Research Journal of Applied Sciences, Engineering and Technology 7(16): 3348-3355, 2014
DOI:10.19026/rjaset.7.680
ISSN: 2040-7459; e-ISSN: 2040-7467
© 2014 Maxwell Scientific Publication Corp.
Submitted: October 03, 2013 Accepted: November 21, 2013 Published: April 25, 2014

Research Article

An Adaptive Hybrid Multi-level Intelligent Intrusion Detection System for Network Security

P. Ananthi and P. Balasubramanie
Kongu Engineering College, India

Abstract: Intrusion Detection System (IDS) plays a vital factor in providing security to the networks through detecting malicious activities. Due to the extensive advancements in the computer networking, IDS has become an active area of research to determine various types of attacks in the networks. A large number of intrusion detection approaches are available in the literature using several traditional statistical and data mining approaches. Data mining techniques in IDS observed to provide significant results. Data mining approaches for misuse and anomaly-based intrusion detection generally include supervised, unsupervised and outlier approaches. It is important that the efficiency and potential of IDS be updated based on the criteria of new attacks. This study proposes a novel Adaptive Hybrid Multi-level Intelligent IDS (AHMIIDS) system which is the combined version of anomaly and misuse detection techniques. The anomaly detection is based on Bayesian Networks and then the misuse detection is performed using Adaptive Neuro Fuzzy Inference System (ANFIS). The outputs of both anomaly detection and misuse detection modules are applied to Decision Table Majority (DTM) to perform the final decision making. A rule-base approach is used in this system. It is observed from the results that the proposed AHMIIDS performs better than other conventional hybrid IDS.

Keywords: Adaptive neuro fuzzy inference system, classifier, decision table majority, intrusion detection system

INTRODUCTION

Due to rapid development of network-based services and responsive information on the networks, the number and the sternness of network-based computer attacks have been increased considerably. Even though an extensive range of security expertise such as information encryption, access control and intrusion prevention can shield their network based systems, there are still a lot of undetected intrusions are presented. Several traditional protection approaches like user authentication, data encryption, keep away from programming errors and firewalls are used as the initial line of protection for computer security. Suppose the password used by the user is weak and it is conciliation, the user authentication cant able to prevent unauthorized use. The firewalls are vulnerable to errors in pattern and expect to indistinct or indeterminate security policies (Summers, 1997). Hence, it is usually not capable to protect against malevolent mobile code, insider attacks and unprotected modems. The system became complex due to the un-avoidance of the programming errors also the application software is developing fast leaving at the back of some vulnerable weaknesses. Therefore, computer systems are possible to stay unsecured for the predictable future.

Intrusion detection system has been developed at 1980 to protect the computer threats by monitoring and surveillance which plays a more important role in many fields. Dorothy Denning's in John *et al*. (2000), said about "An Intrusion Detection Model," present a practical structure that is stimulated in many researchers and put down the foundation for commercial products such as discussed in this study. Still, in spite of considerable research and viable investments, ID technology is undeveloped and its usefulness is inadequate. Within its limits, it is useful as one portion of a suspicious bearing, but should not be relied ahead as an individual means of protection. Many new media information point to the need for comprehensive protection of ID is a vital part.

As stated in Anderson (1995) and Tiwari (2002) the resources they monitor, IDS systems are separated into two categories: Host based IDS systems and Network Based IDS systems. The Host based IDS systems are established in the vicinity on host machines. This system also evaluates the behavior and access to key servers ahead which a Host based IDS agent has been located (Lichodzijewski *et al*., 2002). The network based IDS systems examine the packets transient from end to end network.

Anomaly detection can be categorized into two types based on machine learning techniques namely supervised and unsupervised approaches (Portnoy *et al*., 2001). In supervised anomaly detection, the normal behavior of networks is formed by training with a

Corresponding Author: P. Ananthi, Kongu Engineering College, India

normal dataset (Daniel *et al*., 2001). These normal behavior models are utilized to organize new network connections. The system produces an alarm if a connection is identified to have malicious behavior. In order to train a supervised anomaly-based method, normal data are not readily accessible. It consumes larger time and moreover, it is error-prone to manually classify large number of data instances as benign or malign. Machine learning approaches like neural networks (Mukkamala *et al*., 2003) Linear Genetic Programming (LGP) (Mukkamala *et al*., 2004a), Support Vector Machines (SVM), Bayesian networks, Multivariate Adaptive Regression Splines (MARS) (Mukkamala *et al*., 2004b), Fuzzy Inference Systems (FISs) (Shah *et al*., 2004), etc., have been widely used for the design of IDS.

IDS generally act as a network monitor or alert. It raises an alarm before the intruder begins to attack and protects the system from various attacks. The two major models of intrusion detection include anomaly detection and misuse detection (Kemmerer and Vigna, 2002). Anomaly detection creates a model of normal behavior and compares the model with detected behavior. Anomaly detection has a high detection rate, but higher false positive rate. The misuse detection model is constructed in such a way that the attack type is identified by comparison with the attack behavior. The misuse detection has high accuracy, but the detection rate is lower. The misuse detection cannot identify unknown attacks, which are not in the model base. In recent years, the model of hybrid detection has been widely used to attain the advantages of both anomaly detection and of misuse detection (Depren *et al*., 2005). This integration determines unknown attacks, through the detection rate of anomaly detection and the accuracy of misuse detection. The Hybrid Intrusion Detection System (HIDS) performs well with high detection rate and low false positive rate.

In this research work, a novel Adaptive Hybrid Multi-level Intelligent IDS (AHMIIDS) is presented to detect the intrusion in networks. Fuzzy based IDS have observed to provide significant results. In order to improve the overall performance of the IDS, this approach uses three models in the hybrid system namely Anomaly detection model, Misuse detection model and Decision Making model.

In this hybrid system, anomaly detection is based on the Bayesian Network and Misuse detection approach is based on the Adaptive Neuro-Fuzzy Inference System (ANFIS) (Zahra *et al*., 2012). Then, the decision model approach is formulated through Decision Table Majority (DTM) approach (Pfahringer, 1995).

LITERATURE REVIEW

Research and implementation on snort-based hybrid intrusion detection system: In Yu-Xin and Ai-Wu (2009) the Intrusion Detection System (IDS) consists of two detection methods called anomaly detection and misused detection. The author said that this system contains a combination of both the detection methods called Hybrid Intrusion Detection System (HIDS). These methods contain three sub-modules, misused detection module, anomaly detection module and signature generation module. The source of misused detection is snort. Anomaly detection module is build by frequent episode rule. And signature generation module is based on an alternative of a priori algorithm. Misused detection module makes use of the signature of attacks to finding the known attacks.

HIDS-DT: An effective hybrid intrusion detection system based on decision tree: A hybrid intrusion detection technique combing both misuse detection and anomaly detection can identify recently revealed attacks whereas maintaining a reasonably high detection rate (Jie Yang *et al*., 2010). This study presents a system based on protocol investigation and decision tree algorithms. The evaluation of the proposed system is performed by means of Generalized Stochastic Petri Nets (GSPN).

A real-time hybrid intrusion detection system based on principle component analysis and self organizing maps: A novel hybrid intrusion system is introduced by the author, which is the combination of Principle Component Analysis and Self Organizing to begin a real-time intrusion model with high detection accuracy (Xiaorong and Shanshan, 2010). The performance of the system is evaluated using KDD 1999 Cup dataset.

A hybrid system for reducing the false alarm rate of anomaly intrusion detection system: In Om and Kundu (2012) the author introduces a combination of k-Means and the other two classifiers like K-nearest neighbor and Naïve Bayes for anomaly detection. The features are selected by means of entropy based feature selection algorithm which selects the significant attributes and take away the unnecessary attributes (Om and Kundu, 2012). This system can notice the intrusions and additionally categorize them into four groups: Denial of Service (DoS), User to Root (U2R), Remote to Local (R2L) and probe. The performance of the novel scheme is evaluated using KDD-99 Data set.

Hybrid intrusion detection system for enhancing the security of a cluster-based wireless sensor network: In Wireless Sensor Networks (WSNs) (Jie Yang *et al*., 2010), they are more significant to various security problems. WSNs are vulnerable to several types of attacks as they are not expensive and tiny devices and are positioned in open and unprotected environments. An Intrusion Detection System (IDS) is formed using a cluster head. The presented IDS are a Hybrid Intrusion Detection System (HIDS) contains anomaly and misuse detection module. The objective is to increase the detection rate and decrease the false positive rate by the compensation of misuse detection and anomaly detection. Though, a decision-making section is worn to combine the detect results and to report the types of attacks.

CONSUMER: A novel hybrid intrusion detection system for distribution networks in smart grid: Smart meters have been structured at global level which is speedily that facilitates real-time communications capability at the utilization level in power distribution networks (Bhavani Sankar *et al*., 2012). The author is to study about FDI attack by introducing the Combination Sum of Energy profiles (CONSUMER) attack in a synchronized method on a number of customer smart meters that results in lower energy consumption reading for the attacker and higher for the others in a locality. The author introduced an attack model that is put together into one type of coin modify problems, which decrease the number of compromised meters subject to the equality of an combined load in order to avoid detection. The presented hybrid system is combined with grid sensor placement algorithm to increase the detection rate.

METHODOLOGY

The proposed HIDS in this study consists of three models as shown in the Fig. 1. The anomaly detection and misuse detection model is used to identify intrusion so as to filter a huge number of packet records by means of the anomaly detection model and to formulate an additional detection with the misuse detection model. Lastly, the decision making model combine the outputs of anomaly detection and misuse detection models. It determines that if intrusions take place and the classifier classifies the type of attack. The output of the decision making model is then send information to the administrator for follow-up work.

Anomaly detection model: The Anomaly detection model is used to identify and prevent the attacks in networks using Bayesian Networks. The representation of the fundamental dependencies between random variables in Bayesian Networks is specified in graphical structure. A small group of the probabilities are specified with reference to the adjacent nodes, the joint probability distribution of the random variables can be considered. This group will have the information about the prior probabilities of each root nodes and conditional probabilities of all non root nodes given with all promising group of their direct predecessors. This BN are a Directed Acyclic Graph, (DAG) which consist of arcs for denoting the causal dependence among the parent and child permit the storage of the proofs when the values are recognized about some variables and if the proof is identified then it provides a computational arrangement for finding the conditional values of the remaining random variables. This network has a significant advantage and cannot be execute by other method.

The event relation does not depend upon the expert knowledge but it shows the mutual relation with the events in a particular area. In this method, redundant communication and processing overload are banned as the events used to calculate approximately the probability of the attacks are investigated at the position of the network where it is takes place. Therefore, the problem of a variety of control record mismatch does not occur.

Monitoring system: It is an agent should be present in all system and its use is to gather information in its system from application layer to the routing layer. The proposed system gives an exact solution using three procedures. The system monitors its own system and also it's surrounding. The classifier construction is used to identify the local anomaly. When the node have to transmit information from node G to B, it will be commenced by propagating a message to F and A. Earlier sending the message, node G gathers information about the nearby nodes F and B by means of t mobile agent. It uses the classifier rule to detect the

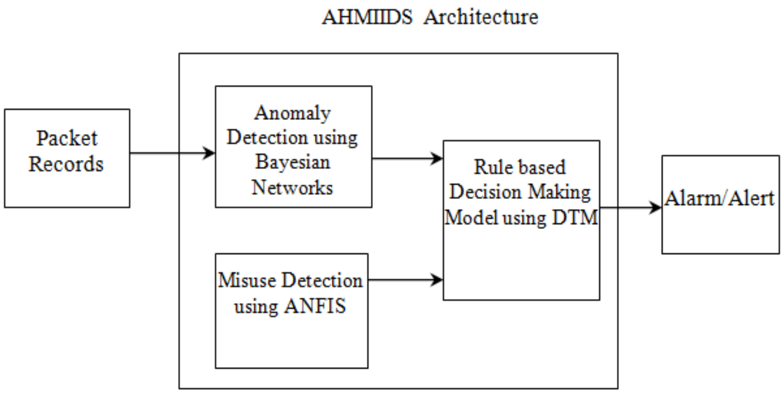
AHMIIDS Architecture
Packet Records
Anomaly Detection using Bayesian Networks
Misuse Detection using ANFIS
Rule based Decision Making Model using DTM
Alarm/Alert

Fig. 1: System architecture

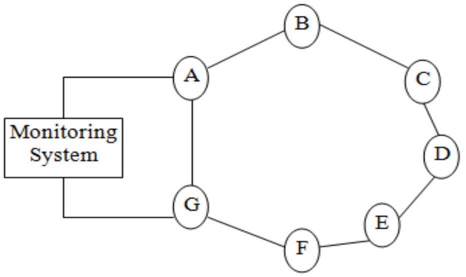

Fig. 2: Outline of the system architecture

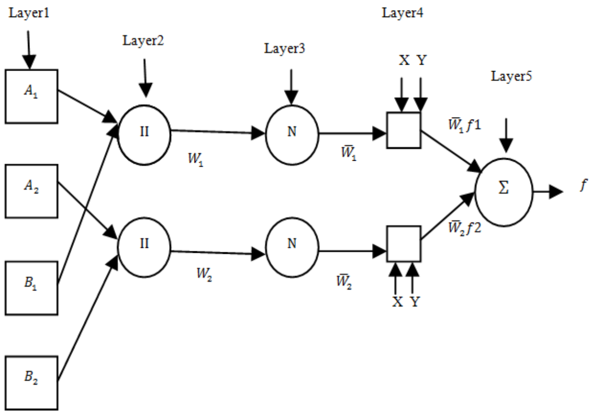

Fig. 3: ANFIS architecture

attacks by the testing training data. The abnormal packets are detected using the anomaly detection model that packets are given as an input to the misuse detection model (Fig. 2).

Misuse detection model: The misuse detection model uses different models of known attack behaviors, so according to that behaviors a classifier model is constructed using Adaptive Neuro Fuzzy Inference System (ANFIS). The ANFIS helps to train the data efficiently, because most of the instruction detection system performance is measure using the training data.

The ANFIS constructs a Fuzzy Inference System (FIS) with the given input and output data set. The parameters of the membership function are adjusted by a back propagation algorithm (Kohavi, 1995). The FIS system integrates with the human knowledge to execute interference and decision making. The combination of fuzzy system and the neural network is used to characterize knowledge in an explainable phenomena and a neural network is used to optimize its parameters. A good selection of the number, type and the parameter of the fuzzy membership functions and rules is essential for attaining a greater performance.

The misuse detection model using ANFIS includes an input layer, a membership layer, rule base layer and an output layer (Fig. 3). The abnormal packets are obtained by the anomaly detection model is used as an input vector. The number of processing units in input layer is defined in the course of the selected features for packet. And then the number of processing units in membership layer is considered via if then rules method, output layer correspond to eight different attacks and one normal behavior, to decide whether the inputted packet is an intrusion and make a classification.

The training data is normalized initially before given as an input to ANFIS. Or else convert the packet records into binary values through preprocessing then give input to ANFIS. Initially, the network parameters are set for obtaining better convergence (actual learning rate is set as 0.5 or between 0.1 and 1.0 is done through simulation). Also allocate values between 0 and 1 as the weights and biases arbitrarily. Later the training data is providing for ANFIS, the actual output through the system of feed forward. And determine the error and improvement of output and hidden layers through the method of back propagation to update the weights in anticipation of all training data have been done to stop and it is called one epoch. Learn the training data frequently and adjust the weights between layers always, through many epochs, until the output of network is analogous to the target value up to the training is complete.

Layer 1: Calculate membership value for premise parameter: The nodes in this layer are not fixed nodes (adaptive) with the degree of the membership of the input are represented as:

Output $O_{1,i}$ for node $i = 1, 2$ $O_{1,i} = \mu_{Bi}(x_2)$

Output $O_{1,i}$ for node $i = 3, 4$ $O_{1,i} = \mu_{Bi}(x_2)$

Layer 2: Firing strength of rule: The nodes are not adaptive which is present in this layer. These are labeled to function like multiplier. The outputs of these nodes are known by:

$$O_{2,I} = \mu_{Ai}(x_1)\mu_{Bi}(x_2)$$

The output of each node is this layer is the firing strength of the rule.

Layer 3: Normalize firing strength: The nodes present in this layer are a fixed node and it is represented as N to show that these perform a normalization of the firing strength from previous layer. The output is given by:

$$O_{3,i} = \overline{w} = \frac{w_1}{w_1 + w_2} \; for \; i = 1,2.$$

Layer 4: Consequent parameters: All nodes in this layer are adaptive nodes. The output of each node is the product represented as:

$$O_{4,i} = \overline{w}_1 f_i = \overline{w}_1(p_1\chi_1 + q_1\chi_2 + r_1)$$

where, p_i, q_i and r_i are design parameters (consequent parameter deal with the then-part of the fuzzy rule).

Layer 5: Overall output: This layer has only one node labeled Σ denote that is performs the function of a simple summer. The output of this single node is given by:

$$O_{5,i} = \sum_i \overline{w}_t f_i = \frac{\sum_i w_i f_i}{\sum_i w_i}$$

Hence the overall output is calculated. Finally the output is deliver to the decision making model to put together.

Decision making model: DTM classifiers are a form of nearest neighbor classifiers where the similarity function is limited to returning stored samples that are exact matches with the instance to be classified (Pfahringer, 1995).

DTM returns the majority of the training set if the decision table cell matching the new sample is empty, i.e., it does not contain any training instances (Kohavi and Sommerfield, 1998).

DTM is been widely used for classification in which if an unseen item exactly matches a stored item in the body then the decision table allocates the stored item's decision to the unseen item. But, if there is no exact match then the decision table allots the majority class across all items to the unseen item (Kohavi, 1995).

Rules for training the decision table majority: If anomaly detection model detects an attack and misuse detection model does not detect attack then it is not an attack and it is erroneous classification.

If anomaly detection model detects an attack and misuse detection model detects attack then it is an attack and determines the class of attack. This model also utilizes on rule based approach, using the rules to combine the outputs of two detection models and its main advantages are that it is very simple and fast in terms of computation.

RESULTS AND DISCUSSION

In this section, the proposed structural design is evaluated through simulation. Because the rules in the anomaly detection model are defined by experts, cannot verify its performance through the simulation. As a result, the experiment in this research would evaluate the performance of misuse detection model, adopted by ANFIS.

Collection of data: The KDDCup'99 dataset (Jie Yang *et al*., 2010) is used to validate the performance of the misuse detection model. The KDDCup'99 dataset is taken from the Columbia University was prearranged from intrusions replicated in a military network environment at the DARPA in 1998.

The features comprises of 34 categories of numerical features and 7 categories of symbolic features, based on different properties of attack. Moreover, KDDCup'99 dataset consist of several attack behaviors, broadly categorized into four groups namely Probe, Dos, U2R and R2L. It also encloses a type of normal communication. Therefore, five behaviors are utilized for the classification of IDS in the simulation format. In this research, kddcup.data_10_percent.gz is used as the sample of training and testing dataset. This includes 10% data in the KDDCup'99 dataset and the total number of communication records is 494021. It randomly samples 30000 records as training data and 15000 records as testing data. But, as the sample number of Probe, U2R and R2L is less, their whole records, can be sampled with two-thirds data as training data and one-third data as testing data. The other sample numbers are sampled based on their ratio from kddcup.data_10_percent.gz, they are categorized to Normal and DoS type separately. The Normal types would results in about 20% where as the Dos type would have about 80%. The data sampling number and ratio are shown in Table 1.

Simulation results: The experiments are carried out using KDD Cup 99 benchmark dataset which will be appropriate for the evaluation and comparison between the proposed approaches and the previous approaches.

In this research, first sample the training and testing data from the KDDCup'99 dataset and filter some insignificant and noise features, to decrease the dimension of the data. Then normalize the data through the preprocessing step and use the data to train the ANFIS model.

In this study, two methods are trained with the simulation and observe the change in learning affects the performance. When the ANFIS training is complete, input of 15000 testing data to make classifications, so as to evaluate its performance and observe its classification accuracy. Two groups of parameters exist in this experiment that represents two different experiments. The design of experimental parameters is shown in Table 2.

The dataset will cover four major groups of attacks which is Probe, DoS, R2L and U2R. For evaluation some parameters selected to compare results between existing system and proposed system. An IDS requires high accuracy and detection rate also low false alarm rate. Usually, the performance of IDS is evaluated in term of accuracy, detection rate and false alarm rate as in the following formula:

Table 1: Amount and ratio of data sampling

	Data					
	10% dataset		Training data		Testing data	
Category	Amount of total data	Ratio (%)	Amount of training data	Ratio (%)	Amount of testing data	Ratio (%)
Normal	97278	19.69	5295	17.65	2648	17.65
Probe	4107	0.83	2738	9.13	1369	9.13
DoS	391458	79.24	21181	70.60	10591	70.61
U2R	52	0.01	35	0.12	17	0.11
R2L	1126	0.23	751	2.50	375	2.50
Total	494021	100	30000	100	15000	100

Table 2: The design of experimental parameters

	Learning rate	Iterations
For experiment 1	0.5	5000
For experiment 2	0.1	5000

Table 3: The performance evaluation of IDS

	DR (%)	FP (%)	Accuracy (%)
For experiment 1	99.90	0.58	99.85
For experiment 2	99.90	0.58	99.85

Table 4: Experiment 1-the table of detailed classification

Classification of attacks	Amount of corrected detection/amount of sample	Detection Ratio (DR) (%)
Normal	2635/2648	99.45
Probe	1360/1369	99.21
DoS	10590/10591	99.99
U2R	11/17	58.83
R2L	368/375	97.62

Table 5: Experiment 2-the table of detailed classification

Classification of attacks	Amount of corrected detection/amount of sample	Detection Ratio (DR) (%)
Normal	2635/2648	99.45
Probe	1360/1369	99.21
DoS	10590/10591	99.99
U2R	11/17	58.83
R2L	368/375	97.62

- Accuracy = (TP + TN) / (TP + TN + FP + FN)
- Detection Rate = (TP) / (TP + FP)
- False Alarm = (FP) / (FP + TN)

Observe that the performance in different learning rate in Table 3. Experiment 1 has a learning rate of 0.5 and that the DR amounts to 99.90%. Its FP is 0.58%, while accuracy amounts to 99.85%. In experiment 2, the learning rate is set to 0.1 and to verify whether or not the lower learning rate could get a better convergence on ANFIS, notice that the DR, FP and accuracy are all the same with experiment 1, using the results of the experiment. Therefore, by setting the learning rate to 0.5, the network gains a better convergence, so as to achieve better performance.

Also examine each class of attacks in Table 4 and 5, to study about the individual detection performance. From that table detection performance of the U2R is very poor when compared with other. It happens due to the training data of U2R are too less and result in the low detection performance.

Also that the experiments is conducted and the simulated results are compared with the other typed of intrusion detection system. For that certain comparison the parameters like measurement of precision, recall and f-value of the systems are taken into consideration:

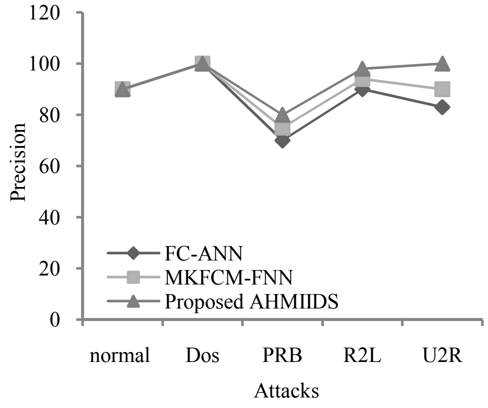

Fig. 4: Precision comparison (%)

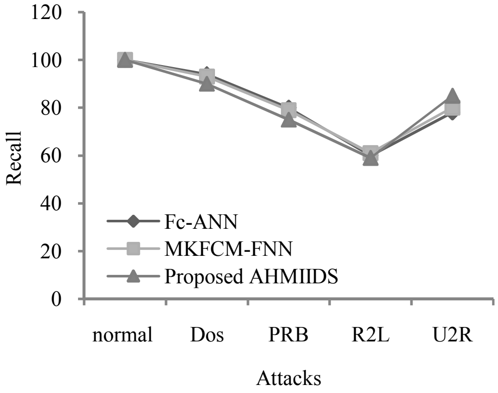

Fig. 5: Recall (%) of different methods

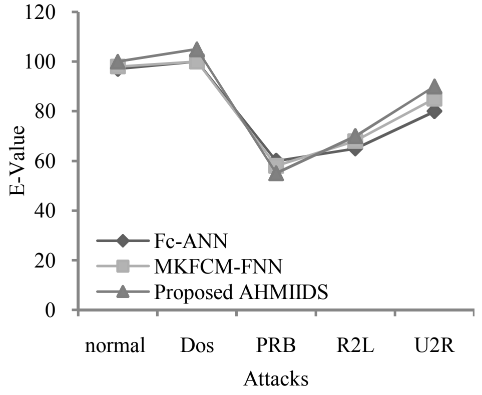

Fig. 6: F-value (%) of different methods

$$Precision = \frac{TP}{TP + FP}$$

$$Recall = \frac{TP}{TP+FN}$$

$$F - value = \frac{1+\beta^2 * Recall * Precision}{\beta^2 (Recall + Precision)}$$

From the Fig. 4 to 6 the proposed AHMIIDS technique gives better performance when compared with the other existing techniques like FC-ANN, MKFCM-FNN.

CONCLUSION AND RECOMMENDATIONS

Intrusion detection is a most significant field in the network security research and it is a latest one tries to reduce the anxiety associated with instinctive technology of the network security. Therefore, a better intrusion detection system is presented and implemented in this study. A hybrid technique is proposed in this study using anomaly detection and misuse detection. The anomaly detection is done using Bayesian Networks and then the misuse detection is performed using ANFIS. The outputs of both anomaly detection and misuse detection modules are applied to Decision Table Majority to perform the final decision making. The simulation result shows that the proposed AHMIIDA scheme performs better than the existing approaches such as FC-ACC and MKFCM-FNN approaches.

REFERENCES

Anderson, J., 1995. An Introduction to Neural Networks. MIT Press, Cambridge.

Bhavani Sankar, A., D. Kumar and K. Seethalakshmi, 2012. A new self-adaptive neuro fuzzy inference system for the removal of non-linear artifacts from the respiratory signal. J. Comput. Sci., 8(5): 621-631.

Daniel, B., C. Julia, J. Sushil and W. Ningning, 2001. Adam: A testbed for exploring the use of data mining in intrusion detection. ACM SIGMOD Record, 30: 15-24.

Depren, O., M. Topallar, E. Narim and M.K. Ciliz, 2005. An intelligent Intrusion Detection System (IDS) for anomaly and misuse detection in computer networks. Expert Syst. Appl., 29(4): 713-722.

Jie Yang, X.C., X. Xudong and W. Jianxiong, 2010. HIDS-DT: An effective hybrid intrusion detection system based on decision tree. Proceeding of the International Conference on Communications and Mobile Computing (CMC), 1: 70-75.

John, M., C. Alan and A. Julia, 2000. Defending yourself: The role of intrusion detection systems. IEEE Software, 17(5): 42-51.

Kemmerer, R.A. and G. Vigna, 2002. Intrusion detection a brief history and overview. Computer, 35(4): 27-30.

Kohavi, R., 1995. The Power of Decision Tables. Proceedings of European Conference on Machine Learning. LNAI 914, Springer-Verlag, pp: 174-189.

Kohavi, R. and D. Sommerfield, 1998. Targeting business users with decision table classifier. Proceeding of 4th International Conference on Knowledge Discovery and Data Mining, pp: 249-253.

Lichodzijewski, P., A. Zincir-Heywood and M. Heywood, 2002. Host-based intrusion detection using self-organizing maps. Proceedings of the IEEE International Jiont Conference on Neural Networks (IJCNN, 2002). Honolulu, HI.

Mukkamala, S., A.H. Sung and A. Abraham, 2003. Intrusion detection using ensemble of soft computing paradigms. Proceeding of the 3rd International Conference on Intelligent Systems Design and Applications. Tulsa, USA, pp: 239e48.

Mukkamala, S., A.H. Sung and A. Abraham, 2004a. Modeling intrusion detection systems using linear genetic programming approach. Proceeding of the 17th International Conference on Industrial and Engineering Applications of Artificial Intelligence and Expert Systems (IEA/AIE). Ottawa, Canada, pp: 633e42.

Mukkamala, S., A.H. Sung, A. Abraham and V. Ramos, 2004b. Intrusion detection systems using adaptive regression splines. In: Seruca, I., J. Filipe, S. Hammoudi and J. Cordeiro (Eds.), Proceeding of the 6th International Conference on Enterprise Information Systems (ICEIS'04). Portugal, 3: 26e33.

Om, H. and A. Kundu, 2012. A hybrid system for reducing the false alarm rate of anomaly intrusion detection system. Proceeding of the 1st International Conference on Recent Advances in Information Technology (RAIT).

Pfahringer, B., 1995. Compression-based feature subset selection. Proceedings of the IJCAI-95 Workshop on Data Engineering for Inductive Learning. Morgan Kaufmann Publishers, Montreal, Quebec, Canada, San Francisco, CA, USA, pp: 109-119.

Portnoy, L., E. Eskin and S.J. Stolfo, 2001. Intrusion detection with unlabeled data using clustering. Proceeding of the ACM CSS workshop DMSA-2001, Philadelphia, PA, November 8, pp: 5-8.

Shah, K., N. Dave, S. Chavan, S. Mukherjee, A. Abraham and S. Sanyal, 2004. Adaptive neuro-fuzzy intrusion detection systems. Proceeding of the IEEE International Conference on Information Technology: Coding and Computing (ITCC'04), pp: 70-74.

Summers, R.C., 1997. Secure Computing: Threats and Safeguards. McGraw-Hill, New York.

Tiwari, P., 2002. Intrusion detection technical report. Department of Electrical Engineering Indian Institute of Technology, Delhi.

Xiaorong, C. and W. Shanshan, 2010. A real-time hybrid intrusion detection system based on principle component analysis and self organizing maps. Proceeding of the 6th International Conference on Natural Computation (ICNC), 3: 1182-1185.

Yu-Xin, D.M.X. and L. Ai-Wu, 2009. Research and implementation on snort-based hybrid intrusion detection system. Proceeding of the International Conference on Machine Learning and Cybernetics, 3: 1414-1418.

Zahra, A.O., M. Ezzat, H.N. Ahmad, A.A. Amir Azimi and M. Mir Kamal, 2012. Using adaptive neuro-fuzzy inference system in alert management of intrusion detection systems. Int. J. Comput. Netw. Inform. Secur., 11: 32-38.