Volume 5, Issue 8, August 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

An Hybrid Genetic Algorithm, Kernel SVM ANFIS Based Multilayer Attack Classification System Size

[1]C. Daniel Nesa Kumar[*], [2]P. Lalitha, [3]M. Hasina Banu
[1, 2, 3]Asst. Professor
[1]Department of MCA, [2, 3] Department of BCA
[1, 2, 3]Hindusthan College of Arts and Science, Tamil Nadu, India

Abstract— An Intrusion Detection System (IDS) gathers information from a network or computer system, and observe the information used for symptoms of system breaks. IDS examine each and every one inbound and outbound network activity and recognize mistrustful patterns with the intention of might designate a network attack beginning somebody effort in the direction of split into or cooperation a system . A predefined threshold value is used in these schemas to designate the stage of normalcy. While there are incidences of latest intrusion events which are more and more a key component of system safety, the arithmetical method cannot distinguish them, some of the classification algorithm has been also proposed to solve IDS problem, but these classification schemas may not perform well because of time to complete the process. To overcome this issue, learning techniques are used which help out in recognize original intrusion activities in a computer system. The objective of the proposed system is to design a new intrusion detection schema by using Swarm Intelligent and other multilayered classification system for Attack detection .This proposed schema used to identify and classify the intruders. In the proposed Intelligent ANFIS Layered Attack Classification System (IALACS), we use an Adaptive Neuro Fuzzy Inference System (ANFIS). The first layer involves Kernel Support Vector Machine (KSVM) classification for detecting the normal and attack. The middle layer involves Neural Network (NN) classification to categorize the attacks into several classes. The third layer involves Genetic Algorithm (GA) to categorize the attacks into various subclasses. The proposed SIANFIS be able to be able to notice an intrusion behavior of the networks, since the IALACS system contains a five intelligent layer classification and better set of rules.

Keywords—Distributed Denial Service of Attacks, Intrusion Detection System (IDS), Support Vector Machine, Neural Networks, Fuzzy Inference System, Kernel Support Vector Machine (KSVM), Adaptive Neuro Fuzzy Inference System (ANFIS), Genetic Algorithm (GA).

I. INTRODUCTION

The aspire of Intrusion Detection System (IDS) is to notice attacks alongside computer systems and system. IDS distinguish effort through rightful users of the information systems in the direction of exploitation their rights and effort through exterior parties to penetrate system to cooperation confidential information, or to reject service. There are two most important propose available to IDSs designed for distinguish attacks: 1) the misuse detection and 2) the anomaly detection [1-2]. These two methods distribute numerous distinctiveness, however are corresponding in with the intention of they each contain strengths and weaknesses. Knowledge-based plan notice intruders through pattern-matching user activity against known attack signatures. Strength of misuse detection example is with the intention of when it signals with the intention of an attack has happen; it is extremely likely with the intention of an attack have essentially happen. In IDS terms, it decreases false positives. A weak point of misuse detection is with the intention of only attacks recorded in the file are able to be accepted. New attacks cannot be recognized. This outcome in disappointment to information some attacks. Conversely, anomaly detection systems proposed in recent works have a higher false alarm rate, at the same time as non-malicious. The extensive investigate on IDS are appropriate to the complexity of ensuring with the intention of an information system determination exist free of charge of security flaws [2]. These existing schemas provide a prevention and detection in layered wise network traffic. Some of the works presented in the recent work is described as follows. Farid et al [3] Misuse-based IDS are extremely successful designed for detecting known attacks however principally unsuccessful designed for notice novel attacks whose pattern has not stored in the database until now. It performs pattern matching in the direction of equivalent an attack pattern equivalent to identified attack patterns in the database. Anomaly-based IDS recognize new attacks through examine anomalous behavior beginning usual behaviors. It has a comparatively elevated discovery rate designed for new attack, however generate numerous false positives. In compound classification domains, input attributes of dataset might enclose false correlations, which hamper the categorization procedure.

Han et al [4] Evolutionary Neural Network (ENN) is proposed for predictable IDS based on the NN. ENN mightn't follow an any examination and fault cycles designed for network arrangement and the near optimal formation are able to be attaining mechanically. Joo et al [5] develop a novel IDS is to differentiate among intruders and normal users. It is complicated to eliminate each and every one possible error appropriate to the huge diversity and difficulty of today's

networks. Even though data mining has become an extremely helpful method through reducing the information overload and enhancing the performance of IDS. Liu & Yu [6] develop a new feature selection, and compare with existing schema. This survey examines several feature selection algorithms, and dissimilarity among the categories. It further addresses a problem springing from the very core of the success of this field - a dilemma faced by most data mining practitioners.

Bivens et al [7] presents a new machine learning based IDS schema, since throughout this time choose engine ports designed for monitoring, decide the formation of the NN, prepare the SOM, and train the NN. The NN system is able to discontinue the learning phase and initiate detection. Basically grouping the information through sources determination not makes a uniform illustration of information designed for the NN which is solved in this work. Ngamwitthayanon et al [8] considered a multi-state IDS scheme to categorize normal information and each attack category by means of the KDD99 dataset. It achieves higher detection rate in when compare to existing methods. Zainal et al [9] proposed a new IDS schema with decrease redundant identification. Consequently, the principle of traffic monitoring is two-folds; to decrease quantity of information to be predictable and to keep away from avoidable identification. For this ANFIS and Linear Genetic Programming (LGP) in the direction of outline ensemble classifiers with the intention of shows a little development using the ensemble approach designed for DoS and R2L classes (attacks).

This paper focal point on capturing the packets of used which is transmitted all the way through the network and mine the attributes from the packet. From the extracted and mined attributes, values of the attributes are noticed to classify the packets into intruders or not inside the file. This file through class label is second-hand as training data designed for KSVM. The output of KSVM gives the records which are notice as attack and this is given as input to NN where training and testing is done. The output of KSVM networks is given to hidden layer FNN and then rules are generated these work, to distinguish the data into two classes. Based on the rules generated in the FNN, the type of attack is detected, then lastly joins these results addicted to greatest combination of a large amount attacks and less attacks consequences using the Genetic Algorithm.

II. PROBLEM STATEMENT

Let 'S' exist the server which is to be present attacked, $A = \{A_1, A_2, A_3, \dots, A_n\}$ is denoted as the attacking users and $L = \{L_1, L_2, L_3, \dots, L_n\}$ is denoted as the legitimate users. Some of the legitimate users, say L_i necessitate the information beginning server S. Throughout the normal access the attacking sources $A = \{A_1, A_2, \dots A_n\}$ unreasonably needs the server S following found the association through the server. If the legitimate users state L_i appeal information beginning server 'S', the service might not be provided. An IDS 'D' is necessary in the direction of categorize request from legitimate users L_i and attacking sources A_i as $DL = \{L_1, L_2, \dots, L_n\}$ and $DA = \{A_1, A_2, \dots, A_n\}$.

III. PROPOSED METHODOLOGY

The objective of the proposed, Intelligent ANFIS Layered Attack Classification System (IALACS) which assist in detecting and classifying the intrusions. The intelligent multi layered approach encloses five intelligent layers. The first layer involves KSVM classification designed for detecting the normal and attack. The second, third and fourth layer involves FNN classification in the direction of categorize the attacks into classes of attacks. The final layer involves GA in the direction of categorize the attacks into various subclasses. The proposed IALACS be able to be able in the direction of notice an intrusion behavior of the networks. ANFIS [11] is a type of ANN. Since it integrates both NN and fuzzy logic principles, it has possible to confine the benefits of together in a particular framework. Its inference system communicates to a set of fuzzy IF–THEN rules with the intention of contain knowledge capability to estimated nonlinear functions.

1. If protocol =TCP, syn =low, port & IP is unequal regarding target =TCP then classify attack1 as TCPflood
2. If protocol = TCP, syn = high, port &IP is unequal corresponding target = TCP then classify attack1 as synflood
3. If protocol =TCP, syn =low & high , port & IP is equal and unequal regarding target =TCP then classify attack1 as Backattack
4. If protocol =TCP, syn =high , port & IP is unequal regarding target =TCP then classify attack1 as Landattack

The file size is symbolized in MB. The table 1 indicates the details for 10 bytes and 100 bytes of packet size.

TABLE. I. PACKETS AND FILE SIZE

Type of attacks	File size(MB)		Number of packets	
	10 bytes	100 bytes	10 bytes	100 bytes
UDP	354	398	612487	459767
TCP	548	348	111154	564797
ICMP	289	254	278974	214578
SMURF	389	189	481971	226899

Kernel support vector machine classification

SVM [12] is learning machines that plot the training vectors in high dimensional feature space, labeling each vector by its class. SVMs provide a generic mechanism to fit the surface of the hyper plane to the data through the use

of a kernel function. The user may provide a function to the SVMs during the training process, which selects support vectors along the surface of this function. The preliminary step is to label the records in preprocessed file. Two class labels are used namely 1 for attack records and -1 for normal records. This labeled file is used for training the SVM. The output is written in two files one containing only attack records and the other contains normal records. Given a set of training examples, each marked as belonging to one of two categories, an SVM training algorithm builds a model that assigns new examples into one category or the other, making it a non-probabilistic binary linear classifier. An SVM model is a representation of the examples as points in space, mapped so that the examples of the separate categories are divided by a clear gap that is as wide as possible. New examples are then mapped into that same space and predicted to belong to a category based on which side of the gap they fall on. In addition to performing linear classification, SVMs can efficiently perform a non-linear classification using what is called the kernel trick, implicitly mapping their inputs into high-dimensional feature spaces. To keep the computational load reasonable, the mappings used by SVM schemes are designed to ensure that dot products may be computed easily in terms of the variables in the original space, by defining them in terms of a kernel function $K(x, y)$ selected to suit the problem. Given some training data D, a set of n points of the form

$$D = \{x_i, y_i\} | x_i \in \mathbb{R}^p, y_i \in \{-1,1\}_{i=1}^n \quad (1)$$

where the y_i is either 1 or -1, indicating the class to which the point x_i belongs. Each x_i is a p-dimensional real vector. Find the maximum-margin hyperplane that divides the points having $y_i = 1$ from those having $y_i = -1$. Any hyperplane can be written as the set of points x satisfying. Maximum-margin hyperplane and margins for an SVM trained with samples from two classes. Samples on the margin are called the support vectors.

$$w.x - b = 0 \quad (2)$$

where $\cdot$ denotes the dot product and w the (not necessarily normalized) normal vector to the hyperplane. The parameter $\frac{b}{||w||}$ determines the offset of the hyperplane from the origin along the normal vector w. If the training data are linearly separable, can select two hyperplanes in a way that they separate the data and there are no points between them, and then try to maximize their distance. The region bounded by them is called "the margin". These hyperplanes can be described by the equations $w.x - b = 1$ and $w.x - b = -1$. By using geometry, find the distance between these two hyperplanes is $2/||w||$, so we want to minimize $||w||$. As we also have to prevent data points from falling into the margin, add the following constraint: for each i either $w.x_i - b \geq 1$ of the first class 1 for attack records or $w.x_i - b \leq -1$ for the second normal records . This can be rewritten as: $y_i(w.x_i - b) \geq 1 \quad for\ all\ 1 \leq i \leq n$ Minimize (w, b) $||w||$ subject to (for any $i = 1,..n$) $y_i(w.x_i - b) \geq 1$. If the kernel used is a Gaussian radial basis function, the corresponding feature space is a Hilbert space of infinite dimensions. Maximum margin classifiers are well regularized, so the infinite dimensions do not spoil the results. Polynomial (homogeneous): $K(x_i, x_j) = (x_i, x_j)^d$

$$k(x,y) = \left(\sum_{i=1}^{n} x_i y_i + c\right)^2 = \sum_{i=1}^{n} (x_i^2)(y_i^2) + \sum_{i=2}^{n} \sum_{j=1}^{i-1} (\sqrt{2x_i}\, x_j)\, (\sqrt{2y_i}\, y_j) + \sum_{i=1}^{n} (\sqrt{2c}\, x_i)(\sqrt{2c} y_i) + c^2 \quad (3)$$

Algorithm 1. Kernel Support Vector Machine (KSVM) algorithm

Input: Number of the training samples x as input for SVM classification

Output: Classification result and prediction of the intrusion detection

- Procedure SVM (x) // input training data results from the SVM classification
- Begin
- Begin
- Initialize C=0 //initially the class labels should be zero
- Get input file feature subset x for training //.
- Read the number of input packet data x from original dataset
- $(x_i . w + b)k_i = 0$ ////Input packet data X is represented as matrix and denoted by x_i and w is the weight value matrix whose product is summed with b bias value to give the class value.
- $(x_i . w + b)k_i = 1$ // This above equation marks a central classifier margin. This can be bounded by soft margin at one side using the following equation.
- Decision function $f(W) = (x_i . w - b)k_i$ //decision function f(w) decides the class labels for the SVM classification training examples ,
- If $f(W) \geq 1$ for x_i is the first class // if the F(w) is greater than or equal to the 1 is labeled as first class (accepted data)
- Else
- $f(W) \leq -1$ for x_i is the first class // if the f(w) is less than or equal to the value of -1 is labeled as second class
- The prediction result for (i=1,…n) number of document //after the classification result are performed then check the classification result by testing phase it is check the below function
- $y_i(x_i . w - b) \geq 1$ //if the function is greater than one the results or classified document as predicted (non accepted data)
- Display the result //finally we display the classification result

TABLE.II DATA SET USED FOR KSVM

Training samples	Attack records	Normal records	Total records
Training set	**300**	**400**	**700**
Testing set	1040	1198	1238
Total set	1340	1598	1938

The Dataset used in the experimentation work is specified in table.2. The total number of samples consists of 1340 records regarding to attacks. The total number of samples consists of 1598 records regarding to normal records. The total number of samples consists of 1938 records regarding to total records. From the table 2 it is observed that the testing records are three times greater than the normal training records.

Fuzzy Neural Network for hidden layer: Fuzzy Neural Network (FNN) [13] is knowledge mechanisms with the intention of discover the parameters of a fuzzy system through exploiting estimate techniques beginning NN. NN be able to only move toward interested in cooperate if the problem is expressed through an adequate amount of observed examples. In FNN frequently extremely time consuming and error-prone. To solve this problem , primary algorithm construct the first formation of the network by means of KNN and continue adding together more rules designed for covering data points through the maximum miscalculation in anticipation of the rewarding RMSE is accomplished. Subsequently, the number of rules is optimized by means of GA which tries to decrease the neuron numbers at the same time as retaining network error is very low. The second algorithm does the same although make use of Mean- Shift algorithm designed for discovery a good set of preliminary rules. The class label specified designed for every type of attack is shown in Table.3.3. The table point toward the target value second-hand designed for dissimilar attack types. A user distinct value is able in the direction of is second-hand designed for target value. According to the table a value of 0.4 represents TCP flood attack. FNN input attributes is followed as , Count, Syn count , Echo request count, Protocol, Flag for same IP address , Flag for same port, Class label and Source bytes

TABLE .III. CLASS TYPES

Attack Type	Class label
TCPFlood attack	0.4
UDPFlood attack	0.5
ICMPFlood attack	0.6

***KNN* algorithm [14]** is considered in two major phases such as Rule generation and rule reduction. In the rule generation stage, the K-Nearest-Neighbor (KNN) algorithm is proposed to classify the samples under less error value. In the rule reduction phase, a reduces or decrease the number of rules depending on Genetic Algorithm. After adding or removal rules from the dataset rule, least square error value is examined to NN to categorize the most excellent consequent parameters. In the initial phase rules are generated using K Nearest Neighbor (KNN). The KNN algorithm attempt to establish these local optimums through examining each point through its KNN. Designed for a training data point $X = (x_1, x_2, \ldots, x_n)^T$, describe A_x as the set of K training input points through the nearest Euclidean distance in the direction of x. Thus, designed for the known training points set P , set the center vectors of initial fuzzy rules as follows,

$$M = \{x = (x_1, \ldots, x_n) \in P | y(x) < y(A_x) \text{ or } y(x) > y(A_x)\} \quad (4)$$

In this algorithm, Gaussian function through a mean and width $\sigma_0 = (\sigma_0^1, \sigma_1^1, \ldots, \sigma_n^1$ is preferred as a membership function of fuzzy sets. .A good heuristic can in addition be employ which make use of the standard deviation of KNN as width values. After creation of first fuzzy rules through KNN method, the consequent parameters be supposed to be learned. These consequent parameters be able to be identified using LSA. Important the consequent parameters as vector $C = (c_0^1., c_1^1, \ldots, c_n^1)$, approximation C by means of LSA; with the intention of is:

$$C = (H^T H)^{-1} H^T Y \quad (5)$$

For generated rules obtain RMSE values, apply GA to reduce the RMSE error value. In GA, a population is generated from training samples and genetic algorithms such as like crossover and mutation are applied to training samples. In each generation, a selection process is applied to training samples. In the selection step, a fitness value is determined to training samples. Represented in the form of binary string bit 1 belongs to corresponding neuron is selected and 0 means that the corresponding neuron is not selected. Fitness value of the GA is determined as follows,

$$fitness = \begin{cases} RMSE * M & if\ RMSE > 2 * \tau \\ L & Otherwise \end{cases} \quad (6)$$

In fuzzy set triangular membership function is determined for $x = (x_1, x_2, \ldots, x_n)$ which is described as follows:

$$i = \arg\max \left\{ \prod_{j=1}^{D_i} t(xa_j^i, b_j^i, c_j^i) \right\} \quad (7)$$

where $t(x; a, b, c)$ is a triangular-shaped membership function,. a_j^i, b_j^i, c_j^i are values represents low, medium and high of j -th fuzzy triangular set in i-th dimension, correspondingly. For fuzzy rule i, $C_i = (c_i^1., c_i^2, \ldots, c_i^n)^T$, denotes the

center vector and $A_i = (a_i^1., a_i^2, \ldots, a_i^n)^T$ and $B_i = (b_i^1., b_i^2, \ldots, b_i^n)^T$ denotes low and middle vectors of triangular. Newly generated fuzzy rule through the subsequent center vector is making:

$$C^{M+1} = [c_1^{M+1} \ldots., c_r^{M+1}], c_j^{M+1} = \begin{cases} c_j^i & j \neq r \\ x_r & j = r \end{cases} \quad (8)$$

Determine the degree to which this signal be in the right place to the neuron‟s fuzzy set

$$y_i^2 = f(x_i^2) \quad (9)$$

where f denotes the activation function in FNN i. The third layer apply a single first-order Sugeno fuzzy rule - a rule neuron receives signals simply beginning the fuzzification neurons with antecedents and consequents parts is described as follows,

$$y_i^3 = \prod_c^m x_i^3 \, C_i \quad (10)$$

Where x_i^3 be the third layer resutls with c. y_i^3 is the output signal of FNN and m denotes the antecedents parts of fuzzy rule neuron i. The fourth layer, results might be updated depending on the following equation (11) :

$$y_i^4 = \frac{x_d^4}{\sum x_d^4} \quad (11)$$

The output of NN is accumulating in a file alongside through additional attributes. This file is given as input to GA where the rules are written. Genetic algorithm (GA) [15] is a investigate heuristic with the intention of mimics the procedure of natural assortment. This heuristic is characteristically second-hand to make useful solutions in the direction of optimization. Genetic Algorithms belong to the larger class of Evolutionary Algorithms (EA), which generate solutions to optimization problems is motivated by means of natural development, such as inheritance, chosen ,crossover and mutation . In a GA, every one candidate solution has consists of set of chromosomes. The development frequently starts beginning a population of indiscriminately generated individuals called a generation. In each generation, the fitness of every one individual in the population is evaluated; the fitness function is commonly determined to select optimal solution. In this work the number of rules are definite lower than through synchronization and IP is in use as the fitness value subsequently it practical to subsequent rules in the direction of classify the attacks

- If protocol =TCP, syn =low, port & IP is unequal regarding target =TCP then classify attack1 as TCPflood
- If protocol = TCP, syn = high, port &IP is unequal corresponding target = TCP then classify attack1 as synflood
- If protocol =TCP, syn =low, port & IP is equal and unequal regarding target =TCP then classify attack1 as Backattack
- If protocol =TCP, syn =high , port & IP is equal and unequal regarding target =TCP then classify attack1 as Landattack

The steps of Genetic algorithm are the following:

1. Initialize the population with random number of the rules in the hidden layer.
2. Evaluate all individuals in the present population, assigning a numeric rating or fitness value to each one from the attributes.
3. If the termination criterion is fulfilled, then execute
4. The last step. Otherwise continue.
5. Reproduce the best n individuals into the next generation population.
6. Select m individuals that will compose the next generation with the best parents.
7. Apply the genetic operations to all individuals selected. Their offspring will compose the next population. Replace the existing generation by the generated population and go back to Step 2.
8. Present the best individual(s) in the population as the output of the evolutionary process.

The algorithm stops until it reaches the required maximum number of cycles or iterations. The fifth level, i.e. the fourth hidden layer is the defuzzification level. Every one neuron in this layer is associated to the individual normalization neuron in the fourth layer and moreover receives first input data,

$$y_i^5 = x_i^5(k_{i0} + k_{i1}x_1 + k_{i2}x_2 + \cdots . + k_{in}x_n) \quad (12)$$

IV. EXPERIMENTATION RESULTS

The proposed schemas are implemented with the help of MATLAB and extract the attributes beginning the packet. A very significant conclusion is the selection of feature [10] with the intention of would be second-hand in attack detection. The features of network traffic be supposed to be in a appropriate structure in order to be without difficulty processed and representative of NN activity be proficient in the direction of differentiate usual and abnormal action. It is significant with the intention of the selected features increase the contrast among usual and irregular action regarding attacks. The examination about diverse types of attacks and the attributes essential designed for that attack are done. The rules designed for each and every one attacks and attributes necessary designed with the purpose of rules are identified through learning. The attributes known below are taken designed for dispensation and some of the attributes are described below. The a large amount important features designed for the discovery of DDOS attacks comprise,

- Source Address - IP address of the source machine which sends packet
- Destination Address - IP address of the destination machine to which the packet is forwarded

- Source port - Port number of the application in source
- Destination port - Port number of the application to which the packet is sent
- Count - Total number of packets for the same source and destination
- Syn Count - Total number of packets with syn flag enabled
- Echo Request Count -Total number of packets with echo request flag enabled
- Protocol - Type of the protocol
- Source Bytes - Displays how many bytes have been transferred in packet

The IDS detection rate of the proposed IALACS and the existing ANFIS, ANN learning schemas is measured using the classification parameters namely precision, recall and accuracy .These schemas is implemented and experimented with the help of the MATLAB environment. The detection accuracy results are measured and evaluated using the following metrics which is described as follows.

Precision: Precision value [16] is determined based on the detection results at true positive prediction, false positive .In medical application , precision is determined based on the percentage of positive results returned that are relevant.

$$Precision = TP/(TP + FP) \quad (13)$$

Recall: Recall value [17] is determined based on the detection results at true positive prediction, false negative. In medical application, recall is defined as the percentage of positive results returned and it is also referred to as the TPR,

$$Recall = TP/(TP + FN) \quad (14)$$

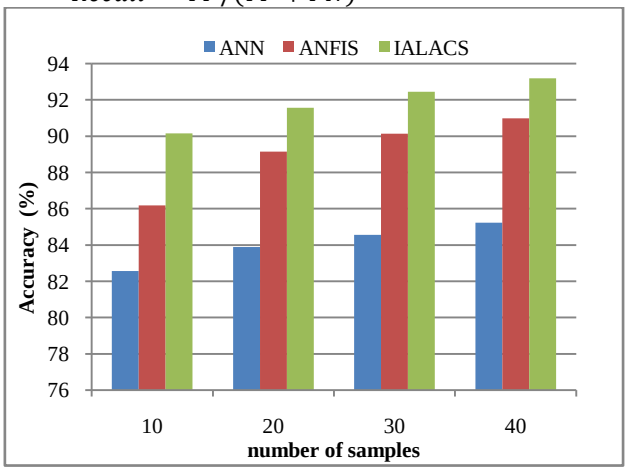

Fig.1. Accuracy vs. methods

In the Fig.1 shows the performance accuracy [18] comparison results of the proposed IALACS and the existing ANFIS , ANN learning methods for IDS ,it shows that the performance comparison results of the proposed IALACS is high .Since it uses five layer neural network learning structure and individual layers uses the different classification methods such as the KSVM for input layer , FNN for hidden layer and genetic algorithm for output layer than the existing ANN with input layer for SVM ,hidden layer for ANN and output layer for Fuzzy Inference System (FIS).

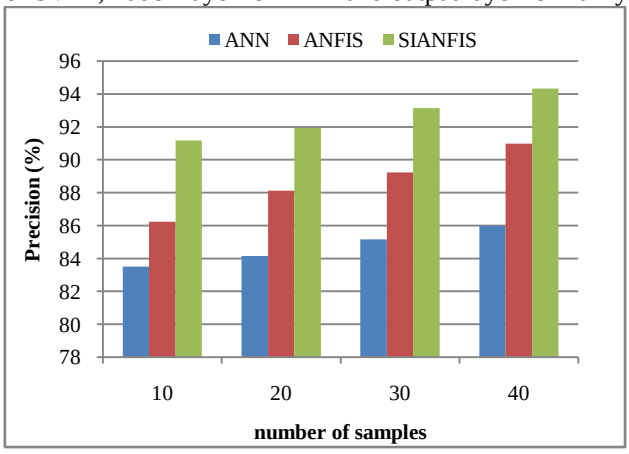

Fig.2.Precision vs. methods

Fig.2 shows the precision comparison results of the proposed IALACS and the existing ANFIS , ANN learning methods for IDS ,it shows that the precision results of the proposed IALACS system is high .Since it uses five layer NN learning structure and individual layers uses the different classification methods such as the KSVM for input layer ,FNN for hidden layer and genetic algorithm for output layer than the existing ANN with input layer for SVM ,hidden layer for ANN and output layer for FIS.

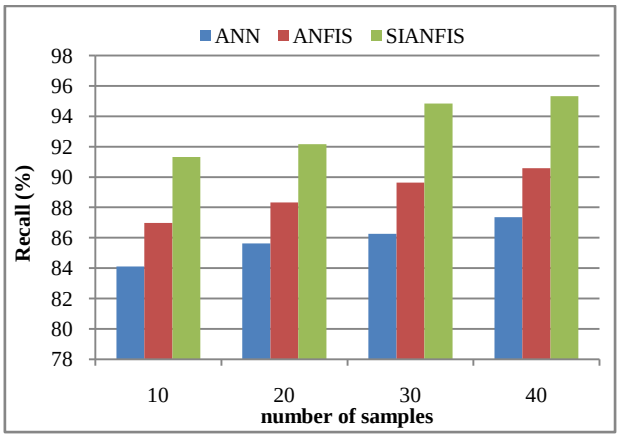

Fig.3. Recall vs. Methods

Fig.3 shows the recall comparison results of the proposed IALACS and the existing ANFIS, ANN learning methods for IDS, it shows that the precision results of the proposed system is high .Since it uses five layer neural network learning structure and individual layers uses the different classification methods such as the KSVM for input layer, FNN for hidden layer and GA for output layer than the existing ANN with input layer for SVM, hidden layer for ANN and output layer for FIS.

V. CONCLUSION AND FUTURE WORK

In this paper proposed a novel Intelligent ANFIS Layered Attack Classification System (IALACS) approach, it consists of two major phases preprocessing and classification. In preprocessing, the formation of real time dataset is completed and in classification there are five layers are used to classify the packets into intruder or not .In layer 1 KSVM binary classification is done, Fuzzy Neural Network classification as layer 2 ,3 and layer 4 where most important classes of attack type are detected and final layer Genetic Algorithm classification as layer 5 where subclasses of attack type are detected. This IALACS schema improves detection rate of the intrusion than the existing three layer neural network algorithm. IALACS algorithm achieves higher classification results in terms of classification metrics like, Precision, Recall and Accuracy. In the future the scope of the present schema is expanded to diverse misuse detection type of attacks and it be able to be combined through a few other classifiers. In future work refer other data mining techniques to advance the detection rate and decrease False Negative Rate.

REFERENCES

[1] Asokan, N., Niemi, V., & Nyberg, K, *Man-in-the-middle in tunnelled authentication protocols*, In Security Protocols , Springer Berlin Heidelberg ,pp. 28-41,2005

[2] Stakhanova, N., Basu, S., & Wong, J, "Taxonomy of intrusion response systems," *International Journal of Information and Computer Security*,vol.1,no.1-2,pp. 169-184, 2007.

[3] Farid, D. M., Harbi, N., & Rahman, M. Z , "Combining naive bayes and decision tree for adaptive intrusion detection," arXiv preprint arXiv:1005.4496, 2010

[4] Han, S. J., & Cho, S. B, "Evolutionary neural networks for anomaly detection based on the behavior of a program," *IEEE Transactions on Systems, Man and Cybernetics Part B: Cybernetics*, vol.36, pp.559–570,2006.

[5] Joo, D., Hong, T., & Han, I, "The neural network models for IDS based on the asymmetric costs of false negative errors and false positive errors", *Expert Systems with Applications*, vol.25, no.1, pp.69-75,2013.

[6] Liu, H., & Yu, L , "Toward integrating feature selection algorithms for classification and clustering", *IEEE Transactions on Knowledge and Data Engineering*, vol.17,no.4, pp.491-502,2005.

[7] Bivens, A., Palagiri, C., Smith, R., Szymanski, B., & Embrechts, M , "Network-based intrusion detection using neural networks", *Intelligent Engineering Systems through Artificial Neural Networks*, vol.12,no.1, pp.579-584, 2002.

[8] Ngamwitthayanon, N., Wattanapongsakorn, N., Charnsripinyo, C., & Coit, D. W , "Multi-stage network-based intrusion detection system using back propagation neural networks", *In Asian International Workshop on Advanced Reliability Modeling (AIWARM), Taiwan* , pp. 609-619, 2008.

[9] Zainal, A., Maarof, M. A., & Shamsuddin, S. M, "Data reduction and ensemble classifiers in intrusion detection", *Second Asia International Conference on Modeling & Simulation, AICMS 08*. pp. 591-596, 2008.

[10] Sangkatsanee, P., Wattanapongsakorn, N., & Charnsripinyo, C , "Practical real-time intrusion detection using machine learning approaches", *Computer Communications*, vol.34, no.18, pp.2227-2235, 2008.

[11] Jang, J. S. R, ANFIS: "Adaptive-Network-based Fuzzy Inference System*", IEEE Transactions on Systems, Man and Cybernetics*, 23(3), 665-685, 1993.

[12] Fung, G. M., & Mangasarian, O. L , "Multicategory proximal support vector machine classifiers", *Machine learning*, vol.59, no.1-2, pp.77-97.

[13] Cheng, H. D., & Cui, M, *Mass lesion detection with a fuzzy neural network*, Pattern Recognition, vol.37,no.6, pp.1189-1200,2002.

[14] Malek, H., Ebadzadeh, M. M., & Rahmati, M, "Three new fuzzy neural networks learning algorithms based on clustering, training error and genetic algorithm", *Applied Intelligence*, vol.37, no.2, pp.280-289,2012 .

[15] Gonçalves, J. F., de Magalhães Mendes, J. J., & Resende, M. G, "A hybrid genetic algorithm for the job shop scheduling problem", *European journal of operational research*, vol.167,no.1, pp.77-95, 2005.

[16] Ting, K. M. , *Precision and recall*, In Encyclopedia of machine learning , Springer US, pp. 781-781.

[17] Shafi, S. M., & Rather, R. A. , " Precision and recall of five search engines for retrieval of scholarly information in the field of biotechnology", *Webology*,vol.2,no.2, 2005.

[18] Diebold, F. X., & Mariano, R. S., "Comparing predictive accuracy", *Journal of Business & economic statistics*, 2012.

