Improve Accuracy of Intrusion Detection System Using the Synthesis Computing Classifier Methodology

M. V. Siva Prasad and Ravi Gottipati

***Abstract*—Network security is the most critical part in organizations, social and enterprise systems. There are different levels in security. (The first level being preventions) The Most important level is Intrusion Detection System (IDS). IDS's are responsible for monitoring security issues, network traffic etc., But it's most essential task is detection of intrusions. Computing classifiers play a major role in all research areas including IDS. IDS have been achieved following different procedures and methods which have been projected in various research works. But, many of them aren't able to compute the problem with full accuracy assessment. So, main objective of my research work is to integrate numerous computing techniques into a categorized system, to detect and classify intrusions from usual activities based on the attack type in a computer network and try to improve the accuracy assessment. One of the most used mechanisms for creating rule sets is Decision-tree approach. Decision tree creations, using numerous algorithms, have been produced by different people. So far, the best algorithm is a C4.5/SEE 5.0. Using this algorithm constructs rule set 1. More than this a prominent approach to create rules other hand soft computing methods is Neural Network Theory and Fuzzy Logic. The next step, to create rule set 2, using both approaches are amalgamate and allocate. Final rule set derivation, in a process called Synthesis Computing Classifiers, can be done using Build decision boundary methodology based on the above rule set1 and set 2. The investigational result sets clearly show that the proposed new systems have achieved higher precision in identifying whether the records are normal or attack one.**

***Index Terms*—Intrusion detection system (IDS), C4.5/SEE5.0, neural network theory, fuzzy logic, build decision boundary and synthesis computing classifiers.**

I. Introduction

Intrusion Detection Systems have been a vital part in research and development since long time. With the increased artificial intelligence and particularly heightened attacks on computers and networks, in the recent years, improved - and essentially - automated surveillance has become a necessary addition to IT security. Intrusion recognition is the process of observing the events that are happening in an organization system or communications network and analyzing them for signs of intrusions.

There are two main approaches to developing intrusion detection systems: The first one is Misuse detection approach, which uses patterns (called signatures) to detect the presence of known attacks. The second one is Anomaly detection approach which builds a model of normal behavior of the system. Any system behavior that does not match with this model is reported as an anomaly.

While anomaly detection typically utilizes threshold monitoring to indicate when a certain established metric has been reached, misuse detection techniques frequently utilize a rule-based approach using computing methods. The use of comprehensive rules is critical in the application of expert systems for intrusion detection. Most current approaches to the process of detecting intrusions utilize some form of rule-based analysis. Rules system examination based on sets of existing rules that are provided by a system organizer, automatically created by the system, or both. The use of expert system techniques in intrusion detection mechanisms was a significant milestone in the development of effective and practical detection-based information security systems. Expert rules are generating based on different methodologies, most likely Data Mining, Neural Networks methods, Soft Computing and etc. Most traditional method, for generating a rule-set, is based on decision tree (ID3 algorithm). It's been used by many researchers from earlier days to the present days. After ID3, a number of advanced decision tree algorithms were proposed by various research teams. But, the most successful rule based algorithm is C4.5 (SEE 5.0). This paper proposes a method to construct rules using C4.5 algorithm in novel approach. Based on proposing novel approach, it is possible to generate a better rule-set compared to any existing rule-set generation algorithms [1]. The next most popular rules-set-generation methods are Neural Networks techniques, Fuzzy Logic based methods and Neuro-fuzzy (referred to as combinations of artificial neural networks and fuzzy logic). The neural network consists of a collection of processing elements that are highly interconnected and transform a set of inputs to a set of desired outputs. The result of the transformation is determined by the characteristics of the elements and the weights associated with the interconnections among them. By modifying the connections between the nodes the network is able to adapt to the desired outputs [2], [3]. Unlike expert systems, which can provide the user with a definite answer if the characteristics which are reviewed exactly match with those which have been coded in the rule base, a neural network conducts an analysis of the information and provides a probability estimate that the data matches the characteristics which it has been trained to recognize.

The neural network architecture which was selected for [4] was a self-organizing feature map which uses a single layer of neurons to represent knowledge from a particular domain in the form of a geometrically organized feature map. The proposed network was designed to learn the characteristics of normal system activity and identify statistical variations from the norm which may be an indication of a virus. Next one of

Manuscript received January 21, 2014; revised April 1, 2014.

M. V. Siva Prasad is with the Anurag Engineering College, Kodad 508206, India (e-mail: magantisivaprasad@gmail.com).

Ravi Gottipati is with the Tripod Technologies, Hyderabad 500082, India (e-mail: softtotime@gmail.com).

the most surface techniques, Fuzzy logic starts and builds on a set of user-supplied human language rules. The fuzzy systems convert these rules to their mathematical equivalents. Additional benefits of fuzzy logic include its simplicity and its flexibility. The latest in fuzzy is to use the Markov model. As suggested in a Window Markov model is proposed, the next state in the window equal evaluation to be the next state of time t, so they create Fuzzy window Markov model. As discussed, researchers propose a technique to generate fuzzy classifiers using genetic algorithms that can detect anomalies and some specific intrusions. Fig. 1 shows the general of the fuzzy logic system for this research process.

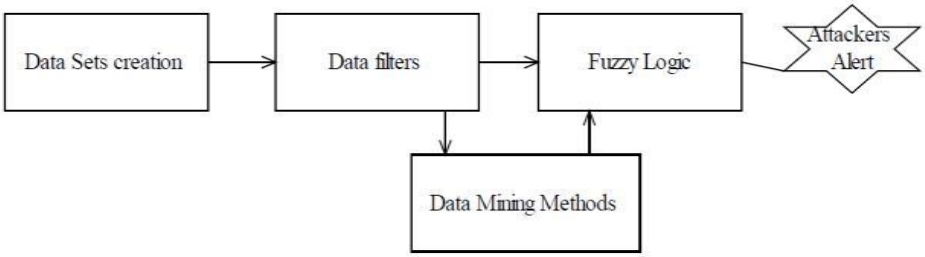

Fig. 1. Outlines for contract fuzzy logic system.

The main idea is to evolve two rules, one for the normal class and other for the abnormal class using a profile data set with information related to the computer network during the normal behavior and during intrusive (abnormal) behavior.

The crux of the this paper is to automatically extract rule set from the data using computing classifier and to use this rule set in classifies attackers. Generally rule base is created using expert's knowledge and experience. This method of knowledge acquisition is a long and repeated process. On the other hand, knowledge base in form of classified-rules generated using decision tree is comprehensive, easier to interpret and to use.

II. Background

The first widely-used program for generating decision trees was "AID" (Automatic Interaction Detection) developed in 1963 by J. N. Morgan and J. A. Sonquist1. Written in FORTRAN and limited by the hardware of the time, AID was suitable only for small to medium size data sets, and it could generate only regression trees. AID was followed by many other decision tree generators including THAID by Morgan and Messenger in 1973 [2], and ID3 and, later, C4.5 by J. Ross Quinlan [5]. The theoretical underpinning of decision tree analysis was greatly enhanced by the research done by Leo Breiman, Jerome Friedman, Richard Olshen and Charles Stone that was published in their book Classification and Regression Trees. Much of their research was embedded in a program they developed called ―CART [5]. Learning systems based on decision trees are the easiest to use and to understand among all other machine-learning methods. The automatic construction of decision trees begins with the studies developed in the social sciences by Morgan and Sonquist (1963) and Morgan and Messenger (1973). The main difference among the various algorithms used, is the criterion followed to carry out the partitions of training samples. The See5 algorithm is the latest version of the ID3 and C4.5 algorithms developed by Quinlan. The criterion employed in See5 algorithm to carry out the partitions is based on some concepts from Information Theory [6]. The main idea shared with this algorithm is to choose a variable that provides more information to realize the appropriate partition in each branch in order to classify the training set. The advantages of decision tree classifier over traditional statistical classifier include its simplicity, ability to handle missing and noisy data, and non- parametric nature i.e., decision trees are not constrained by any lack of knowledge of the class distributions.

More advantages compared to parametric classification methods but in this also having disadvantages some information is lost in comprised time. These disadvantages are overcome by using Fuzzy Logic and Neuro-Fuzzy Logic. If we use fuzzy classifier, in all most all of the application areas, fuzzy gives more classifier accuracy when compared to legacy classifiers.

Fuzzy logic was invented by Zadeh [7] in 1965 for handling uncertain and imprecise knowledge in real world applications. It has proved to be a powerful tool for decision-making, and to handle and manipulate imprecise and noisy data. Another reason is that when to raise an alarm is fuzzy, more useful for classifier in the abnormal situations. There would be too many alarms if we raise an alarm every time we find an intrusion event. At what degree of intrusion we should raise an alarm often depends on different situation. Not only IDS in other areas also playing more important role in research now days. The term rule generation encompasses both rule extraction and rule refinement. Note that rule extraction here refers to extracting knowledge from the ANN, using the network parameters in the process. Rule refinement, on the other hand, pertains to extracting refined knowledge from the ANN that was initialized using crude domain knowledge. Rules learned and interpolated for fuzzy reasoning and fuzzy control can also be considered under rule generation. Although the focus is on neuro– fuzzy models, we also briefly deal with other fuzzy, neural, genetic algorithms, and rough set-based approaches to rule generation. Here concentrate on categorizing the different neuro–fuzzy approaches, based on their level of integration, in a unified soft computing framework. The concept of a type-2 fuzzy set was introduced by Zadeh [8] as an extension of the concept of an ordinary fuzzy set i.e., a type-1 fuzzy set. Mizumoto and Tanaka studied the set theoretic operations of type-2 fuzzy sets and properties of membership grades of such sets [9]; and examined type-2 fuzzy sets under the operations of algebraic product and algebraic sum [10].

III. Proposed Methodology

This paper proposes to improve the accuracy of the classification process, to reduce the amount of data needed for processing and to improve the false alarm rate by using the best rule-set using the Decision tree approach, Fuzzy Logic theory, and Neural Network and Neuro-Fuzzy classifiers with computing algorithm.

This methods explains the methodology followed during the research on classification based on the decision tree classifier and its various aspect related to the training size and pruning. Fig. 1 explains the conceptual flow chart of the full methodology. In Fig. 1, left side first black represented about the training data. In step in Fig. 2, is computing methodologies: Those are explained in below

1) Knowledge in the form of classification rules will be extracted from the training data by using the Decision Tree approach. Classification rules will then be applied to classify the new data identifies intrusion alarms. Create rule set 1 using advanced algorithms in decision tree methods, in my research part consternation on C4.5/SEE 5.0.
2) To implement rules set using Fuzzy Logic theory, Neural Network and compare with decision tree rule set. Fabricate greatest accuracy rule set2.
3) To construct rules set using neuro-fuzzy classifiers and compare with rule set 1 and 2. Stimulate best accuracy rule set.
4) Evaluation of Performance accuracy assessment of rule set1, set2 and best set. Final simulate automotive best set from Synthesis of the proposed classifiers for reduce the amount of data needed for processing and the false alarm rate.

Fig. 2, next two steps are testing on Defense Advanced Research Projects Agency (DARPA) [11] data set 1998, 1999 and 2000, conclude best automation process of the rule generation for IDS.

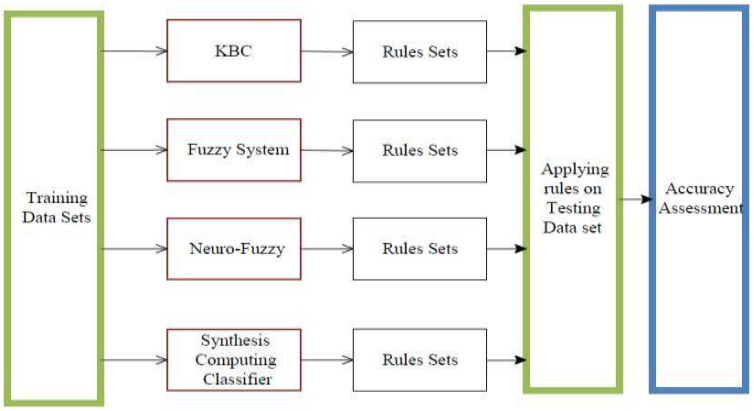

Fig. 2. Outline complete methodology.

The training dataset for the decision tree is different as it is non-parametric classifier. Decision tree was generated using See5 decision tree software. The main advantage of See5 is that it can convert a decision tree into classification rules. The decision tree generated from the DARPA data was then converted to classification rules to form a knowledge base. The knowledge base created from this process was then used in further classification of the IDS attackers' signature. Basically four types of classification were performed and one type novel process computing classifier:

1) Decision tree classifier
2) Fuzzy Logic theory
3) Neural Network
4) Neuro-Fuzzy classifiers
5) Synthesis Computing Classifiers

Finally the accuracy assessment was done for all the Classification methods using different standard metrics considering mainly the following parameters:

1) Classification rate of attackers
2) User accuracy
3) Procedure accuracy
4) Overall accuracy

Evaluation of the performance accuracy is assessment of rule set1, set2 and best set. Final simulate automotive best set from Synthesis of the proposed classifiers for reduce the amount of data needed for processing and the false alarm rate.

Final testing on Defense Advanced Research Projects Agency (DARPA) data set 1998, 1999 and 2000, conclude best automation process of the rule generation for IDS.

A. Test Data

The data set has 41 attributes and one class label. The actual total data full data set contains 743M uncompressed with lacks of records. Actual data set contains 22 attack types. Those attacks can be prominently divided into four groups [11]: Denial of Service (DoS), Unauthorized Access from A Remote Machine (R2L), Unauthorized Access to Local Super User (U2R) and Surveillance and Other Probing (Probing).

B. Decision Tree Classifier

Measures the information that is gained by partitioning T in accordance with the test X. The gain criterion isselects a test to maximize this information gain. The gain criterion has one significant disadvantage - it is biased towards tests with many outcomes.

The information generated by dividing T into n subsets is given by

$$\text{Split Info}(X) = \pm\Sigma i=1n\ |Ti|/|T|.\log2(|Ti|/|T|)$$

The proportion of information generated by the split that is useful for classification is:

$$\text{Gain ration} = \text{gain}(X)/\ \text{split info}(X)$$

Stratified random sampling methods were used to collect separate training and test data sets from actual KDD Cup data set. The data collected by random sampling were divided into two subsets, one of which was used for training and the other for testing the classifiers. Mainly attributes data types are continuous and symbolic. Symbolic means having some fixed values for attribute that means example attribute protocol type is symbolic it is having only tcp or icmp or udp not possible to allow other values. Here some attributes are Booleans but that attributes are also converted to symbolic, for example Is_host_login and Is_guest_login.

Using the training set samples created above, the classifier was built in the form of a decision tree. Fig. 3 shows the decision tree generated using See5 algorithm for specified in section A test data.

```
Read 179 cases (41 attributes) from mvsp.data

Decision tree:

num_file_creations > 0: u2r (30)
num_file_creations <= 0:
:...dst_host_same_src_port_rate > 0.49: Probing (30)
    dst_host_same_src_port_rate <= 0.49:
    :...num_compromised > 0: dos (48)
        num_compromised <= 0:
        :...src_bytes > 51: normal (38/1)
            src_bytes <= 51:
            :...srv_count <= 1: r2l (30)
                srv_count > 1: normal (3)
```

Fig. 3. Sample decision tree of the one TestCase.

Decision trees can sometimes be quite difficult to understand. To simplify a decision tree and convert them into rules, which are easier to understand and to implement, every path from the root to a leaf is converted to an initial rule by regarding all the test conditions appearing in the path as the conjunctive rule antecedents, while regarding the class label held by the leaf as the rule consequence. An important feature of See5 is its ability to generate classifiers called rule sets that consist of unordered collections of (relatively) simple "if then" rules. Fig. 4, Shows the rules of the Fig. 3 decision tree using See5 methodology.

```
Rules:

Rule 1: (48, lift 3.6)
        num_compromised > 0
        ->  class dos  [0.980]

Rule 2: (30, lift 5.8)
        dst_host_same_src_port_rate > 0.49
        ->  class Probing  [0.969]

Rule 3: (30, lift 5.8)
        src_bytes <= 51
        srv_count <= 1
        dst_host_same_src_port_rate <= 0.49
        ->  class r2l  [0.969]

Rule 4: (30, lift 5.8)
        num_file_creations > 0
        ->  class u2r  [0.969]

Rule 5: (38/1, lift 4.3)
        src_bytes > 51
        num_compromised <= 0
        num_file_creations <= 0
        ->  class normal  [0.950]

Rule 6: (35/1, lift 4.2)
        num_compromised <= 0
        srv_count > 1
        ->  class normal  [0.946]

Default class: dos
```

Fig. 4. Sample rules of the one TestCase.

Each rule consists of:

1) A rule number, which serves only to identify the rule. Statistics (*n*, lift *x*) or (*n*/*m*, lift *x*) that summarizes the performance of the rule
2) Similarly to a leaf, *n* is the number of training cases covered by the rule and *m*, if it appears, shows how many of them do not belong to the class predicted by the rule. The rule's accuracy is estimated by the Laplace ratio (*n*-*m*+1) / (*n*+2). The lift *x* is the result of dividing the rule's estimated accuracy by the relative frequency of the predicted class in the training set.
3) One or more condition that must all be satisfied if the rule is to be applicable.
4) A class predicted by the rule.
5) A value between 0 and 1 that indicates the confidence with which this prediction is made.

For each corresponding path from the root of a decision tree to a leaf, a separate classification rule is generated. There are chances that some redundant and undesirable rules are also extracted, therefore care should be taken to remove such rules which do not contribute in improving the accuracy of the classification. The following strategy was adopted to filter out the desired rules out all extracted rules: If only one rule is activated, which means the attribute values match the conditions of this rule, let the final class be the same as stated by this rule. If several rules are activated, let the final class be the same as stated by the rule with the maximum confidence. If several rules are activated and the confidence values are the same, then let the final class be the same as stated by the rule with the maximum coverage of learning samples. If no rule is activated, then let the final class be the same as stated by the default class.

If the split is near trivial, split information will be small and this ratio will be unstable. Hence, the gain ratio criterion selects a test to maximize the gain ratio subject to the constraint that the information gain is large. To investigate the effect of the size of training set on the accuracy of the classifier, different training samples of different sizes were prepared (Ex: 5000, 20000, 30000 samples etc).

C. Fuzzy Logic and Neuro-Fuzzy Classifiers Rule Sets

Mainly, decision tree classifier identifies only covered scaling attacker and not covered mixed attacker. Some attacker data set behavior is normal but that having outside scaling data set is abnormal. So, this type of the problem is not possible to identify using the decision tree classifier.

And plus using decision tree it is not able to cover all noise data. The Best method for solving the above problem is using the Fuzzy Logic. Because, fuzzy logic covers outside of normal data set and it is a generate rule set for different types scaling and none formal data sets.

IDS systems play a major role in security. So it is required to construct the best IDS. We need the best knowledge rule to classify the attackers or users, and attacks types. Having different attackers in the present world, enable identify using normal classifiers those attackers so required to construct IDS using best classifier rules set. So the best classifier rules set construct from the Fuzzy Rules Set comparatively tradition algorithms like Decision Trees.

For example, a simple general most popular example is

based on temperature and winds that action play or not play might look like this:

IF temperature="very cold" AND wind="high" THEN not play.

IF wind="normal" AND temperature ="cold" THEN play.

IF wind="very high" and temperature="normal" THEN not play.

IF temperature ="very hot" THEN not play.

There is no "ELSE" – all of the rules are evaluated, because the different degree is going validation is required at same time. Main components of the creating fuzzy decision tree: Set Patterns, Fuzzy Sets Defining, Fuzzy Reasoning and Fuzzy Decision Tree. Fig. 5 shows main components flow of the Fuzzy Decision Tree.

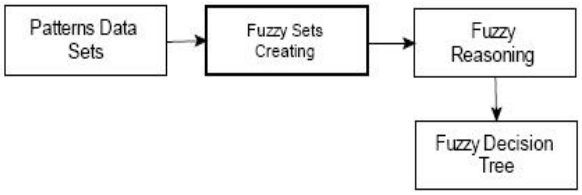

Fig. 5. Main components in construction of fuzzy decision tree.

Major parts in Fuzzy Decision Tree first step is Set Patterns in identify the patterns from the IDS data sets using the optimize profitability of the identified patterns. In my research using KDD data set for patterns. In second component of FDT to define fuzzy sets selection. For fuzzy sets defining, we use triangular fuzzy membership function corresponds to each patterns. In next fuzzy reasoning, we check that given fact for an antecedent in a fuzzy production rule does not match exactly with the antecedent of the rule, and then consequent can be drawn by using our proposed similarity-based fuzzy reasoning method. After fuzzy reasoning we construct fuzzy decision tree for training data. In the following sections these components are outlined in detail. [12].

Definition of the Fuzzy system in our research is characterized by a set of linguistic statements based on expert knowledge. Normal expert knowledge is shows in the rules. And Fuzzy Set D in I1 is characterized by an association function which is easily implemented by fuzzy conditional statements. For example, if the access member is true to some degree of association, then the subsequent is also true to that same degree.

Simple rules are following below statements:

If Num_Comromised<= 0 and Src_bytes>51 **then** Normal **Else** DOS attacks

If Num_Comromised<= 0 and Src_count>1 **then** Normal **Else** U2R attacks

In decision rule each rule is going final class but no one having the else case that means doesn't support association function ship and subsequent rules. In fuzzy classification system, sequence can be classified based on generation fuzzy rules. These fuzzy rules are based on the KDD data set attributes values. In each rule having weight like accuracy in chapter 3, value is in between of the 0 and 1 range.

Every rule has a weight, which is a number between 0 and 1, and this is applied to the number given by the antecedent. It involves 2 distinct parts. The first part involves evaluating the antecedent, fuzzifying the input and applying any necessary fuzzy operators.

Union: μ AUB (x) = Max[$\mu A(x)$, $\mu B(x)$]

Intersection: μ A$\cap$B(x)=Min[$\mu A(x)$, $\mu B(x)$]

Complement: $\mu\bar{A}(x)$=1- $\mu A(x)$

where μ is the association function.

The second part requires application of that result to the consequent, known as inference. To build a fuzzy classification system, the most difficult task is to find a set of fuzzy rules pertaining to the specific classification problem.

A Fuzzy Inference System (FIS) is a rule-based system that uses fuzzy logic, rather than Boolean logic, to reason about data. Its basic structure includes four main components:

1) A fuzzier, which translates crisp (real-valued) inputs into fuzzy values.
2) An inference engine that applies a fuzzy reasoning mechanism to obtain a fuzzy output.
3) A de-fuzzier, which translates this latter output into a crisp value.
4) A knowledge base, which contains both an ensemble of fuzzy rules, known as the rule base, and an Ensemble of membership functions known as the database.

The decision-making process is performed by the inference engine using the rules contained in the rule base. These fuzzy rules define the connection between input and output fuzzy variables.

In my part of the study, I propose four types of methods for construction of the Fuzzy Rules. Using Mean and the Standard Deviation of Attribute Values, based on histogram of Attribute Values, based on Simple Fuzzy Grid and based on Neuro-Fuzzy Approach.

Each Class having one single rule it's generating from the Fuzzy rules system. The fuzzy if-then rule for the k^{th} class can be written as

$$\text{If } x_1 \text{ is } A_1 \text{ and } \ldots \text{ and } x_n \text{ is } A_n \text{ then Class } k$$

where A_i is an antecedent fuzzy set for the *ith* attribute. The association function of A_i is defined as

$$A_i(x_i) = \exp\left[\frac{(x_i - \mu_t)^2}{2(\sigma_i)^2}\right]$$

where μ_i is the mean of the i^{th} attribute value x_{pi} of the Class k patterns, and σ_i is the standard deviation. Fuzzy if then rules for the two dimensional two class pattern classification problem are written as following.

The Association function of each antecedent fuzzy set is specified by the mean and the standard deviation of attribute values.

The main motivation of this approach is fuzzy systems by neural networks is based upon the inherent capability of neural networks to perform massive parallel processing of information. Because this very important feature in fuzzy controllers and more general, fuzzy expert systems that are required process large numbers of fuzzy inference rules in Instruction Detection Systems.

Another advantage of this approach gives high

performance accuracy in an implemented IDS hardware and also on other side this approach is most helpful because of fuzzy inference rules are processed in parallel, but in the first, second and third methods not having Parallel processed system. So that reasons those methods take time identifies attacker and accuracy is low compare with Neuro Fuzzy System. Hence this results in high computational efficiency which is crucial in many applications.

Actual Neuro-Fuzzy means arrangement of the artificial neural networks and fuzzy logic. It was proposed by J. S. R. Jang. Two types of possible arrangement in Neuro-Fuzzy systems are: First method is users sending inputs from the Fuzzy system or Fuzzy Interface to Neural Network system, NN system generate decisions, and NN system improves the performance using feedforward learning algorithm. And Second arrangement reverse of the first approach that means input data set submit to Fuzzy system through NN system and feedforward connect entire system, first method output system feedforward to only NN system but here feedforward inputs apply to Fuzzy system also.

Based upon the computational process involved in a Neuro-Fuzzy system, one may broadly classify the fuzzy neural structure as feed forward (static) and feedback (dynamic). A new hard Fuzzy-Neuro system is ARIC (Approximate Reasoning Based Intelligent Control) architecture**.** It is a neural network model of a fuzzy controller and learns by updating its prediction of the physical system's behavior and fine tunes a predefined control knowledge base.

The system is able to learn, and the knowledge used within the system has the form of fuzzy IF-THEN rules. By predefining these rules the system has not to learn from scratch, so it learns faster than a standard neural control system.

In my research, proposed ARIC method in IDS, because it's more support to run continuously without human supervision, very automated based on IDS physical system. And proposed system learn itself new knowledge and identified new patterns attackers and doesn't required supervisors guide lines. And performance very high, most intelligent system, because its combination of the NN and Fuzzy systems.

The ARIC system consists of two Feed-Forward neural network systems, the Action-state Evaluation Network (AEN) and the Action Selection Network (ASN).

The ASN is a multilayer neural network representation of a fuzzy controller. ASN main function is receives the current system state x as its input and computes a recommended action F. The AEN also receives the system state and measure state goodness.

ASN determines an action based on the system's state. It is a fuzzy logic controller (FLC) represented as a neural network, using nodes and weighted connections.

The Action-State Evaluation Network (AEN) is a neural network that evaluates state of the system. This evaluation is called prediction of reinforcement, u. It's used to produce the internal reinforcement, $\hat{r}$.

The AEN has three layers of neurons as shown in below Figure. It has $n=n_1+1$ input neurons, h hidden neurons and one output neuron. The input to the network is a vector containing the n_1 system states plus a constant bias x_0. By using a bias we add a number of extra weights to the network. It is a feed-forward neural network with One hidden layer, which receives the system state as its input and error signal r from the physical system as additional information. The output u [t, t`] of the network is viewed as a predication of future reinforcement that depends of the weights of time $t$ and the system state of time $t$`, where t` may be t or t+1. Better states are characterized by higher reinforcement. The weight changes are determined by a reinforcement procedure that uses the output of the ASN and the AEN. The ARIC architecture was applied to cart-pole balancing and it was shown that the system is able to solve this task.

D. Synthesis Computing Classifiers

Classification done using such knowledge is known as knowledge base classification. But such classification needs strong knowledge base, which sometimes become drawback of this process because of the knowledge acquisition process. Generally knowledge base is created with the help of knowledge acquired by interacting with the experts. The traditional way of knowledge acquisition is that the knowledge engineer interacts with the corresponding domain expert; write up his /her experience and knowledge in a interpretable form and then feed the entire acquired knowledge in the computer in a symbolic form such as if-then rules [13], [14].

If-then rules are generate from different methods of the classifiers, but each method having own advantages and disadvantages, here problem building of the better rule system comparing with all. In building process one method is not sufficient for build better system. Then using combination of the different computing methods for build batter knowledge and identify the attacker using the knowledge. Here very important rule bounder, rule is false or true that's depends on rule bounder. Construction rules with better bounder with combination of the different rules, different rules from the different classifiers.

Mainly motivation of the proposed method is decision boundaries are not always clear cut. That is, the transition from one class in the feature space to another is not discontinuous, but gradual. This effect is common in fuzzy logic based classification algorithms, where membership in one class or another is ambiguous. Based on the discussed problem here required construct better rules set for classification of the attackers.

Fuzzy Decision Boundary: Final testing accuracy parameters identify the best approaches generation for rule construction. Next step explain build of the best rules for identify attackers.

Common Rule Set Generation: An information system is a pair A= (U, A) where U is a non-empty, finite set called the Universe and A – a non-empty finite set of attribute. Elements of U are called objects and interpreted eg: any variable, rule character etc... Here consider a special case of information system called decision table. A decision table is an information system of the form

$$A = (U, A \cup \{d\})$$

where d set not in A is a distinguished attribute called the

decision

Strength of Rule Set: Next step in common rules set, after using above approximation algorithm also even having some conflict using rules that's means set rules related to the common class. Main about rule weight discussed in chapter 3, but that's covered only for single decision tree, that's not possible applicable in this section (common rules set).

W= (*W, A* U {*d*}) is a universal decision rules.

A = (*U, A* U {*d*}) is a given different decision classifier table rules ut Є W is a tested object.

Rul (*Xj*) is a set of all calculated basic decision rules for *A*, classifying objects to the decision class *Xj*

MRul (*Xj* ,*ut*) sub set equal Rul (*X*j) is asset of all decision rules from Rul (*Xj*) matching tested objects ut .

Defined and used server measures for the rule set MRul(*Xj, ut*) depending on the number of rules from this set matching tested objects, the number of objects supporting decision rules from this set and the stability coefficient of rules.

IV. Performance Analysis

Divide accuracy three type based error matrix calculations: Overall Accuracy**,** Producer's accuracy and User's accuracy.

In our motivation comparatively accuracy can't reach better accuracy using exist model. That's reason construct best rules set from collect rules different classifier models. Here used approximation algorithm for better rules set construct from the common rules sets and order for rules set application propose defined each rule strength. Based on better rules set and rank of the rules set applied that rules set on tested data set, reach accuracy 98% comparatively other model very more, here consider training data set is 1500, samples of the records. And based on this model found the new attacks types in KDD system.

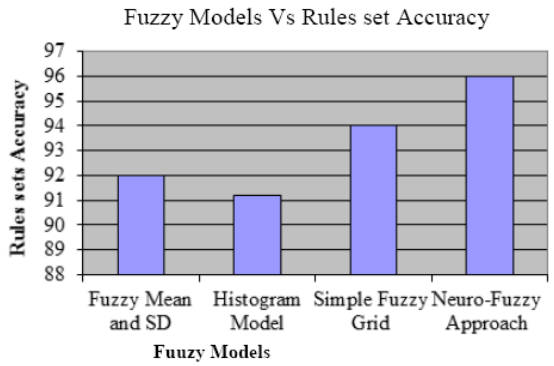

Fig. 6. Accuracy for two data sets.

Fig. 6 shows the accuracy of the all classifiers generated using different training set sizes on the test cases. In Fig. 6, following showing in X-axis Decision tree, Fuzzy, Neuro-Fuzzy and Synthesis Computing Classifiers

The proposed model support not only Intrusion detection system, its applicable in so many decision Applications. Decision applications place more role in real time situations major in medical, image classification, share market, business decisions etc.

Image classification application decision rules are crates good knowledge for classification images. Image classification is a particular case of Pattern Recognition. The overall objective of the classification process is to automatically classify all pixels in an image into land cover classes based on the predefined classification model. The term pattern in case of image classification refers to the set of radiance measurements obtained in the various wavelength bands for each pixel.

There are numerous classification algorithms. Classifiers are described under broad categories such as supervised and unsupervised classifiers, parametric and non-parametric, knowledge base classifiers and NN etc.

This proposed method useful for classification mixed orientated pixel and useful for highest classification accuracy.

Medical application area also used decision making knowledge in form of rules. Construct rules using proposed model its gives more accuracy and takes less time to compute the problem. And same time it's covered some conflict decision problem. Almost all decision problem application covered proposed model.

V. Conclusion

IDS more important in network origination, in that system main building of the knowledge very important for classify the attackers. The knowledge defines in terms of the rules set. A rule set construct and classify the rules set definition is very important in IDS.

The accuracy assessment of the rules set construct using Knowledge Base Classification or decision tree, fuzzy classifier, neuro-fuzzy classifier and syntheses computation classifier is emphasized in the study. The KBC produced 76 % and 78% of overall accuracy. This is due to bounder of the decision tree is scaled so that reason, unable identify more misclassified attackers.

In same process used the histogram of attribute values based method overall accuracy is produced 88.6 % for both data sets, comparatively first fuzzy process method that's means mean and standard division model little bit more accuracy but its take more complexity for construct the design of this method comparatively first method.

And next method in fuzzy process is Simple Fuzzy Grid method gives more accuracy comparatively first and second method, this method produced accuracy is 92% and 93% of the test data sets in different levels. Main difference between with other methods it's covered in simple grid of the each rules so that's reason it's produced more accuracy comparatively other two method in process of the fuzzy system.

Final method of the fuzzy system used neuro-fuzzy method, this method produced accuracy is 94% and 95% for different data sets. Comparatively fuzzy process four methods best accuracy is neuro-fuzzy system, because its work different layers neurons used in construct rules set.

In model and proposed model is Syntheses computing classifier, this method produced ultimate accuracy produced is 98% both different data sets. In this method used common rules set construction that reason this method consider better rules from the all above methods and add another important rules set generation type-2 fuzzy system. And this method

gives each rule had strength. So that reason order of the classification rules very easy in common rules set. Otherwise it's produced less accuracy comparatively exist accuracy.

Finally results demonstrate that Syntheses computing classifier surpasses other classification methods. Syntheses computing classifier method gives more accuracy in all other decision rule set making applications.

Current study only mixed of the few classifier generate synthesis computing classifier used more other method with different styles. And used different approximation for contract common rules set and compares the accuracy. Same apply the different application domains compare helpful identify the domain best domain identification this method. So many possibilities are there for extended of the proposed model.

REFERENCES

[1] U. M. Fayyad, G. P. Shapiro, P. Smyth, and R. Uthurusamy, *Advances in Knowledge Discovery and Data Mining*, AAAI/MIT Press, Menlo Park, CA, 1996, ch. 6, pp. 62-83.

[2] E. M. Hassib, A. Osman, A. Elgwad, and A. I. Saleh, "A hybrid intrusion prevention system for web database security," *International Journal of Engineering Science and Technology*, vol. 2, no. 7, pp. 2745-2762, July 2010.

[3] M. Cramer *et al.*, "New methods of intrusion detection using control-loop measurement," in *Proc. Technology Information Security Conference*, May 1995, pp. 1-10.

[4] L. Fu, "A neural network model for learning rule-based systems," in *Proc. International Joint Conference on Neural Networks*, June 1992, pp. 343-348.

[5] M. Pal and P. M. Mather, "Decision tree based classification of remotely sensed data," presented at 2011 Asian Conference on remote sensing, Singapore, Nov. 5-9, 2001.

[6] J. R. Quinlan. Data mining tools See5 and C5. [Online]. Available: http://www.rulequest.com/see5-info.html.

[7] D. Dubois and H. Prade, *Fuzzy Sets and Systems: Theory and Applications*, Academic Press, Inc., New York, 1980, ch. 2, p. 393.

[8] J. Nieminen, "On the algebraic structure of fuzzy sets of type-2," *Kybernetica*, vol. 13, no. 4, pp. 261–273, Oct. 1977.

[9] N. N. Karnik and J. M. Mendel, "Applications oftype-2 fuzzy logic systems: handling the uncertainty associated with surveys," in *Proc. FUZZ-IEEE 99*, August 1999, pp. 327-348.

[10] Q. Liang and J. M. Mendel, "Interval type-2 fuzzy logic systems: theory and design," *IEEE Trans. Fuzzy Systems*, vol. 8, no. 5, pp. 535-550, Oct. 2000.

[11] Intrusion Detection Systems. [Online]. Available: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html.

[12] S. Peddabachigari, A. Abraham, and J. Thomas, "Intrusion detection systems using decision trees and support vector machines," *International Journal of Applied Science and Computations*, vol. 76, no. 16, pp. 1-6, June 2004.

[13] K. L. Fox, R. R. Henning, and J. H. Reed, "A neural network approach towards intrusion detection," in *Proc. the 13th National Computer Security Conference*, October 1990, pp. 421-432.

[14] L. Fu, "A neural network model for learning rule-based systems," in *Proc. the International Joint Conference on Neural Networks*, June 1992, pp. 343-348.

M. V. Siva Prasad is the principal of Anurag Engineering College who is a renowned educationist, engineer and administrator. He was born at Khammam, A. P., India in 1970. He received B.E. [CSE] degree from Gulbarga University, M.Tech. [SE] degree from VTU, Belgaum and he was awarded Ph.D degree from Nagarjuna University, Guntur. He worked in various engineering colleges in different capacities and attained 20+ years of experience. He guided various projects at UG & PG level and published 10 no's international and national journals.

He has over 20 years of academic and administrative experience. He attended numbers of conferences/seminars/ guided various projects at UG and PG Level and published number of papers in international & national journals. He is a life member of ISTE M.No. : LM 53293 / 2007. Besides, he has been recognized as one of the most authoritative voices in the area of network security. His expertise has been heavily utilized by many institutions in AP and assumed charge as principal of Anurag Engineering College from Nov. 2012.

Ravi Gottipati is a senior software engineer in Tripod Technologies, who was born at Narasaraopet, A. P, India in 1985. He received B.E. [CSE] degree from JNTU, M.Tech. [CSE] degree from OU. He worked as an IT consultant and assistant professor in CBIT, Hyderabad. He guided various projects at UG & PG level and published 7 no's international and national journals.

He has over 5 years' experience of research, IT and teaching. He attended number of conferences/seminars/ guided various projects at UG and PG Level and published numbers of papers in international & national journals. He has good experience in big data and data pattern mining in computing methodologies.