat", Proceedings of the Int. Conf on Information Science and Applications (ICISA), **(2010)**, pp. 407-410.
[21] V. Sathish and P. S. A. Khader, "The Role of Botnet Threat in Today's Distributed Networks A Survey", Proceedings of the 5th Nat. Conf. on Emerging Trends in Information & Communication Technology (ETICT), **(2013)**, pp. 147-150.
[22] V. Sathish and P. S. A. Khader, "A Proposed Hybrid Framework for Improving Classifiers Detection Accuracy over Intrusion Trace", IEEE- International Conference on Electrical, Electronics and Optimization Techniques, Published in IEEE Digital Library, **(2016)**.

