Particle Swarm Optimization For Adaptive Anomaly-Based Intrusion Detection System Using Fuzzy Controller

K.Kavitha M.C.A., B.Ed.[1], S.Ranjitha Kumari M.Sc., M.Phil.[2]

[1] *Mphil Scholar, Department of Computer Science, R.V.S College of Arts & Science,Coimbatore. Tamil nadu, India*

[2] *Assistant professor, Department of Computer Science, R.V.S College of Arts & Science,Coimbatore, Tamil nadu, India.*

Abstract— **The major work of intrusion detection systems is used to detect the anomaly and new attackers in the networks, even still various false alarms are caused in order to neglect this necessary feature. Existing system present an anomaly-based intrusion detection system to improve the system performance. Fuzzy rule-based modeling and fuzzy controller are used to create a detection model in the training phase and update this model in the test phase respectively. After that, system user verifies these decisions and fuzzy controller tunes detection model using system user's feedbacks. To improve the accuracy of detect the anomaly in the system. The proposed system is mainly concentrate on finding the optimum membership functions of a fuzzy system using particle swarm optimization (PSO) algorithm. The proposed algorithm it is used to optimize the Gaussian membership functions of the fuzzy model system. It is clearly proved that the optimized membership functions (MFs) provided better performance than a fuzzy model for the same system, when the MFs were heuristically defined.PSO has no evolution operators such as crossover and mutation.**

Keywords— **Adaptive anomaly-based intrusion detection, fuzzy-rule based modeling, fuzzy control, PSO.**

I. Introduction

MANET is a group of mobile nodes without requiring centralized administration or fixed network infrastructure, In this network through cooperatively forwarding packets , nodes can communicate with other nodes out of their direct transmission ranges. They communicate through wireless connections. Due to the lack of infrastructure, resource constraints of mobile devices, shared wireless medium, node mobility, and bandwidth limitations, Security designs for mobile ad hoc networks are complicated. Development of dynamic routing protocol is the major challenges in the design of an ad-hoc network which efficiently finds a route between mobile nodes.

For basic network functions like packet forwarding and routing security in MANETs is an essential component. These operations can be easily compromised when countermeasures are not embedded into basic network functions at the early stages of their design. This deviation is at the core of the security problems which are specific to ad hoc networks.

Among various attacks, routing attacks have received considerable attention since it could cause the most devastating damage to MANET. This is because of the dynamic nature of network infrastructure.

In this research HADOF and Secure Routing uses Trust Levels (SRT) has been proposed. Secure Routing uses Trust Levels (SRT) scheme in Node transition probability (NTP) protocol provides secure routing in mobile ad hoc networks .To defend against routing disruptions in mobile ad hoc networks, HADOF mechanism has been implemented.

In SRT scheme the nodes in the network fall into one of the three lists. Based on the degree of trust these lists are classified as ally list, associate list and acquaintance list. The trust calculation process involves grouping of nodes in the network which is based on the parameter called Trust rate (T_{rate}). The nodes in a specific security level are made active for routing depending on their trust value based on the level of security needed for the data, Then to detect and punish malicious nodes, and improve network performance HADOF has been implemented. For each node malicious nodes may submit false report, the next mechanism is to keep a cheating record database for the other nodes. This node will be excluded from the future routes, and its packets will not be forwarded by other nodes as punishment once the node is detected as dishonest.

II. RELATED WORK

In [1] proposed a framework for holistic approach to network security. It includes intrusion detection system to identify the malicious attacks and to evaluate the effects of undetected attacks. To integrate intrusion detection with the survivability analysis to provide a complete view of network security. Based on the neural networks, that uses genetic algorithms to develop an intrusion detection system. Develop a model for probabilistically predicting the state of the system. The hybrid model tracks the complete sequence of events linked with a network intrusion or attack. The hybrid model has the potential to direct to a Decision Support System (DSS) that could facilitate systems managers make more informed decisions about the IDSs for their sites and about the kind of protection their systems . The main feature of this method is that learning is done through the data and does not use predefined learning method. So the learning process changes with the dataset, making the model more adaptive.

In [2] proposed a prototype intelligent intrusion detection system that uses the fuzzy logic and genetic algorithms to show the effectiveness of data mining techniques. This method merges both using fuzzy data mining techniques anomaly based intrusion detection and misuse detection using traditional rule-based expert system techniques. The anomaly-based components seem for deviations from stored patterns of usual behavior. The misuse detection components look for previously explained patterns of behavior that are likely to specify an intrusion. The inputs used in this system are network traffic and system audit data. By using the genetic algorithms the membership functions are tuned to enhance performance. To select the set of features available from the audit data that offers the most information to the data mining component.

In [3] proposed Fuzzy Intrusion Recognition Engine for the network security. This method is an anomaly-based intrusion detection system that utilizes fuzzy logic to evaluate the malicious activity on a network. To process the network input data it utilizes the simple data mining techniques and help expose metrics that are predominantly important to anomaly detection. These metrics are then estimated as fuzzy sets. FIRE relies on fuzzy network traffic profiles as inputs to its rule sets. While FIRE is not exclusively a network-based detection system. The main objective of the FIRE is how fuzzy systems are used in the intrusion detection system. To recognize the data sets that is more suitable for fuzzy intrusion detection systems. To minimize the size of the input data sets we combine the input data with data mining techniques. By choosing the features that highlight anomalies, fuzzy logic can be an effectual means of defining network attacks.

In [4] proposed integrated intrusion detection system by using the soft computing. In this method, we consider Intrusion detection as a data analysis process. By introducing high level of generality when deploying the subset of the most important features of the dataset, we achieve high detection rate. B using the feature selection process it is possible to decrease the number of input features significantly which is very important due to the fact that the Radial Basis Function networks can efficiently be prevented from over fitting. The Genetic algorithm exploits only the eight most relevant features for each attack category for rule generation. The created rules signal an attack as well as its category and it is end for training to RBF network. To examine the attacks, the optimal subset of features combined with the generated rules can be utilized.

In [5] proposed adaptive anomaly detection system is used to detect the security attacks. Without a priori knowledge of the underlying non-stationary data distributions, this method employs unsupervised evolving connectionist systems to find out system, network or user behavior. This adaptive anomaly detection framework completes one-pass clustering of the input data stream that symbolizes a monitored subject’s behavior patterns. Each new incoming instance is allocated to one of the three states: normal, uncertain and anomalous. Two different alarm levels are defined to reduce the risk of false alarming. Based on the Fuzzy Adaptive Resonance Theory and Evolving Fuzzy Neural Networks, we evaluate the anomaly detection system. This anomaly detection method significantly reduced the false alarm rate.

In [6] Proposed Traditional intrusion detection systems to identify the attacks in the wireless networks. This method focus on network anomaly detection, which is effectively the machine learning problem of modeling normal network traffic from training set. This anomaly detection method is vary from the classical classification task in machine learning because only one class exists in the training data. Firstly, it is nonstationary, modeling probabilities based on the time since the last event rather than on average rate. This avoids alarm floods. Secondly, the IDS learns protocol vocabularies in order to identify unknown attacks that challenge to develop implementation errors in poorly tested features of the target software.

In [7] proposed Incremental Hybrid Intrusion Detection to detect the intrusions. This method combines both incremental misuse detection and incremental anomaly detection. To improve the intrusion detection with high detection rate, , with the ability of detection new unknown attacks, and continually adapt model to cope with new network behaviors. Whenever the intrusion detection dataset is so large the entire dataset is not loaded into the main memory. So, the original dataset is divided into several subsets, and then the detection model is vigorously customized according to other training subsets after the detection model built on one subset. Based on the incremental learning, we use hybrid intrusion detection system. Compare to other frameworks this method uses ensemble of weak classifiers usually possesses lower computational complexity which using strong classifier, because of using weak classifier with suitable parameter to satisfy weak hypothesis.

In [8] proposed a novel intrusion detection system based on the integration of a few soft computing methods including neuro-fuzzy, fuzzy and genetic algorithms. The main work in the intrusion detection system is to build a classifier that can classify the normal and intrusive event data from the original dataset. ANFIS as an Adaptive neuro fuzzy inference system based on the target system sample data; it has the capability to create models solely. This ability among others qualifies ANFIS as a fuzzy classifier for intrusion detection. To classify the activities in the network, several neuro-fuzzy classifiers use extracted features of the audit data. Based on the outputs of the classifiers of previous layer the fuzzy inference system makes the final decision on whether the current activity is normal or intrusive. At last, genetic algorithms are used to optimize the structure of fuzzy sets of the fuzzy decision-making engine.

III. PROPOSED WORK

A. *Intrusion Detection System*

The architecture is composed of four main components it shown in Fig.1: Generate Detection Model, an IDS Engine, a Fuzzy Model Tuner and a Buffer. Generate Detection Model is responsible for creating a detection model. The model consists of a number of fuzzy rules that each one has a prediction confidence ratio. IDS Engine classifies test records by using this model. After that, test classification results and parameters that are required for updating the detection model are stored in the Buffer. System user verifies test results that have a predefined delay and sends these verified results to the fuzzy model tuner. Fuzzy model tuner employs parameters needed for updating and verified results to update the confidence prediction ratio of effective rules in test sample's classification. Fix delay means if a test record was arrived at t, the model is updated at t+delay using fuzzy controller.

1. *Generate Detection Model*

Fuzzy rule-base is used to generate detection model. In order to utilize this model, identifying fuzzy set of each input feature and trust rules are requested. The first problem is determining fuzzy sets. Some of the features have numeric values such as duration and src-bytes while others have symbolic values such as service and protocol. FCM is used to obtain fuzzy sets of features with numeric values. In addition, the number of clusters is considered to be equal to six. In order to ensure that the number of clusters is sufficient, we used subtractive clustering method, which is a fast one-pass algorithm for estimating the number of clusters and cluster centers. The number of estimated clusters for each numeric feature is less than six by this algorithm, so we have used number six as the number of clusters for each numeric feature. Total possible values for features with symbolic values are considered as fuzzy sets. Each value is belongs to only one fuzzy set. In fact its membership value in that fuzzy set is one, while in the other fuzzy sets this value is zero.

Finding the best and most confident rules is the second problem. A genetic algorithm approach is used to find the best and trustable rules. In this area, there are two learning approaches called Pittsburgh and Michigan. In this paper, the second approach is used. Inside of each rule, five fuzzy terms are appeared and "is" or "is not" can be included in each term. Genetic algorithm is ran separately for each normal and attack class. Meanwhile learning normal rules, normal class is the considered class and attack class is the opposite one and vice versa.

We followed the laws with the highest prediction confidence ratio in addition we are able to classify the greatest number of considered class correctly by adjusting following function as the fitness function

$$FitFunc = \frac{CCI_c}{CCI} * \frac{SC}{SC + 1.5 * WC}$$

CCI is the abbreviation for Considered Class's Instances and SC is Successfully Classified and WC is the abbreviation for Wrong Classified.

The first term is used to classify maximum percentage of considered class's instances correctly (CCIC). The second term is employed in order to achieve rules with highest prediction confidence ratio for this purpose; we multiplied wrong classified by 1.5. This action leads to finding more confident rules.

Considered instances of classes with compatibility higher than 0.5 and instances of opposite class with compatibility less than 0.5 are successfully classified (SC) samples and those of opposite class with compatibility higher than 0.5 are wrong classified samples. Compatibility of each training sample $x=(x_1,x_2,\dots x_n)$ with the rule r is calculated. S is the feature set that is available in the rule, F is the fuzzy set of each feature and μ is the membership function of each fuzzy set.

Find best membership function for each and every fuzzy set by tuning the membership values in the data using optimization methods. In this paper proposed a PSO with fuzzy membership function to tune the values in the dataset. The PSO optimization technique is a stochastic search through an n-dimensional problem space aiming the minimization (or maximization) of the objective function of the problem. PSO is a population-based technique and each individual of the population has an adaptable velocity (position change), according to which it moves in the search space. Moreover, each individual has a memory, remembering the best position of the search space it has ever visited. Thus, its movement is an aggregated acceleration towards the best individual of a topological neighborhood. From the results proposed for finding the optimum membership functions of a fuzzy system using particle swarm optimization (PSO) algorithm is shown in Fig.2.

The algorithm process in the following manner:

(1)Each individual particle i is considered as membership function $\mu_{F[n]}$ has the following properties

(2)A current position in search space, x_{id}, a current velocity, a personal best position in search space, p_{id}

(3)The personal best position, p_{id}, corresponds to the positionin search space where particle I presents the smallest error as determined by the objective function minimization task.

(4)The global best position marked by represents the position yielding the lowest error amongst all the p_{gd}

During the iteration every particle in the swarm is updated using the following two equations:

$$V_{id}(t+1) = W.V_{id}(t) + c_1 r_1 (p_{id} - X_{id}(t)) + c_2 r_2 (p_{gd} - X_{id}(t))$$

$$X_{id}(t+1) = X_{id}(t) + V_{id}(t+1)$$

Where $V_{id}(t+1)$ and V_{id} (t) are the updated and current particles velocities, respectively, X_{id} (t + 1) and X_{id} (t)the updated and current particles positions. C_1 and C_2 are two positive constants and r_1 and r_2 random numbers within the range [0,l]).

These particle dimensions represent fuzzy membership function parameter values. The first column shows the input and output variables. In this column, number represents the input variable. Basic integration of this hybrid algorithm. The assumptions are listed as below:

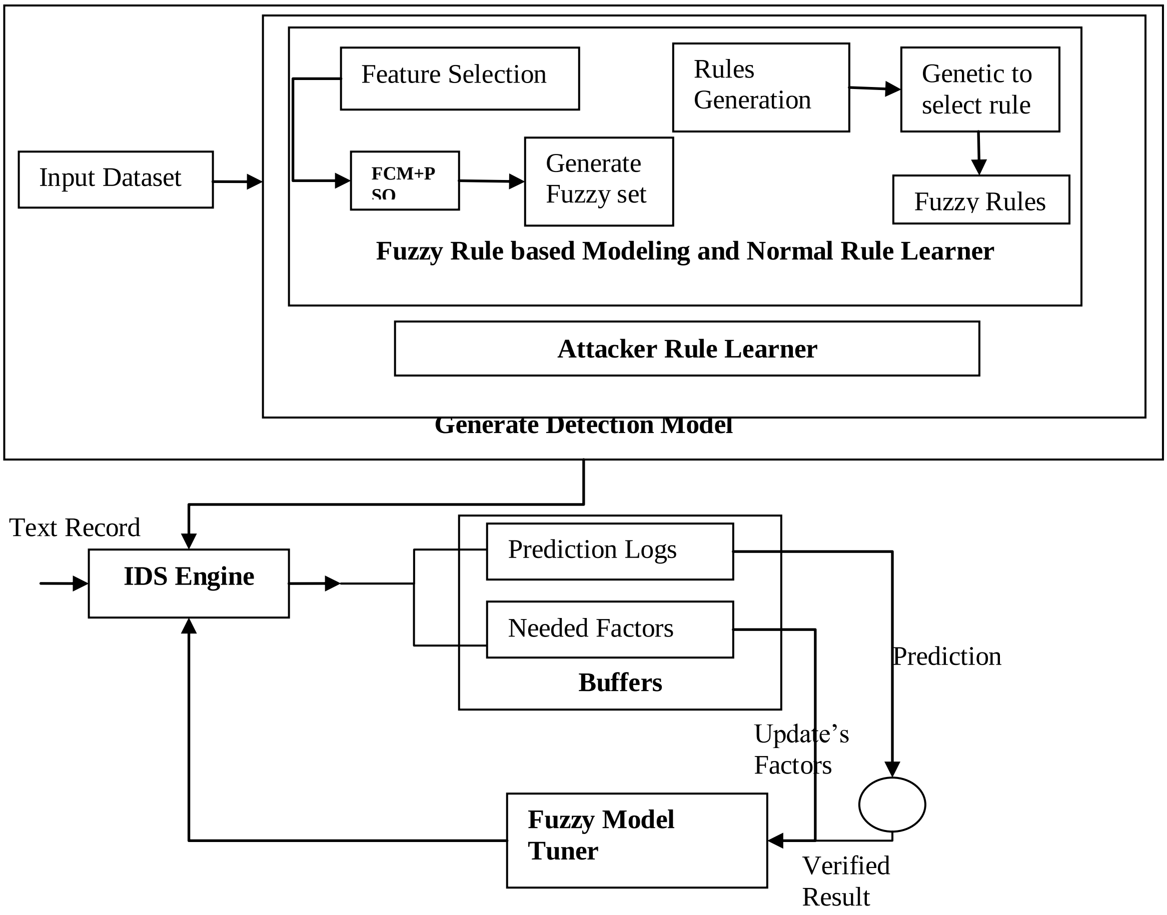

Fig.1. PSO with Fuzzy based anomaly detection

These particle dimensions represent fuzzy membership function parameter values. The first column shows the input and output variables. In this column, number represents the input variable. Basic integration of this hybrid algorithm. The assumptions are listed as below:

(i) Gaussian membership functions were used for input and output variables.

(ii) Complete rule-base was considered. A rule considered complete when all possible combinations of input membership functions of all the input variables participate in fuzzy rule-base formation.

The integration between optimization logic problems is as follow:

(i)The parameters are the mean value and standard deviation of each fuzzy membership function $\mu_{F[n]}$.

(ii) These parameters act as particles and looking for the global best fitness.

(iii) It starts with an initial set of parameters.

(iv) After the parameters had been adjusted using optimization method, this parameter will be used to check the performance of the fuzzy logic.

(v) This process is repeated until the goal is achieved.

After the step 5 is completed then return the membership function results that is $\mu_{F[n]}$

$$Com(x, r_i) = {}_{n=1}^{n=5}\min\left(\mu_{F[n]}(x_{S[n]})\right)$$

Prediction confidence ratio (PCR) of each rule is calculated. A suggested rule can be inserted in the rule set, if and only if it has a confidence ratio higher than 50 percent.

$$PCR(r_i = \frac{SC}{SC + WC})$$

Using Michigan approach, after each iteration instances that are covered by the taught rule are removed from the training dataset. Removing training instances gradually reduces the degree of credibility of rules, because deleted instances could not be measured by subsequent rules. So we have determined more difficult conditions to remove one instance from training set. Only considered class's instances with compatibility higher than 0.5 and opposite class's instances with compatibility less than 0.3 with the taught rule are removed from training set.

2. IDS Engine

The IDS engine employs the detection model to classify test samples. Each test sample is given to normal and attack rules. Calculates the instance membership value for each category.

Finally, the test sample belongs to the category with the highest membership value. We have also considered equal number of rules for each category. In the following formula, C is a normal or attack classes and n is the number of learned rules in each class.

$$M_c(x) = \sum_{i=1}^{5} Com(x, r_i) * CF_i$$

Since the number of rules in each normal and attack class is equal, M_c could be used without worrying about correctness of this decision formula.

3. Buffers

Prediction logs and compatibility of test samples with each rule are buffered. The system administrator monitors the prediction class of each test record with a predefined delay. He verifies this prediction and reports to the fuzzy model tuner module. We should also consider that the related record is deleted after employing each tuning.

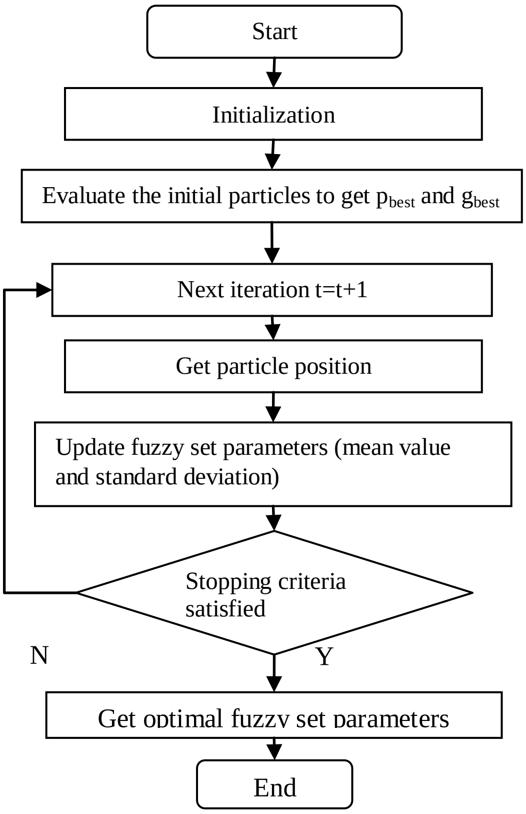
Start
Initialization
Evaluate the initial particles to get p_{best} and g_{best}
Next iteration t=t+1
Get particle position
Update fuzzy set parameters (mean value and standard deviation)
Stopping criteria satisfied
N
Y
Get optimal fuzzy set parameters
End

Fig.2. Flowchart of Particle Swarm Optimization to adjust Fuzzy Membership Function

4. Fuzzy Model Tuner (Fuzzy Controller)

Without updating the static detection model, it is not feasible to reach the total accuracy of higher than 85 percent. For this reason and due to existing new attacks in the test dataset, the learned model is tuned using a fuzzy controller. Moreover, fuzzy controller determines adaptation intensity. In order to decide about the class of a test sample, we have employed the results of available rules for both normal and attack classes.

IV. EXPERIMENTAL RESULTS

As mentioned before, due to changes in normal behavior of the network and appearance of new attacks, using the static model for intrusion detection systems is not relevant. Here we have improved the performance of detection by updating the detection model substantially. This section describes the experimental result obtained for Proposed PSO based Fuzzy system. To compare the results with PSO based Fuzzy system andFuzzy system as Shown in Fig 3.

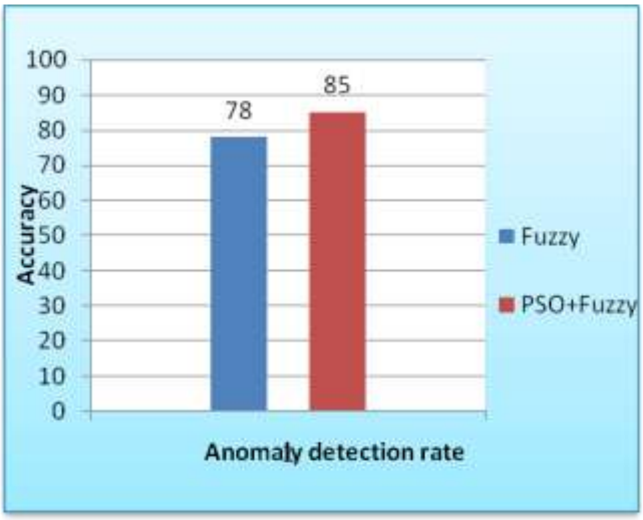

Figure 3: The performance of PSO based Fuzzy vs. Fuzzy System

V. CONCLUSION AND FUTURE WORK

Anomaly based intrusion detection systems are provided in order to protect computer networks against novel attacks and improve network security. These systems perform intrusion detection by comparing current network traffic with a behavioral model of normal network activity. As the pattern of network traffic changes over time, static models are not appropriate to monitor malicious activities. As the static models could be tuned with respect to changes in traffic pattern, adaptive models are used in this manner. In this paper, we have presented an PSO based Fuzzy for anomaly dection in intrusion detection system.

A whole new membership function successfully adjusted from standard fuzzy membership function. It could be done with representation of fuzzy membership function value as particles. The particle represent will be changes to reach the optimal value for each iteration using optimization method. The fuzzy membership function will be shrinks, move or expand through the changes of each value. Based on result experiment, the PSO+ Fuzzy has adjusted fuzzy membership function and improved the performance result in term accurately to destination and faster in speed of convergence. PSO+Fuzzy rule-based modeling is used to create the detection model. In addition, prediction results are delivered to system user for verification. Fuzzy controller module uses verified results in order to tune the detection model.

To improve the accuracy for detect the anomaly in the intrusion detection system we extend our work with Genetic algorithm.

REFERENCES

[1] T. Bhaskar, N. Kamath and S.D. Moitra, “A hybrid model for network security systems: Integrating intrusion detection system with survivability,” International Journal of Network Security, vol. 7, no. 2, pp. 249–260, 2008.

[2] S. M. Bridges and R. B.Vaughn, “Fuzzy data mining and genetic algorithms applied to intrusion detection,” Proceedings of the National Information Systems Security Conference, Baltimore, MD, pp. 16-19, 2000.

[3] John E. Dickerson and Julie A. Dickerson, “Fuzzy network profiling for intrusion detection,” Proceedings of NAFIPS 19th International Conference of the North American Fuzzy Information Processing Society, pp. 301–306, Atlanta, USA, July 2000.

[4] S. S. Kandeeban and R. S. Rajesh, “Integrated intrusion detection system using soft computing,” International Journal of Network Security, vol. 10, no. 2, pp. 87-92, 2010.

[5] Y. Liao, V. R. Vemuri and A. Pasos, “Adaptive anomaly detection with evolving connectionist systems,” Journal of Network and Computer Applications, vol. 30, pp. 60–80, 2007.

[6] M. V. Mahoney, P. K. Chan, “Learning non-stationary models of normal network traffic for detecting novel attacks,” Proceedings of the Eighth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, Edmonton, Canada, pp. 376–385, 2002.

[7] Rasoulifard, A. Ghaemi, and M. Kahani, “Incremental hybrid intrusion detection using ensemble of weak classifiers,” Advances in Computer Science and Engineering: 13th International CSI, Iran, pp. 577-584, March 2008.

[8] N. Toosi and M. Kahani, “A new approach to intrusion detection based on an evolutionary soft computing model using neuro-fuzzy classifiers,” Computer Communications, vol. 30, pp. 2201-2212, 2007.

.

.