TELKOMNIKA Indonesian Journal of Electrical Engineering
Vol. 13, No. 2, February 2015, pp. 223 ~ 231
DOI: 10.11591/telkomnika.v13i2.7045

A Novel and Advanced Data Mining Model Based Hybrid Intrusion Detection Framework

K. Rajasekaran*[1], K. Nirmala[2]
Bharathiar University, Coimbatore
Quiad-E-Millath College for Women 2, Chennai
*Corresponding author, e-mail: krs.salem@gmail.com[1], nimimca@gmail.com[2]

Abstract

An Intrusion can be defined as any practice or act that attempt to crack the integrity, confidentiality or availability of a resource. This may contain of a deliberate unauthorized attempt to access the information, manipulate the data, or make a system unreliable or unusable. With the expansion of computer networks at an alarming rate during the past decade, security has become one of the serious issues of computer systems.IDS, is a detection mechanism for detecting the intrusive activities hidden among the normal activities. The revolutionary establishment of IDS has attracted analysts to work dedicatedly enabling the system to deal with technological advancements. Hence, in this regard, various beneficial schemes and models have been proposed in order to achieve enhanced IDS. This paper proposes a novel hybrid model for intrusion detection. The proposed framework in this paper may be expected as another step towards advancement of IDS. The framework utilizes the crucial data mining classification algorithms beneficial for intrusion detection. The Hybrid framework would hence forth, will lead to effective, adaptive and intelligent intrusion detection.

Keywords: *data mining, intrusion detection, classification, K2, TAN, REP, KDDCup'99, neural network*

1. Introduction

With the development of network techniques andscience technologies, information industry has expandedgreatly. Both organizations such government, enterprises,finance, telegraphy etc., and personal users have depended on networks more and more. At the same time, it has brought lots of information security troubles. Network security is increasingly paid attention to and concerned about, so it is a critical problem how to protect the security of networks and information system.

Intrusion Detection is a necessary supplement of traditional security protection measures such as firewalls and data encryption, because it can provide real-time protection against internal attacks, external attacks and misoperations. Intrusion Detection belongs to the classification and recognition problems with a large number of non-linear conditions, which make it essential to study non-linear integrated approaches to solve the problem [1, 2]. Artificial Neural Network (ANN), often just called "neural network" (NN), is a mathematical model or computational model based on biological neural networks. It consists of an interconnected group of artificial neurons and processes information using a connectionist approach to computation. In most cases an ANN is an adaptive system that changes its structure based on external or internal information that flows through the network during the learning phase. In more practical terms neural networks are non-linear statistical data modeling tools. They can be used to model complex relationships between inputs and outputs or to find patterns in data. The ability to learn and adapt to the uncertainties of ANN are just suitable to solve the intrusion detection problem.

However, an ANN easily drops into a local minimum, so it may not search the global optimum [3]. For thisdefect, the paper will propose an anomaly intrusion detection model based on Genetic Neural Network (GNN), which combines the good global searching ability of genetic algorithm with the accurate local searching feature of BP Networks to optimize the initial weights ofneural networks. The practice can overcome the shortcomings in the BP algorithm such as slow convergence, easily dropping into local minimum and weakness in global searching. And we will carry out simulation experiments to verify the validity of the practice.

Received November 18, 2014; Revised January 8, 2015; Accepted January 25, 2015

Intrusion Detection System is a mechanism that is being used to protect organization from attacks from different sources. Intrusion detection is defined by the Sysadmin, Audit, Networking and Security (SANS) institute as the act of detecting actions that attempt to compromise the confidentiality, integrity or availability of a resource. It is obligatory that IDS can handle huge quantities of information without affecting performance and without loss of data and can detect intrusions reliably without giving false alarms.

IDS are broadly classified as:

a) Misuse Based System

In misuse based IDS, detection is done by searching for the exploitation of known weak points in the system, which can be described by a specific pattern or sequence of events or data. That means these systems can detect only known attacks for which they have a defined signature.

b) Anomaly Based System

In anomaly based IDS, detection is performed by detecting changes in the patterns of utilization or behavior of the system.

2. Related Works

Some import applications of soft computing techniques for Network Intrusion Detection is described in this section. Several Genetic Algorithms (GAs) and Genetic Programming (GP) has been used for detecting intrusion detection of different kinds in different scenarios. Some uses GA for deriving classification rules [5-8]. Gas used to select required features and to determine the optimal and minimal parameters of some core functions in which different AI methods were used to derive acquisition of rules [9-11]. There are several papers [12-15] related to IDS which has a certain level of impact in network security.

The effort of using GAs for intrusion detection can be referred back to 1995, when Crosbie and Spafford [16] applied the multiple agent technology and GP to detect network anomalies [19]. For both agents, they used GP to determine anomalous network behaviours and each agent can monitor one parameter of the network audit data. The proposed methodology has the advantage when many small autonomous agents are used, but it has problems when communicating among the agents and also if the agents are not properly initialized the training process can be time consuming.

Li [6] described a method using GA to detect anomalous network intrusion [19, 20]. The approach includes both quantitative and categorical features of network data for deriving classification rules. However, the inclusion of quantitative feature can increase the detection rate, but no experimental results are available. Goyal and Kumar [18] described a GA based algorithm to classify all types of smurf attack using the training dataset with false positive rate is very low (at 0.2%) and detection rate is almost 100% [20].

Lu and Traore [7] used historical network dataset using GP to derive a set of classification [19]. They used support-confidence framework as the fitness function and accurately classified several network intrusions. But their use of genetic programming made the implementation procedure very difficult and also for training procedure more data and time is required

Xiao et al. [17] used GA to detect anomalous network behaviours based on information theory [19, 20]. Some network features can be identified with network attacks based on mutual information between network features and type of intrusions and then using these features a linear structure rule and also a GA is derived. The approach of using mutual information and resulting linear rule seems very effective because of the reduced complexity and higher detection rate. The only problem is it considered only the discrete features.

Gong et al. [19] presented an implementation of GA based approach to Network Intrusion Detection using GA and showed software implementation. The approach derived a set of classification rules and utilizes a support-confidence framework to judge fitness function.

Abdullah et al. [20] showed a GA based performance evaluation algorithm to network intrusion detection. The approach uses information theory for filtering the traffic data.

Min Yang et al [31] discussed a model based on contiguous expert voting algorithm. Although early methods detect most anomalies, unsuccessful match doesn‟t mean an abnormity, as normal rules may not cover all normal data. The Detection rate in this is not commendable but it has vast future scope for improvement.

3. Neural Networks for Intrusion Detection

A limited amount of research has been conducted on the application of neural networks to detecting computer intrusions. Artificial neural networks offer the potential toresolve a number of the problems encountered by the othercurrent approaches to intrusion detection. Artificial neural networks have been proposed as alternatives to thestatistical analysis component of anomaly detection systems, [5-6], [10, 23, 26]. Statistical Analysis involves statistical comparison of current events to a predetermined set of baseline criteria. The technique is most often employed in the detection of deviations from typical behavior and determination of the similarly of events to those which are indicative of an attack [8]. Neural networks were specifically proposed to identify the typical characteristics of system users and identify statistically significant variations from the user's established behavior.

A Neural network approach for intrusion detection one promising research in Intrusion detection concerns the application of the Neural Network techniques, for the misuse detection model and the anomaly detection model. Performance evaluations presented in this paper all refer to the DARPA Intrusion Data Base Neural Network approach an artificial Neural Network consists of acollection of treatments to transform a set of inputs to a setof searched outputs, through a set of simple processing units, or nodes and connections between them. Subsets ofthe units are input nodes, output nodes, and nodes between input and output form hidden layers; the connection between two units has some weight, used to determine how much one unit will affect the other. Two types ofarchitecture of Neural Networks can be distinguished.

Supervised training algorithms: where in the learning phase, the network learns the desired output for a given input or pattern. The well known architecture of supervised neural network is the Multi-Level Perceptron (MLP); the MLP is employed for Pattern Recognition problems.

Unsupervised training algorithms: where in the learning phase, the network learns without specifying desired output.

Neural Networks (NNs) have attracted more attention compared to other techniques. That is mainly due to the strong discrimination and generalization abilities of Neural Networks that utilized for classification purposes [19]. Artificial Neural Network is a system simulation of the neurons in the human brain [20]. It is composed of a large number of highly interconnected processing elements (neurons) working with each other to solve specific problems. Each processing element is basically a summing element followed by an active function. The output of each neuron (after applying the weight parameter associated with the connection) is fed as the input to all of the neurons in the next layer. The learning process is essentially an optimization process in which the parameters of the best set of connection coefficients (weights) for solving a problem are found [21].

An increasing amount of research in the last few years has investigated the application of Neural Networks to intrusion detection. If properly designed and implemented, Neural Networks have the potential to address many of the problems encountered by rule-based approaches. Neural Networks were specifically proposed to learn the typical characteristics of system's users and identify statistically significant variations from their established behavior. In order to apply this approach to Intrusion Detection, I would have to introduce data representing attacks and non-attacks to the Neural Network to adjust automatically coefficients of this Network during the training phase. In other words, it will be necessary to collect data representing normal and abnormal behavior and train the Neural Network on those data. After training is accomplished, a certain number of performance tests with real network traffic and attacks should be conducted [22]. Instead of processing program instruction sequentially, Neural Network based models on simultaneously explorer several hypotheses make the use of several computational interconnected elements (neurons); this parallel processing may imply time savings in malicious traffic analysis .

4. Proposed Method

The proposed system (shown in Figure 1) is a hybrid intrusion detection framework based on the combination of two classifiers i.e. Tree Augmented Naïve Bayes (TAN) and Reduced Error Pruning (REP). The TAN classifier is used as a base classifier while the REP classifier is used as a Meta classifier. The Meta classification is the learning technique which learns from the Meta data and judge the correctness of the classification of each instance by base classifier. The judgement from each classifier for each class is treated as a feature, and then builds another classifier, i.e. a meta-classifier, to make the final decision [11]. Hence it can be said that the Meta-classification re-classifies the classification judgments made by classifiers.

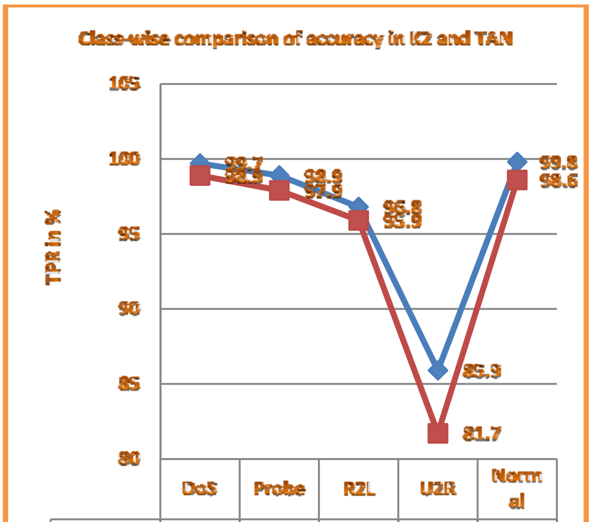
The working of hybrid framework can be understood in following algorithmic steps:

Step 1: Input dataset
Step 2: Perform preprocessing of the dataset
Step 3: Select TAN as the base classification algorithm
Step 4: Choose REP algorithm for Meta classification
Step 5: Perform classification on base classifier for Meta Rules
Step 6: Set the obtained Meta rules as input for Meta classification
Step 7: Perform re-classification using Meta classifier

The main idea of using this technique is to improve the overall classification performance resulting in better outcomes than any other existing technique. The two classifiers indulged in the proposed system can be understood as:

4.1. Detailed Description of the Hybrid IDS Framework

This section describes about all the modules incorporated in the Hybrid IDS framework shown in Figure 1. Following is the brief discussion about each module:



	DoS	Probe	R2L	U2R	Normal
TAN	99.7	98.9	96.8	85.9	99.8
K2	98.9	97.9	95.9	81.7	98.6

Figure 1 Class-wise comparison of accuracy in K2 and TAN

4.2. KDD Cup 99 Data Set Description

Since 1999, KDD'99 [3] has been the most wildly useddata set for the evaluation of anomaly detection methods. This data set is prepared by Stolfo et al. [5] and is built based on the data captured in DARPA'98 IDS evaluation program [6]. DARPA'98 is about 4 gigabytes of compressed raw (binary) tcp dump data of 7 weeks of network traffic, which can be processed into about 5 million connection records, each with about 100 bytes. The two weeks oftest data have around 2 million connection records. KDD training dataset consists of approximately 4,900,000 single connection vectors each of which contains 41 features and is labeled as either normal or an attack, with exactly onespecific attack type.

In the preprocessing module the class label presents in the 42nd feature of KddCup'99 dataset is recast intofive major categories for the sake of decreasing complexity of performance evaluation of the proposed model.As the original KddCup'99 dataset having 22 types of attack labels, it was very inconvenient to assess the performance of the classification model. Hence the attack labels are modified to their respective categories for the ease of analysis. Finally five major classes are formed as the class label i.e. DoS, Probe, R2L, U2Rand Normal.

4.3. Dataset Splitter

The Dataset Splitter module partitions the dataset into two parts received from the preprocessing module. To partition the dataset into two parts a method named holdout is used. In this method, the given data are randomly partitioned into two independent sets, a training set and a test set [17]. The 66% of the data isallocated to the training set and the remaining 44% of the dataset is allocated to the testing set. The training set is used to derive the proposed framework while the test set is used to assess the accuracy of the derived model. When the KddCup'99 dataset passed through the data splitting module then it gets divided into the training set which consists of 326054 instances and the testing set which consists of 167967 instances.

4.4. Learning Phase

The learning phase involves two steps for generating the classification rules. In the first step, the learning ofbase classifier i.e. TAN using the training dataset is achieved. The outcome of this base classifier is assumed as the input data (known as Meta data) for the second step. This meta-level training set is composed by usingthe base classifiers' predictions on the validation set as attribute values, and the true class as the target [18]. From these predictions, the meta-learner adapts the characteristics and performance of the base classifier and computes a meta-classifier which is a model of the original training data set. This meta-classifier in second step fetches the predictions from the base classifier for classifying an unlabeled instance, and then makes the final classification decision.

4.5. Testing Phase

The classification rules that are generated in Learning Phase are stored for the performance evaluation of hybrid intrusion detection framework. In this phase, the Testing Set generated in Data Splitting module isused as input to assess the performance. The outcome of this module is further forwarded to next module i.e.Classifier Performance Evaluator module.

4.6. Classifier Performance Evaluator

Table 1

True class → Hypothesized | class V	Pos	Neg
Yes	TP	FP
No	FN	TN
	P=TP+FN	N=FP+TN

a) Accuracy = (TP+TN)/(P+N)
b) Precision = TP/(TP+FP)
c) Recall/TP rate = TP/P
d) FP Rate = FP/N
e) ROC Analysis moves the threshold between the positive and negative class from a small FP rate to a large one. It plots the value of the Recall against that of the FP Rate at each FP Rate considered.

4.7. Visualization

The result generated in the Performance Evaluation phase can be visualized in the visualization module. These results can be in the form of text or graph etc.

5. Experimental Analysis

This section describes the experimental outcomes of the developed hybrid intrusion detection framework and its comparison with various other techniques present in the scenario. It has been noticed that the outcomes of the hybrid IDS framework excelled most of the algorithms in respect of performance (prominently accuracy). Following Table 2 and 3 is the comparison of the two algorithms i.e. TAN and REP utilized in the hybrid IDS framework with respect to the frequently preferred bayes net based K2 algorithm.

Table 2. Performance Comparison of TAN, REP, HYBRID and K2

Class	TAN		K2		REP		HYBRID	
	TPR	FPR	TPR	FPR	TPR	FPR	TPR	FPR
DoS	0.997	0.000	0.989	0.000	1.001	0.001	1.000	0.001
Probe	0.989	0.000	0.979	0.005	0.979	0.000	0.988	0.000
R2L	0.968	0.000	0.959	0.001	0.984	0.000	0.973	0.000
U2R	0.859	0.000	0.813	0.005	0.668	0.000	0.835	0.000
Normal	0.998	0.001	0.986	0.002	0.999	0.000	0.998	0.000

Next the Table 2 shows the comparison of the developed framework with the K2 algorithms proving its effectiveness with improved results in case of each type of attacks.

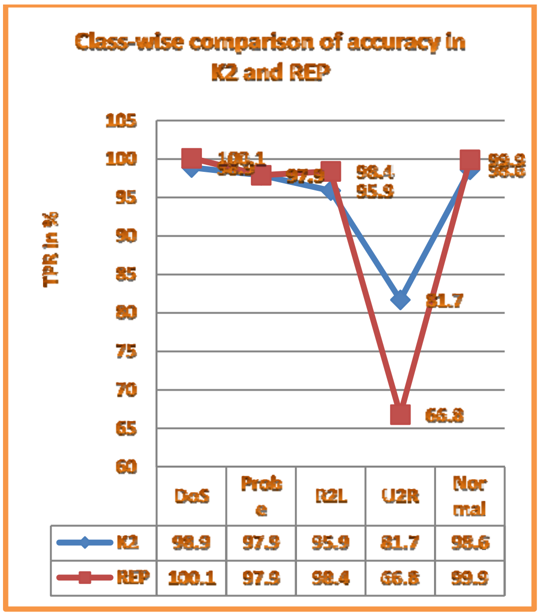


Figure 2. Class-wise comparison of accuracy in K2 and REP

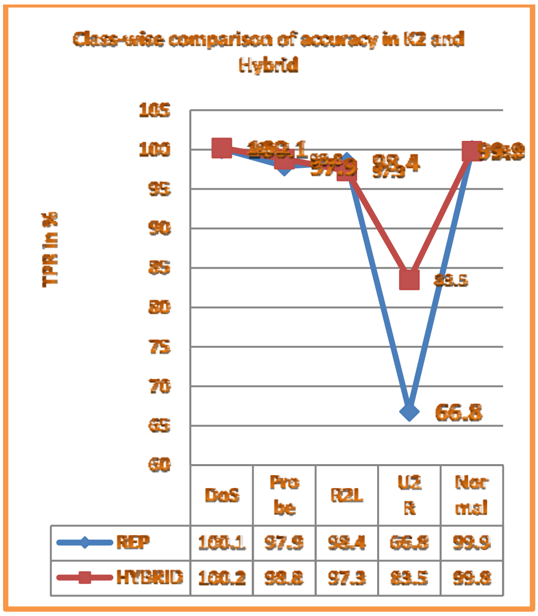


Figure 3. Class-wise comparison of accuracy in REP and Hybrid

When the developed framework is compared with the respective various available data mining techniques for intrusion detection, the resultant obtained shows the favorable opinion to opt as the hybrid technique. The lead may be understood from the above comparison graph.

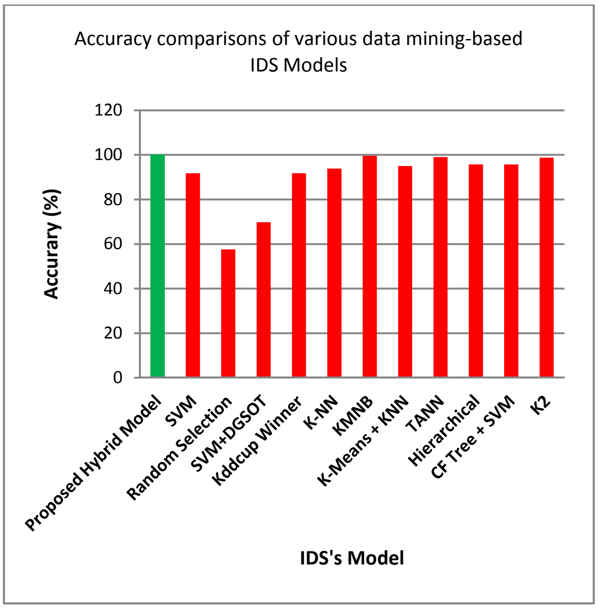


Figure 4. Accuracy comparisons of various data mining-based IDS Models

6. Conclusion

In this paper, I have described an overview of some of the current and past intrusion detection technologies which are being utilized for the detection of intrusive activities against computer systems or networks. The intrusion classifier based on multiple attribute selection algorithms has been proposed in this paper. The new system has six combinations with different representative attribute selection algorithms and different classification algorithms. Through comparing with classification performance and real time, the advantage or disadvantage of different combinations comes out. It is positive significance for deploying different algorithm combinations based on the concrete context. In the future, we will try to apply the intrusion classifier in the field of wireless sensor networks. Some core code of intrusion classifier should be simplified. The classifier will be improved to be the next module of the lightweight detection.

Acknowledgements

I would like to extend my sincere thanks and gratefulness to our college staff members of DB Jain College, Chennai.India for his kind help, moral support and guidance in preparing this article.

References

[1] M Bahrololum, M Khaleghi. Anomaly Intrusion Detection System Using Hierarchical Gaussian Mixture Model. *IJCSNS International Journal of Computer Science and Network Security*.2008; 8(8).
[2] Jiankun Hu, Xinghuo. A Simple and Efficient Hidden Markov Model Scheme for Host-Based Anomaly Intrusion Detection. *IEEE Network Journal.* 2009; 23(10).
[3] R Nakkeeran, T. Aruldoss Albert and R.Ezumalai. Agent Based Efficient Anomaly Intrusion Detection System in Ad-hoc networks. *IACSIT International Journal of Engineering and Technology*. 2010; 2(1).
[4] Jiong Zhang, Mohammad Zulkernine. *Anomaly Based Network Intrusion Detection with Unsupervised Outlier Detection.* IEEE International Conference on Communications. 2006.
[5] Ahmed Awad E. Ahmed, IssaTraore. *Anomaly Intrusion Detection based on Biometrics*. IEEE Workshop on Information Assurance. 2005.
[6] Vijay Bhuse, Ajay Gupta. Anomaly Intrusion Detection in Wireless Sensor Networks. *ACM Journal of High Speed Network*s, 2006.
[7] Hossein M Shirazi. Anomaly Intrusion Detection System Using Information Theory, K-NN and KMC Algorithms. *Australian Journal of Basic and Applied Sciences.* 2009; 3(3): 2581-2597.
[8] Dayu Yang, Alexander Usynin, J Wesley Hines. Anomaly-Based Intrusion Detection for SCADA Systems. *IAEA Technical Meeting on Cyber Security of NPP I&C and Information systems*, Idaho Fall, ID. 2006

[9] M Thangavel, Dr P Thangaraj, K Saravanan. Defend against Anomaly Intrusion Detection using SWT Mechanism. *IACSIT.* 2010.
[10] Miao Wang, Cheng Zhang, Jingjing. *Native API Based Windows Anomaly Intrusion Detection Method Using SVM*. IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing. 2006.
[11] Manikopoulos C, Papavassiliou S. Network Intrusion and Fault Detection: A Statistical Anomaly Approach. *IEEE Communications*. 2002.
[12] Jeyanthi Hall, Michel Barbeau, EvangelosKranakis. *Using Mobility Profiles for Anomaly-based Intrusion Detection in Mobile Networks*. IEEE Conference. 2005.
[13] Hazem M El-Bakry, Nikos MastorakisA. Real-Time Intrusion Detection Algorithm for Network Security. *WSEAS Transactions on communications*. 2008; 12(7).
[14] Debar H, Dacier M, Wespi A. A Revised Taxonomy of Intrusion-Detection Systems. Annales des Telecommunications. 2000; 55(7–8): 361–378
[15] Allen J, Christie A, Fithen W, McHugh J, Pickel J, Stoner E. State of the practice of intrusion detection technologies. Technical Report CMU/SEI-99TR- 028, Carnegie-Mellon University - Software Engineering Institute. 2000.
[16] Roesch M. *Snort - Lightweight Intrusion Detection for Networks*. 13th USENIX Conference on System Administration, USENIX Association. 1999; 229–238.
[17] Sourcefire: Snort Network Intrusion Detection System web site. URL http://www.snort.org. 1999.
[18] Wang K, Stolfo SJ. Anomalous Payload-Based Network Intrusion Detection. 7th Symposium on Recent Advances in Intrusion Detection, Volume 3224 of LNCS, *Springer-Verlag.* 2004; 203–222.
[19] Bolzoni D, Zambon E, Etalle S, Hartel P. *POSEIDON: a 2-tier Anomaly based Network Intrusion Detection System*. IEEE International Workshop on Information Assurance, IEEE Computer Society Press. 2006; 144– 156.
[20] B Pfahringer. Winning the KDD99 Classification Cup: Bagged Boosting. SIGKDD Explorations. 2000.
[21] I Levin. KDD-99 Classifier Learning Contest: LL Soft"s Results Overview. SIGKDD Explorations. 2000.
[22] V Miheev, Vopilov A, Shabalin.I. The MP13 Approach to the KDD"99 Classifier Learning Contest. *SIGKDD Explorations*. 2000.
[23] Y Freund, Schapire R. *Experiments with a new boosting algorithm*. Thirteenth International Conference on Machine Learning, Italy. 1996.
[24] Q Yang, Li, F. Support Vector Machine for Intrusion Detection Based on LSI Feature Selection. Intelligent Control and Automation, WCICA. 2006.
[25] JC Platt. Sequential minimal optimization: A fast algorithm for training support vector machines. *Advances in Kernel Method: Support Vector Learning*. 1998.
[26] FE Osuna R, Girosi F. Improved training algorithm for support vector machines. IEEE NNSP"97, 1997.
[27] Y Yao, Wei Y, Gao, FX, Yu G. Anomaly Intrusion Detection Approach Using Hybrid MLP/CNN Neural Network. Sixth International Conference on Intelligent Systems Design and Applications (ISDA'06) Washington, DC, USA 2006.
[28] A Zaknic. Introduction to the modified probabilistic neural network for general signal processing applications. *IEEE Transactions on Signal Processing*. 1998; 46.
[29] DF Specht. Probabilistic Neural Network. International Journal of Neural Networks. 1990; 3: 109-118
[30] L Khan, M Awad, B Thuraisingham. A new intrusion detection system using support vector machines and hierarchical clustering. *The International Journal on Very Large Data Bases*. 2007; 15(4).
[31] Min Yang, Da-peng Chen, Xiao-Song Zhang. Anomaly Detection Based On Contiguous Expert Voting Algorithm. *IEEE*. 2009.
[32] Vasilis A Sotiris, Peter W Tse, Michael G Pecht. Anomaly Detection Through a Bayesian Support Vector Machine. *IEEE Transactions on Reliability.* 2010.
[33] Zhenghong Xiao, Chuling Liu, Chaotian Chen. *An Anomaly Detection Scheme Based on Machine Learning for WSN*. IEEE International Conference on Information Science and Engineering. 2009.
[34] Yunlu Gong, Mabu S, Ci Chen, Yifei Wang, Hirasawa K. Intrusion detection system combining misuse detection and anomaly detection using Genetic Network Programming. ICCAS-SICE. 2009.
[35] Li-li Liu and Yuan Liu. *MQPSO Based on Wavelet Neural Network for Network Anomaly Detection*. 5th International Conference on Wireless Communications, Networking and Mobile Computing. 2009.
[36] JianXu Jing You Fengyu Liu. A fuzzy rules based approach for performance anomaly detection. *IEEE*. 2005.
[37] D Dasgupta. Artificial Immune Systems and Their Applications. Springer. 1999.
[38] SA Hofmeyr, S Forrest. Architecture for an artificial immune system. *IEEE Trans. on Evolutionary Computation.* 2000; 8(N4): 443-473
[39] Sokolov AM. *Int. Res. & Training Center of Informational Technol. & Syst., Kiev, Ukraine,* Proceedings of the International Joint Conference on Neural Networks. 2003.
[40] E Hart, P Ross, J Nelson. Producing robust schedules via an artificial immune system. *IEEE International Conference on Evolutionary Computing*. 1998; 464-469.

[41] D Dasgupta. An artificial immune system as a multiagent decision support system. IEEE International Conference on Systems, Man and Cybernetics. 1998: 3816-3820.
[42] A Gardner, A Krieger, G Vachtsevanos, B Litt. One-class novelty detection for seizure analysis from intracranial EEG. J. Machine Learning Research (JMLR). 2006; 7: 1025–1044.
[43] D Barbar´a, C Domeniconi, J Rogers. Detecting outliers using transduction and statistical testing. *ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD)*. Philadelphia, PA. 2003.
[44] J Ma, S Perkins. *Online novelty detection on temporal sequences*. ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD), Washington, DC. 2003.
[45] A Ihler, J Hutchins, P Smyth. Adaptive event detection with time-varying Poisson processes. ACM SIGKDD Int. Conf. on Knowledge Discovery and Data Mining (KDD), Philadelphia, PA. 2006.
[46] A Munoz and J Moguerza. Estimation of high-density regions using one-class neighbor machines. *IEEE Transactions on Pattern Analysis and Machine Intelligence*. 2006; 28(3): 476–480.
[47] LN de Castro, FJ Von Zuben. Learning and Optimization Using the Clonal Selection Principle. *IEEE Transactions on Evolutionary Computation*. 2002; 6(3): 239-251
[48] Jeyanthi Hall, Michel Barbeau, EvangelosKranakis. Anomaly-based intrusion detection using mobility profiles of public transportation users. *IEEE Wireless and Mobile Computing, Networking and Communications.* 2005.
[49] Ramkumar Chinchani, Aarthie Muthukrishnan, Madhusudhanan Chandrasekaran, Shambhu Upadhyaya. *RACOON: Rapidly Generating User Command Data for Anomaly Detection from Customizable Templates*. 20th Conference of IEEE Computer Society. 2004.
[50] Wei Wang, Xiaohong Guan, XiangliangZhang. Profiling program and user behaviors for anomaly intrusion detection based on non-negative matrix factorization. 43rd IEEE Conference on Decision and Control. 2004; 1: 99-104.
[51] TichPhuoc Tran, Pohsiang Tsai, Tony Jan. A Multi-expert Classification Framework with Transferable Voting for Intrusion Detection. Seventh International Conference on Machine Learning and Applications Publisher. *IEEE Computer Society*. 2008.
[52] Anderson D, Frivold T, Valdes A. Nextgeneration Intrusion Detection Expert System (NIDES). 1995.
[53] Cramer M, et. Al. *New Methods of Intrusion Detection using Control-Loop Measurement*. Proceedings of the Technology in Information Security Conference (I'ISC). 1995: 1-10.
[54] Debar H, Becke M, Siboni D. A Neural Network Component for an Intrusion Detection System. Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy. 1992.
[55] Debar H, Dorizzi B. An Application Recurrent Network to an Intrusion Detection System. In Proceedings ofthe International Joint Conference on Neural Networks. 1992; (11): 478-483.
[56] Denning, Dorothy. An Intrusion-DetectionModel. IEEE Transactions on Software Engineering. 1987; SE-13(2).
[57] Fox, Kevin L, Henning, Rhonda R, Reed, Jonathan H. *A Neural Network. Approach towards Intrusion Detection*. In Proceedings of the 13th National Computer Security Conference. 1990.
[58] Frank, Jeremy. *Artificial Intelligence and Intrusion Detection: Current and Future Directions.* Proceedings of the 17th National Computer Security Conference. 1994.
[59] Helman P, Liepins G. Statistical foundations of audit trail analysis for the detection of computer misuse. *IEEE Trans. on Software Engineering.* 1993; 19(9): 886-901.
[60] Kumar S, Spafford E. *A Pattern Matching Model for Misuse Intrusion Detection.* Proceedings of the 17th National Computer Security Conference. 1994; 11-21.
[61] Kumar S, Spafford E. *Software Architecture to Support Misuse Intrusion Detection.* Department of Computer Sciences, Purdue University; CSD-TR-95-009
[62] Lunt TF. Real-Time Intrusion Detection. *Computer Security Journal*. 1989; VI: 9-14.
[63] Ryan J, Lin, M, Miikkulainen R. *Intrusion Detection with Neural Networks.* AI Approaches to Fraud Detection and Risk Management: MAl Workshop (Providence, Rhode Island). 1997; 72-79.
[64] Sebring M, Shell house E, Hanna M, Whitehurst R. Expert Systems in Intrusion Detection: Stanford-Chen, S. Using Thumbprints to Trace Intruders. UC Davis. 1988.
[65] Tan K. *The Application of Neural Networks to UNIX Computer Security.* Proceedings of the IEEE International Conference on Neural Networks. 1995; 476-481.