Detecting Remote to Local User Attacks with High Ratio

Mehmet Ali ATICI
Dept. of Comp. Eng. Fac. of Eng.
Gazi University
Ankara, Turkey
maatici@alumni.bilkent.edu.tr

Ibrahim Alper DOGRU
Dept. of Comp. Eng. Fac. of Tech.
Gazi University
Ankara, Turkey
iadogru@gazi.edu.tr

Seref SAGIROGLU
Dept. of Comp. Eng. Fac. of Eng.
Gazi University
Ankara, Turkey
ss@gazi.edu.tr

Abstract –In context of detecting anomalous traffic and identifying intrusions, many works have been proposed for classification of normal traffic records and attack records consisting of subcategories which are Denial of Service, Probe, Remote to Local User and User to Root. However the detection rate of Remote to Local User attacks is significantly less than other categories. In this work, a binary classification system based on a multilayer perceptron neural network model is proposed to decide whether a connection record is part of Remote to Local User attacks or not. Multilayer perceptron neural network models are trained and tested by KDD'99 dataset. The system pre-processes the dataset, decreases the effect of anomalies of KDD'99, features are then selected by information gain calculation and finally the classification of Remote to Local User attacks is obtained. We used Detection Rate and False Alarm Rate to evaluate the quality of Remote to Local User Attacks Detection System in accordance with the purpose of collection of KDD'99 datasets. In experiments, very high detection rate of Remote to Local User attacks above %92 was attained by eliminating redundant records and balancing the distribution of data. This result is too higher than the other works since well-tuned Artificial Neural Networks could achieve the local minimums. In addition, the proposed model may improve the success of layered approaches in the context of hybrid designs.

Key Words: **Remote to Local User** ***attacks, intrusion detection, artificial neural networks, KDD'99 dataset.***

I. INTRODUCTION

KDD'99 dataset has been collected and distributed by Defense Advanced Research Projects Agency (DARPA ITO) to evaluate intrusion detection systems in terms of detection rate and false alarm rate [17]. It includes normal traffic records and attack records consisting of subcategories which are Denial of Service (DoS), Probe, Remote to Local User (R2L) and User to Root (U2R) [1].

In DoS attacks, intruders consume the processing or memory resources to force the system to deny normal connections [1].

In Probe attacks, intruders scan the devices or services of a network and gather information about them to identify vulnerabilities [1].

In U2R attacks, intruders obtain root privileges to access the system [1].

In R2L attacks, intruders obtain privileges of a local account to access device on the network [1]. The R2L attack connections contain not only the network level but also the host level features and this is why it is mostly difficult to detect them [7].

Full training dataset of KDD'99 contain 4.898.431 records. 1.074.992 of these records are unique. There are 494.021 records in %10 training dataset but only 145.586 of these records are unique, remaining records are redundant. 22 different attack types exist in both training datasets.

There are 311.029 records in test dataset but like the training datasets most of these records are redundant. Only 77.291 of the test records are unique. There are 37 different attack types in test dataset and unique records of training and test datasets include all kinds of attack types.

The attack types included in test dataset and the training dataset are not the same; test dataset includes some attack types not existing in the training data. This difference reflects the real world situations since some novel attacks may be generated from the existing ones [15].

Detection rate of R2L attacks is significantly less than other categories. In this work, a binary classification system based on a multilayer perceptron neural network model is introduced to decide whether a connection record is part of R2L attacks or not.

The paper is organized as follows: In Section 2, literature works are introduced, In Section 3 information about multilayer perceptron neural networks is given, In Section 4, our approach is introduced and implementation details are provided. In Section 5, the results of the evaluation metrics are discussed. Finally, our findings are summarized and future works are mentioned in Section 6.

II. RELATED WORK

There have been a number of works related to intrusion detection in literature [2,4-5,7-11]. Some of these works [2,9] deal with general classification of packets into normal or attack categories while some others concern the detection of specific attack category like Remote to Local User (R2L) attacks [4,7,10,11].

Sagiroglu et al. proposed and developed an intelligent intrusion detection system (IDS) [2]. They designed different IDS models with the help of KDD'99 dataset by using artificial neural network (ANN). The developed IDS models were performed the tasks with high accuracies between %81.93 and %97.92. Kumar and Selvakumar presented an algorithm called NFBoost using hybrid neuro-fuzzy systems to detect Distributed Denial of Service (DDoS) attacks [4]. They used publicly accessible datasets like KDD, UCI etc. in training and testing. Only the normal and Denial of Service (DoS) attack connection records of KDD dataset are used. The system attained high accuracy ratio over 98% in both training and testing on the KDD dataset. Wu and Yen introduced a research to compare evaluation measures like accuracy, detection rate and false alarm rate on KDD'99 dataset but since its data is not balanced, in comparison, different normal data distributions are used in training and test [5]. The research performs better than KDD Winner when particularly compared against User to Root (U2R) and R2L attacks. Gupta et al. reported a layered intrusion detection method using Conditional Random Fields (CRFs) [7]. It uses KDD'99 dataset and applies sequential attack detections in a layered manner. According to experimental results the proposed system based on layered approach performs better than decision trees and the naive Bayes. It provides significant improvements in terms of detection accuracy especially for U2R and R2L attacks. Kuang et al. expressed a new support vector machine (SVM) approach that combines Kernel Principal Component Analysis (KPCA) and genetic algorithm (GA) for intrusion detection [8]. The model implements a multi-layer SVM classifier to predict whether the action is an attack. In experiments, the proposed SVM classifier attains better accuracy and generalization performance. Mukhopadhyay et al. presented a novel Intrusion Detection System (IDS) method using Back-Propagation Neural Network (BPN) [9]. The experiments conducted on KDD'99 dataset and the system performed 95,6% and 73,9% success rates for two test levels correspondingly. Subbulakshmi and Afroze reported a layered approach for attack detection using Correlation Based Feature Selection (CFS) on KDD'99 dataset [10]. The proposed method attained classification ratios for the R2L attacks ranging from 91% to 99%. Sharma and Mukherjee introduced a layered approach combining naïve bayes classifier (NBC) and Naïve Bayes Tree (NBTree) methods particularly to increase precision and detection rate measures regarding U2R and R2L attacks without decreasing the performance of other attacks [11]. They used KDD'99 dataset connection records in training and testing which contains 24 different kinds of attacks.

III. MULTILAYERED PERCEPTRON NEURAL NETWORKS

Artificial Neural Networks (ANNs) imitates the information processing method of human brain as computer programs. ANNs implement learning algorithms to reveal the relationships existing in datasets. There exist numerous neural networks models in the literature but Multilayered perceptron neural networks (MLPNNs) are the most commonly used ones [14].

A MLPNN architecture consists of one input layer, hidden layer(s) and one output layer [13]. Neurons of the input layer directly send the signals to the hidden layer. Each neuron of the hidden layers or output layer sums up its weighted input signals, gives it to the transaction function and produces its output as the result of the this function which may be a sigmoid or a tangent hyperbolic function etc. [13]. The typical topology of Multilayered perceptron neural network (MLPNN) given in Fig. 1.

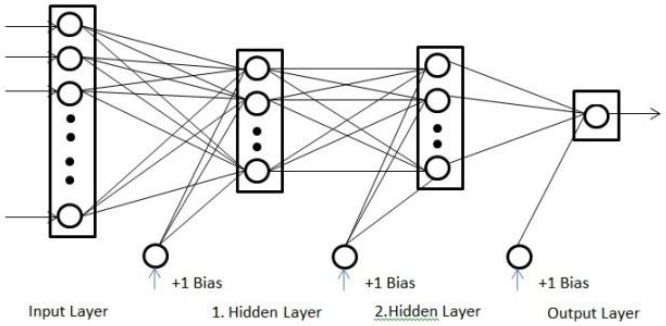

Fig. 1. Backpropagation multilayer perceptron topology.

The MLPNNs are trained by adjusting connection weights through the learning algorithms until the sum of squared errors (difference of target and resultant values of the output neurons) is minimized to an acceptable value [13]. Thus MLPNNs which are capable of revealing complex relations between inputs and targets can obtain different performance values for the same training dataset and reach the local minimums on contrary to the well-known machine learning techniques like decision trees, k-NN and Naïve Bayes.

IV. PROPOSED SYSTEM

The proposed R2L attacks detection system implements an MLPNN as a binary classifier to decide whether a connection record is part of R2L attacks or not. The system consists of four modules as illustrated in Fig. 2.

Database module contains KDD'99 training and test datasets in corresponding tables. As the database of the proposed system, we used PostgreSQL [16] which is an open source database system. By utilizing the database and Java application, the training, validation and test data files are created from the extracted data for different test scenarios. The file system module stores the training and

test data files produced from the KDD'99 dataset tables in database module.

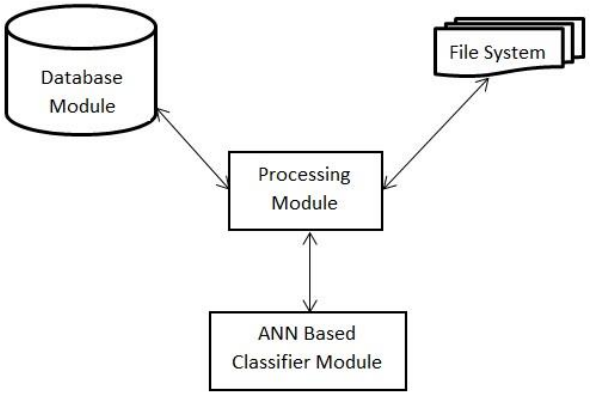

Fig. 2. Proposed Architecture for R2L Attack Detection System

The core units of the system are processing and classifier modules. Processing module is responsible for the transformation of the data, selection of most related features, dealing with the problems of KDD'99 dataset for improving the success rates and preparing the training and test datasets in the file system.

KDD'99 dataset includes 41 data fields apart from the class label. List of these fields is given in Table I. Attack type, protocol type, service type and flag fields are not numeric. Before training and test, these fields are transformed into numeric values.

TABLE I. KDD'99 DATA FIELDS.

KDD'99 Fields
duration, protocol_type, service, flag, src_bytes, dst_bytes, land, dst_host_srv_diff_host_rate, dst_host_serror_rate, dst_host_srv_serror_rate, dst_host_rerror_rate, dst_host_srv_rerror_rate, wrong_fragment, urgent, hot, num_failed_logins, logged_in, num_compromised, root_shell, su_attempted, num_root, srv_rerror_rate, same_srv_rate, diff_srv_rate, srv_diff_host_rate, num_outbound_cmds, is_host_login, is_quest_login, count, srv_count, serror_rate, srv_serror_rate, rerror_rate, dst_host_same_src_prt_rate, dst_host_count, dst_host_srv_count, dst_host_same_srv_rate, dst_host_diff_srv_rate, num_file_creations, num_shells, num_access_files

There are some problems related to KDD'99 datasets that influence the success of classification by ANNs. As given in Section 2, KDD'99 datasets contain significant number of redundant records. This makes learning algorithms of ANNs to be biased to learn from the more frequent records and decrease the positive impact of infrequent but harmful records on success of training [10]. Increasing number of unique samples in the training data makes the trained ANN more robust [6].

In addition to the problem of redundant records, KDD'99 dataset is unbalanced meaning that the distribution of the records on each category is not proportional. A uniform distribution of the training dataset will cause the ANN model to perform well under seldom conditions [6].

It is clear that all features in training dataset may not be useful for classification. Feature Selection is an important process for improving the success of the system. Therefore we used Information Gain calculation to reveal the most distinctive features in the training dataset. Information gain is calculated by entropy. Given a dataset D, entropy is calculated as below [8]:

$$\text{Entropy (D)} = \sum_{i=1}^{c} -P_i \log_2 \mathrm{P}_i \qquad (1)$$

where Pi represents the ratio of the records having class label i to the number of all records and c denotes the number of distinct classes [3]. Entropy of an attribute A with respect to dataset D is calculated as below [19]:

$$Entropy_A(D) = \sum_{v \in Values(A)} \frac{|Dv|}{D} Entropy(Dv) \qquad (2)$$

where v indicates the different values of attribute A and |Dv| denotes the number of the records such that value of A is equal to v. Finally Information Gain of an attribute A is calculated as below [19]:

$$\text{Gain(D, A)} = Entropy(\text{D}) - Entropy_A(\text{D}) \qquad (3)$$

After determining the information gain values of each 41 fields in the training dataset, 13 of them that has the information gain value greater than 0.99 are selected and given in Table II.

TABLE II. SELECTED FEATURES

Selected Features
Duration, Service, Flag, src_bytes, dst_bytes , logged_in, count, srv_count, same_srv_rate, dst_host_count, dst_host_srv_count, dst_host_same_srv_rate, dst_host_same_src_prt_rate

Training Dataset file consists of 2032 records. Each has 14 fields. These records are selected from %10 KDD'99 dataset randomly, 999 of these records are type of R2L attacks and the remaining records consist of normal connection records. Training Dataset is divided into two parts randomly for training and validation. Test data file composed of 76936 records including R2L and normal connection records of KDD'99 test dataset.

Another experiment is also conducted to classify R2L attacks against others (Normal, DoS, PROBE, U2R). Training records are selected from KDD'99 full dataset randomly, nearly half of these records are type of R2L attacks and the remaining records consist of normal and other three attack types (DoS, Probe, U2R) of which numbers are uniformly identified as much as possible. Training Dataset file consists of 2049 records each has 24 fields since 23 features are selected after information gain

calculation as given in Table III. Test data file is composed of all distinct records of KDD'99 test dataset.

R2L Attacks Detection System implements an MLPNN model as a binary classifier to decide whether a network packet is part of R2L attacks or normal. Two different MLPNN models are designed for experiments. MLPNN-1 uses the all 41 features and consists of 41 neurons in input layer, 4 neurons in the hidden layer and one neuron in the output layer.

On the other hand, MLPNN-2 uses only the selected features and input layer of the network consists of 13 nodes, first and second hidden layers consist of 4 and 2 nodes respectively and output layer consists of one node. MLPNN-3 is designed for second experiment and includes 23, 4 and 1 nodes in input, hidden and output layers correspondingly.

TABLE III. SELECTED FEATURES

Selected Features
Duration, protocol_type, Service, Flag, wrong_fragment, count, srv_count, serror_rate, srv_serror_rate, rerror_rate, srv_rerror_rate, same_srv_rate, diff_srv_rate, srv_diff_host_rate, dst_host_count, dst_host_srv_count, dst_host_same_srv_rate, dst_host_diff_srv_rate, dst_host_same_src_prt_rate, dst_host_srv_diff_host_rate, dst_host_serror_rate, dst_host_rerror_rate, dst_host_srv_rerror_rate

Design parameters of these MLPNN models are given in Table IV. MLPNNs like other machine learning models are liable to over fitting but some techniques such as early stopping may help to prevent it [18].

TABLE IV. DESIGN PARAMETERS OF MLPNN MODELS

Parameters	**Model**		
	MLPNN-1	MLPNN-2	MLPNN-3
Number of Input Layer Nodes	41	13	23
Number of Hidden Layer Nodes	4	4 - 2	4
Number of Output Layer Nodes	1	1	1
Ratio of Training Samples	0.85	0.9	0.85
Ratio of Validation Samples	0.15	0.1	0.15
Performance Function	MSE (goal=0)	MSE (goal=0)	MSE (goal=0)
Transfer Function of Hidden Layer	Sigmoid	Sigmoid	Sigmoid
Transfer Function of Output Layer	Linear	Linear	Linear
Number of epochs	3	4	48

So for training the MLPNN models, %10-15 of the samples of dataset are randomly selected and used for validation for early stopping. Training completed without waiting max epochs number which is set to 1000.

V. EVALUATION OF THE PROPOSED SYSTEM

Detection Rate (DR) and False Alarm Rate (FAR) are used to evaluate the quality of R2L Attacks Detection System in accordance with purpose of collection of KDD'99 datasets.

Detection Rate measures the fraction of correctly predicted R2L attacks among R2L attacks on the other hand False Alarm Rate measures the fraction of other connections which are incorrectly classified as R2L attacks among all other connections [5]. Table V. shows the confusion matrix [5] of MLPNN-2 model.

TABLE V. CONFUSION MATRIX.

Confusion Matrix		
	Predicted R2L	Predicted Other
R2L	TP=15057	FN=1288
Other	FP=15292	TN=45299

Given the confusion matrix for training shown in Table 2, detection rate also called as recall [11] and false alarm rate can be formally defined as follows [5]:

$$DR = \frac{TP}{TP+FN} \quad (4)$$

$$FAR = \frac{FP}{FP+TN} \quad (5)$$

All of these measures attained from test results of MLPNN models are listed in Table VI.

TABLE VI. EVALUATION METRICS

Model	DR	FAR
MLPNN-1	0.72	0.25
MLPNN-2	0.92	0.25
MLPNN-3	0.75	0.05

When the results of MLPNN-1 and MLPNN-2 in Table VI are compared it seems that feature selection improves the detection rate significantly and decreases the computational time by reducing dimensions of dataset and input layer of the MLPNN. Detection Rate value of test means that %92 of the R2L attacks can be detected by the system.

The challenging part of KDD'99 dataset is that test dataset has additional attack types which doesn't exist the training dataset. Therefore empirical tests are conducted in this context and detection rates of proposed model are compared with the works in this manner, as given in Table VII.

TABLE VII. COMPARISON OF THE RESULTS

	DR (%) (Selected Features)
Proposed Model	**92**
C4.5 [5]	17.43
SVM [5]	17.46
Layered CRF [7]	27.08
SVM (N-RBF) [8]	24.84
SVM (POLY) [8]	23.91

As seen from Table VII, detection rate values of other works are very low. Especially when compared to the Layered CRF model [7] that have used the same records for test dataset, the proposed MLPNN model obtains very higher result because MLPNNs are capable of revealing complex relations between inputs and targets, they can attain different performance values for the same training dataset and they can reach the local minimums.

VI. CONCLUSIONS AND FUTURE WORK

In this work an ANN based R2L attacks detection system was designed and implemented as a binary classifier to decide whether a connection record is part of R2L attacks or not. The system uses the KDD'99 dataset which is collected to evaluate IDS models in terms of detection rate and false alarm rate [17]. Data processing module of the system removes the redundant records and tunes the distribution of the records in training dataset which are normally unbalanced. Experimental results show that MLPNN models with well-tuned design parameters may attain very high detection rate of R2L attacks above %92 by eliminating redundant records and balancing the distribution of data on KDD'99 training datasets. The attained value of Detection Rate is much higher than the other works as given in Table VII since ANNs could achieve the local minimums.

As for the feature work we will design hybrid layered classifier in binary-binary manner which implements the same data processing issues for attaining higher values even for false alarm rates without hurting performance of detection rate and may use different techniques like MLPNNs, SVMs etc. to integrate the powerful aspects of them for obtaining more accurate results. The designed MLPNN model which attains very high detection rate of %92 for R2L attacks, may be a part of such a hybrid layered approach. In addition, during test of the MLPNNs, we have realized that changing design parameters or initial weights of connections among neurons may result in drastically different performance scores. Therefore designing a well-tuned ANN is as optimization problem. So we are also planning to use optimization algorithms like genetic algorithms or ant colony optimization algorithm for identifying design parameters of neural networks.

APPENDIX

GUTIC is Gazi University Technology and Innovation Center. GUTIC was established on 2012. Professor Sagiroglu currently holds the chair position.

REFERENCES

[1] Internet: http://www.ll.mit.edu/mission/communications/cyber/CSTcorpora/ideval/docs/attackDB.html#u2r, last visited: 16.02.2015

[2] Ş. Sağıroğlu, E.N. Yolaçan, and U. Yavanoğlu, "Zeki Saldırı Tespit Sistemi Tasarımı ve Gerçekleştirilmesi", J. Fac. Eng. Arch. Gazi Univ., vol. 26(2), pp. 325-340, 2011.

[3] C.E. Shannon, "A Mathematical Theory of Communication", The Bell System Technical Journal, vol. 27(3), pp. 379-423, 1948.

[4] P.A.R. Kumar, S. Selvakumar, "Detection of distributed denial of service attacks using an ensemble of adaptive and hybrid neuro-fuzzy systems", Computer Communications, vol. 36, pp. 303-319, 2013.

[5] S.Y. Wu, E. Yen, "Data mining-based intrusion detectors", Expert Systems with Applications, vol. 36, pp. 5605–5612, 2009.

[6] K. Yale, "Preparing the right data diet for training neural networks", IEEE Spectrum, pp. 64-66, 1997.

[7] K.K. Gupta, B. Nath, R. Kotagiri, "Layered Approach Using Conditional Random Fields for Intrusion Detection", IEEE Transactions On Dependable And Secure Computing, vol. 7(1), pp. 35-49, 2010.

[8] F. Kuang, W. Xu, S. Zhang, "A novel hybrid KPCA and SVM with GA model for intrusion detection", Applied Soft Computing, vol. 18, pp. 178–184, 2014.

[9] I. Mukhopadhyay, M. Chakraborty, S. Chakrabarti, T. Chatterjee, “Back Propagation Neural Network Approach to Intrusion Detection System”, 2011 International Conference on Recent Trends in Information Systems, Kolkata, pp. 303-308, December 2011.

[10] T. Subbulakshmi, A.F. Afroze, “Multiple Learning based Classifiers using Layered Approach and Feature Selection for Attack Detection”, 2013 IEEE International Conference on Emerging Trends in Computing, Communication and Nanotechnology (ICECCN 2013), Tirunelveli, pp. 308-314, March 2013.

[11] N. Sharma, S. Mukherjee, “A Novel Multi-Classifier Layered Approach to Improve Minority Attack Detection in IDS”, Procedia Technology, vol. 6, pp. 913–921, 2012.

[12] R. Hunt, S. Zeadally, “Network Forensics: An Analysis of Techniques, Tools, and Trends”, IEEE Computer Society, vol. 45(12), pp. 36-43, 2012.

[13] Ş. Sağıroğlu, U. Yavanoğlu, E.N. Yolaçan, “Web based Machine Learning for Language Identification and Translation”, Sixth International Conference on Machine Learning and Applications, Cincinnati, OH, pp. 280-285, December 2007.

[14] S. Haykin, “Neural Networks: A Comprehensive Foundation”, Macmillan College Publishing Comp., 1994.

[15] Internet: http://kdd.ics.uci.edu/databases/kddcup99/task.html, last visited: 16.02.2015

[16] Internet: http://www.postgresql.org/about/, last visited: 16.02.2015

[17] Internet: http://www.ll.mit.edu/mission/communications/cyber/CSTcorpora/ideval/index.html, last visited: 16.02.2015

[18] S. Lawrence, C.L. Giles, "Overfitting and neural networks: conjugate gradient and backpropagation", IEEE Int. Conf. Neural Networks, Como, pp. 114 -119, 2000.

[19] B. Liu, "Web Data Mining Exploring Hyperlinks, Contents, and Usage Data", Springer, pp. 64-65, 2007.

Mehmet Ali ATICI received his B.Sc degree in Computer Engineering in 2002 from Bilkent University, Ankara, Turkey and his M.Sc. degree in Computer Engineering in 2007 from Gazi University, Ankara, Turkey. He is Ph.D. candidate in Computer Engineering department of Gazi University, Ankara, Turkey. His research interests are data mining, machine learning and cyber security.

Ibrahim Alper DOGRU received his B.Sc degree in computer engineering in 2004 from Atılım University, Ankara, Turkey and a M.Sc. degree in computer engineering in 2007 from Gazi University, Ankara, Turkey and his Ph.D. in electronic-computer education in 2012 from the Gazi University, Ankara, Turkey. He is currently an Assist. Prof. Dr. at Gazi University Department of Computer Engineering. His research interests include mobile network technologies, mobile ad hoc networks, mobile security, and cloud computing system.

Seref SAGIROGLU is professor Department of Computer Engineering at Gazi University. His research interests are intelligent system identification, recognition and modeling, and control; artificial neural networks and artificial intelligence applications; heuristic algorithms; industrial robots; analysis and design of smart antenna; internet, web and information systems and applications; software engineering; information and computer security; biometry, electronic and mobile electronic signature and public-key structure, malware and spyware software. Published over 50 papers in international journals indexed by SCI, published over 50 papers in national journals, over 100 national and international conferences and symposium notice and close to 100 notice are offered in national symposium and workshops. He has three patents and 5 pieces published book. He edited four books. He carried out of a many national and international projects. He hold the many conferences and continues academic studies.