Applying Neural Network to U2R Attacks

Iftikhar Ahmad
DCIS, UTP, Bandar Seri Iskandar, 31750, Tronoh, Perak, Malaysia / DSE, CCIS, King Saud University, P.O. Box 51178, Riyadh 11543, Kingdom of Saudi Arabia
wattoohu@gmail.com

Azween B Abdullah
Department of Computer & Information Sciences, Universiti Teknologi, PETRONAS, Bandar Seri Iskandar, 31750 Tronoh, Perak, Malaysia
azweenabdullah@petronas.com.my

Abdullah S Alghamdi
Department of Software Engineering, College of Computer & Information Sciences, King Saud University, P.O. Box 51178, Riyadh 11543, Kingdom of Saudi Arabia
abdksu@gmail.com

***Abstract*— Intrusion detection using artificial neural networks is an ongoing area and thus interest in this field has increased among the researchers. Therefore, in this paper we present a system for tackling User to Root (U2R) attacks using generalized feedforward neural network. A backpropagation algorithm is used for training and testing purpose. The system uses sampled data from Kddcup99 dataset, an attack database that is a standard for evaluating the security detection mechanisms. The system is implemented in two phases such as training phase and testing phase. The developed system is applied to different U2R attacks to test its performance. Furthermore, the results indicate that this approach is more precise and accurate in case of false positive, false negative and detection rate.**

***Index Terms*—U2R attack, Dataset, Multiple Layered Perceptron, Backpropagation, Detection Rate, Neural Network, False Positive, and False Negative,**

I. INTRODUCTION

The rapid expansion of computer networks and mostly of the Internet has created many security harms. During recent years, a number of attacks on network have dramatically increased .Therefore, securing of network resources are very essential especially U2R attacks. A single U2R attack may cause a big loss of a company. Therefore, protecting company resources (servers, systems & other devices) is very serious from these attacks. In this paper, we propose a model that detects these attacks using a supervised neural network that is backpropagation. The approach is based on classifying good traffic from bad in the sense of U2R. We take different types of U2R attacks samples from standard dataset Kddcup99 for training and some of them for testing the system [2], [3].

In the following sections, we briefly introduce related work, U2R attack and its types, proposed model, implementation, results and discussion, and conclusion. Finally, a suggestion for future research area is provided.

II. RELATED WORK

The detection is very important factor for prevention of any attack. Therefore, accurate detection of attack is very important. A number of attempts have been done in the field of attack detection but they suffered many limitations such as time consuming statistical analysis, regular updating, non adaptive, accuracy and flexibility [18]. Therefore, it is an artificial neural network that supports an ideal specification of an intrusion detection system (IDS) and enhances its performance. As a result, an artificial neural network has become an interesting tool in the applications of attack detection systems due to its promising features [1].

Let us review to some basic concepts and terminologies regarding our research. An unauthorized user who tries to enter in network or computer system is known as intruder. A system that detects and logs in appropriate activities is called as intrusion detection system. The intrusion detection system can be classified into three categories as host based, network based and vulnerability assessment based. A host based IDS evaluates information found on a single or multiple host systems, including contents of operating systems, system and application files. While network based IDS evaluates information captured from network communications, analyzing the stream of packets traveling across the network. Packets are captured through a set of sensors. Vulnerability assessment based IDS detects vulnerabilities on internal networks and firewall [4].

Moreover, intrusion detection is further divided into two main classes such as misuse and anomaly detection. First is the general category of intrusion detection, which works by identifying activities which vary from established patterns for users, or groups of users. It typically involves the creation of knowledge bases which contain the profiles of the monitored activities. The second technique involves the comparison of a user's activities with the known behaviors of attackers attempting to penetrate a system. Misuse detection also utilizes a knowledge base of information [5]. Mostly attack detection tools use the evaluation parameters such as false positive, false negative and detection rate. A false positive occurs when the system classifies an action as anomalous (a possible intrusion) when it is a legitimate action. While a false negative occurs when an actual intrusive action has occurred but the system allows it to pass as non-intrusive behavior [6].

Denning proposed an intrusion detection model in 1987 which became a landmark in the research in this area. The model which she proposed forms the basic core of most intrusion detection methodologies in use today [10]. After this a lot works had been done in this field of intrusion in the form of statistical approaches, rule based, graphical and hybrid system. All of these approaches have limitations as described previously in the background section. Presently researchers are taking much interest in the application of attack detection tools by using neural networks due to its

features. An artificial neural network consists of a group of processing elements (neurons) that are highly interconnected and convert a set of inputs to a set of preferred outputs [7-11]. The first artificial neuron was formed in 1943 by the neurophysiologist Warren McCulloch and the logician Walter Pits [12].

Artificial neural networks are alternatives [19]. The first advantage in the use of a neural network in the attack detection would be the flexibility that the network would provide. A neural network would be capable of analyzing the data from the network, even if the data is incomplete or unclear. Similarly, the network would possess the ability to conduct an analysis with data in a non-linear fashion. Further, because some attacks may be conducted against the network in a coordinated attack by multiple attackers, the ability to process data from a number of sources in a non-linear fashion is especially important.

The problem of frequently updation of traditional attack detector is also minimized by ANN. It has generalization property and hence able to detect unknown and even variation of known attacks. Another reason to employ ANN in U2R attack detection is that, ANN can cluster patterns which share similar features, thus the classification problem in attack detection can be solved by ANN. The natural speed of neural networks is another advantage [13].

A systematic review in the field of intrusion detection using artificial neural networks is described in [1], in which different approaches are analyzed in terms of development, implementation, NN architecture, dataset and testing parameter details. This paper also point out many issues in current traditional as well as intelligent attack detection systems. There are many works in the literature that deal with attack detection in networks but the application of artificial neural networks is a new area in this field.

One of the major challenges for present intrusion detection approaches is to reduce false alarm rates. The false alarm rate is still high for recent neural intrusion detection approaches because they have not sufficient ability to attacks. Aikaterini Mitrokotsa et.al worked on attack detection by using ESOMS that is widely used in this field but the problem is performance accuracy as false positives and false negatives increases [14]. Another work on intrusion detection is done by Stefano Zanero et.al. They also used the SOMS in their experiments with 75% detection rate and but it also suffered increase in false positives [15]. L. Prema Rajeswari et.al worked on intrusion detection and their developed model showed 83.59% accuracy with 16.41% false alarm in terms of attacks.

A detailed comparative study of several anomaly detection schemes was given in [16] for identifying different network intrusions; the comparison of density based local outliers (LOF), nearest neighbor (NN) and Mahalanobis-distance-based outlier detection was reported; the published results indicated that the most promising technique is the LOF approach using both simulation and real network data.

In [17], an experimental framework was developed for comparative analysis of both supervised and unsupervised learning techniques including C.45, multi-layer perceptron (MLP), K-nearest neighbour (KNN), etc; the best approach using C.45 algorithm achieved 95% DR with 1% FPR.

III. U2R ATTACK AND ITS TYPES

User to root attack involves unauthorized access to local super user privileges by a local unprivileged user. Examples of such attacks are Loadmodule, Perl and Buffer overflow.

Loadmodule: This attack exploits a flaw in how SUNOS 4.1 dynamically load modules. This flaw makes it possible for any user of the system to get root privileges.

Perl: Exploits a bug in some PERL implementations on some earlier systems. This bug consists in these PERL implementations improperly handling their root privileges. This leads to a situation where any user can obtain root privileges.

Buffer overflow: Consists in overflowing input buffers in order to overwrite memory locations containing security relevant information.

TABLE 1
SAMPLES OF EXEMPLARS

Type	Signatures
Buffer overflow	198,tcp,telnet,SF,2442,10661,0,0,0,2,0,1,6,1,0,4,0,0,0,0,0,0,1,1,0.00,0.00,0.00,0.00,1.00,0.00,0.00,255,1,0.00,0.37,0.00,0.00,0.00,0.00,0.00,0.00,
Perl	84,tcp,telnet,SF,277,1089,0,0,0,2,0,1,1,1,0,0,4,2,0,0,0,0,1,1,0.00,0.00,0.00,0.00,1.00,0.00,0.00,255,1,0.00,0.07,0.00,0.00,0.14,0.00,0.86,0.00
Load module	62,tcp,telnet,SF,2615,4233,0,0,0,5,0,1,2,1,0,0,0,0,0,0,0,0,1,1,0.00,0.00,0.00,0.00,1.00,0.00,0.00,255,1,0.00,0.07,0.00,0.00,1.00,0.00,0.00,0.00
Normal	0,udp,private,SF,105,146,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1,1,0.00,0.00,0.00,0.00,1.00,0.00,0.00,255,254,1.00,0.01,0.00,0.00,0.00,0.00,0.00,0.00

U2R attacks may result in significant loss of time and money for many organizations. Therefore, the detection of such attacks is very important to ensure security in computer and network systems.

IV. PROPOSED MODEL

The proposed model uses feedforward approach. A feedforward neural net is composed of a number of consecutive layers/components, each one connected to the next by a synapse/connection. The design is a FFNN (feedforward neural network) with three layers connected with synapses. Each layer is composed of a certain number of neurons, each of which has the same characteristics (transfer function, learning rate, etc). This multiple layered perceptron architecture consists of one input, one hidden and one output layer. The architecture of the system is shown in Fig. 1.

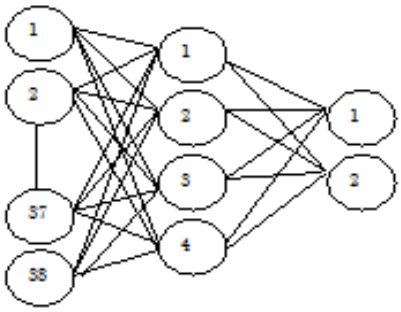

Figure 1. Proposed NN model

The input layer consists of 38 neurons because we selected 38 features out of 41 from the Kddcup99 data set. The other three features have symbolic values so we can remove and these features will have no any impact on results. The hidden layer consists of 4 neurons. The output layer consists of two neurons that classify normal packets from abnormal packets. The Input layer takes input from the input file that contains data for training. The hidden layers take inputs from the outputs of the input layer and apply its activation function. After this the output is sent to the output layer. The output layer allows a neural network to write output patterns in a file that are used for analysis of attacks [3, 13].

V. IMPLEMENTATION

The proposed system is implemented using NeuroSolutions as shown in Fig. 2.

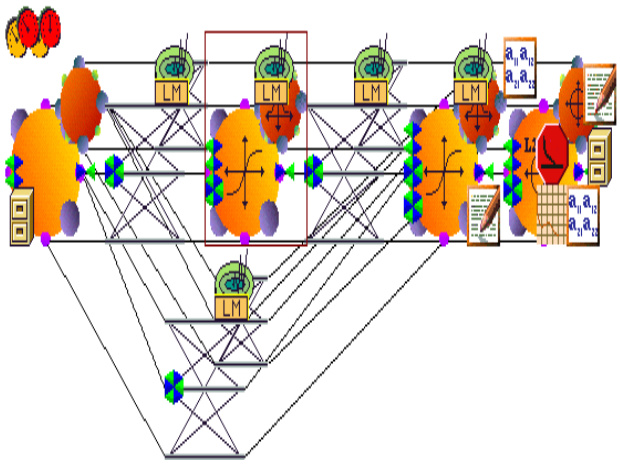

Figure 2. Generalized feedforward NN architecture

The developed NN consists of different components; Axon, TanhAxon, FullSynapse, L2Criterion, BackAxon, BackTanhAxon, BackfullSynapse, BackCriteriaControl, LinearMomentum, StaticControl, BackControl, File, Threshhold Transmitter, DataGraph, MatrixViewer, and DataWriter. Each component of NN performs a specific task during training and testing phases. The implemented system uses the following parameters as shown in Table.

TABLE 2
PARAMETERS USED BY THE SYSTEM

Name of Parameter (s)	Value(s)
Input Processing Elements (PEs)	38
Hidden Processing Elements (PEs)	4
Output Processing Elements (PEs)	2
Exemplars	200
Cross validation	10%
Training data for test	10%
Transfer function	TanhAxon
Learning Rule	LevenbergMarqua
Epochs	1000
Termination MSE Threshold	0.01

The system consists of two phases such as training and testing.

A. Training the System

In the training phase we have both input patterns and desired outputs related to each input vector. Aim of the training is minimizing output produced by the neural network and the desired output. In order to achieve this goal, weights are updated by carrying out certain steps known as training. When using a supervised learning algorithm backpropagation, training process is usually terminated when the MSE is reduced to an acceptable level. There is no standard for the MSE, but usually the lower it is, the better the classification rate is. We used 38 featured packets of U2R attacks from kddcup99 data set [3, 7]. We used Backpropagation algorithm for training of the net because it converges very quickly. The aim of training means to get good responses to input that is similar but not identical. The training algorithm for normal packet is described here.

$$p1, p2, p3, - - - - pn \in D$$

Where "p" is a normal packet of dataset D

$$p1 \rightarrow NN \rightarrow T$$

Where "NN" denotes Neural Network and "T" indicates Target output

$$If co(p) \approx T \text{ then}$$

Where "co" indicates computed output

$$NN \text{ is trained}$$

$$else$$

$$backpropagated\ of\ error;$$

$$adjustment\ of\ weights;$$

The training algorithm for intrusive packet is described here.

$pt1, pt2, pt3, - - - - ptn \in D$

Where pi indicates intrusive packet of dataset D

$pt1 \rightarrow NN \rightarrow T$

Where "NN" denotes Neural Network

$If\ co(pi) \approx T\ then$

Where "co" indicates computed output

$NN\ is\ trained$

Where "T" indicates target output

$else$

$backpropagated\ of\ error\ to\ NN;$

$adjustment\ of\ weights\ of\ NN;$

B. Testing the System

After the training is completed, the weights of the neural networks are frozen and performance of the neural networks is evaluated. Testing the neural networks involves two steps, which are verification step and recall or generalization step. In verification step, neural networks are tested against the data which are used in training. Aim of the verification step is to test how well trained neural networks learned the training patterns in the training dataset.

If a neural network was trained successfully, outputs produced by the neural network would be similar to the actual outputs. In recall or generalization step, testing is conducted with data which not used in training. Aim of the generalization step is to measure generalization ability of the trained network. After training, the net only involves computation of the feedforward phase. The testing algorithm for intrusive/normal packet is described here.

$pi/p \rightarrow NN \rightarrow C$

Where pi/p indicates intrusive/normal packet

$If C \approx 0\ \&1\ then$

Where "C" is classification as produced by trained NN

$packet\ is\ p\ (normal);$

$else\ If C \approx 1\ \&0\ then$

$packet\ is\ pi\ (intrusive);$

$else$

$false\ alaram;$

VI. RESULTS AND DISCUSSIONS

After the training process was completed, testing was conducted. Performance of the NN was evaluated by examining the number of false positives and false negatives on training and testing data. The testing parameters; true positive, true negative, false positive and false negative are used in this work. The efficiency of system is shown in the Table 3.

TABLE 3
PERFORMANCE OF NEURAL NETWORK

Dataset	True positive	True negative	False positive	False negative
Training	100	98.36	0.0	1.64
Testing	95.45	100	4.55	0.0

Correctly predicted attacks= 95.45 (1)
Incorrectly predicted attacks =4.55 (2)
Total=95.5+4.55=100 (3)
Correctly predicted normal packets= 100 (4)
Incorrectly predicted normal packets =0.0 (5)
Total=100+0.0=100 (6)
So,
Correct prediction=95.45+100=195.45 (7)
Incorrect prediction=4.55+0.00=4.55 (8)
Total=200 (9)
The error rate =4.55/200=0.02275 (10)
The accuracy rate =195.45/200=0.9775 (11)

The system shows optimum performance in case of true positives and true negatives as shown in Table 1 that is promising value in case of U2R attack detection. It has been noted that the backpropagation shows best performance as compared to other NN approaches towards attack detection. The focus of our research was to increase attack detection rate. Once attack is detected then there are several available methods to block network attack.

A performance comparison among various approaches is shown in Table 4. The results indicate that adopting generalized feedforward using backpropagation is a feasible that satisfies optimal performance.

TABLE 4
PERFORMANCE COMPARISION WITH OTHER APPROACHES

NN	Detection Rate	False alarms
K-NN	91.88%	8.11%
LOF	73.8%	26.2%
SOMS	75%	25%
GFF	97.725%	2.275%

VII. CONCLUSION

In this paper, a network intrusion detection model is proposed and implemented using generalized feedforward neural network. The backpropagation algorithm is used to train the neural network for U2R attack detection. The dataset used is Kddcup that consists of U2R intrusive packets. The system uses 38 features out of 41 features of the dataset. The symbolic features can be removed and it has no any impact on the performance of the NN. The implemented system is suitable for both misuse and

anomaly detection. The experiments are carried out to indicate the performance of the proposed model on Kddcup dataset. The comparative results prove that the performance of our model outperforms most of the listed approaches in the literature.

VIII. FUTURE RESEARCH

The practical attack detection approach may be developed that have very low error rate, high learning rate and rapid attack detection by using this approach with other neural networks in the form of hybrid architecture such as Genetic Algorithm (GA) or Principal Component Analysis (PCA) with NN.

ACKNOWLEDGMENT

This paper is supported by department of Software Engineering, College of Computer & Information Sciences, King Saud University, Saudi Arabia. Special thanks to honorable Supervisor, Chairman SE, and Dean CCIS, for providing, research environment as well as their kind supervision in this paper.

REFERENCES

[1] Iftikhar Ahmad, Azween B. Abdullah, Abdullah S. Alghamdi, "Artificial Neural Network Approaches to Intrusion Detection: A Review", in the Book TELECOMMUNICATIONS and INFORMATICS", Included in ISI/SCI Web of Science and Web of Knowledge, Istanbul, Turkey, 2009, pp 200-205.

[2] Iftikhar Ahmad, Azween B. Abdullah, Abdullah S. Alghamdi, "Application of Artificial Neural Network in Detection of DOS Attacks", ACM International Conference on Security of Information and Networks (SIN 2009), 6-10 October 2009, Gazimagusa, North Cyprus, Turkey, 229-234.

[3] Erland. Jonsson, Magnus. Almgren, Alfonso, Recent Advances in Intrusion Detection: 7th International Symposium, RAID 2004, Sophia Antipolis - Page 102.

[4] Iftikhar Ahmad, Azween B. Abdullah, Abdullah S. Alghamdi, "Application of Artificial Neural Network in Detection of Probing Attacks", 2009 IEEE Symposium on Industrial Electronics and Applications (ISIEA 2009), October 4-6, 2009, Kuala Lumpur, Malaysia, pp.557-562.

[5] John McHugh, Testing Intrusion detection systems. ACM Transactions on Information and System Security, 3(4). November, 2000.

[6] Morteza Amini, Rasool Jalili and Hamid Reza Shahriari, "RT-UNNID: A practical solution to real-time network-based intrusion detection using unsupervised neural networks", Computers & Security Volume 25, Issue 6, Elsevier Inc, September 2006, pp 459-468.

[7] The 3rd International Knowledge Discovery and Data Mining Tools Competition, website link accessed 2009, http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html.

[8] M. Sabhnani and G. Serpen, "Application of Machine Learning Algorithms to KDD Intrusion Detection Dataset within Misuse Detection Context", http://www.eecs.utoledo.edu/~serpen/.

[9] Denning, Dorothy. (February, 1987). An Intrusion-Detection Model. IEEE Transactions on Software Engineering, Vol. SE-13, No. 2.

[10] Uwe Aickelin, Julie Greensmith, Jamie Twycross, "Immune System Approaches to Intrusion Detection – A Review" Natural Computing, Springer Netherlands, Volume 6, Number 4 / December, 2007, pp 413-466.

[11] Laurene Fausett, Fundamentals of Neural Networks Architecture, Algorithm, and Applications, Pearson Education, Inc. 2008, pp. 21-24.

[12] Iftikhar Ahmad, Azween B. Abdullah, Abdullah S. Alghamdi, "Comparative Analysis of Intrusion Detection Approaches", IEEE UKSIM2010, March 24 – 26 2010, Cambridge University (Emmanuel College), England, pp.586-591.

[13] Aikaterini Mitrokotsa, Christos Douligeris, "Detecting Denial of Service Attacks Using Emergent Self-Organizing Maps", IEEE International Symposium on Signal Processing and Information Technology 2005, pp 375-380.

[14] Stefano Zanero, Sergio M. Savarsi, "Unsupervised learning techniques for an intrusion detection system" ACM Symposium on Applied Computing, Cyprus 2004,pp 412-419

[15] L.Prema Rajeswari, A.Kannan, "An inrusion detection System Based on Multiple Level Hybrid Classifier using Enhanced C045" IEEE-INTERNATIONAL CONFERENCE on Signal processing, Communications and Networking madras Institute of Technology, Anna University chemai india, 2008, pp 75-79

[16] A. Lazarevic, L. Ertoz, V. Kumar, A. Ozgur, J. Srivastava, A comparative study of anomaly detection schemes in network intrusion detection, in: Proceedings of the Third SIAM Conference on Data Mining, 2003.

[17] L. Pavel, D. Patrick, S. Christin, K. Rieck, in: Learning Intrusion Detection: Supervised or Unsupervised, Lecture Notes in Computer Science, vol. 3617, Springer, Berlin, Heidelberg, 2005, pp. 50–57.

[18] Iftikhar Ahmad, Azween B. Abdullah, Abdullah S. Alghamdi, Evaluating Intrusion Detection Approaches Using Multi-criteria Decision Making Technique, Information Sciences and Computer Engineering(IJISCE), Australia, vol.1, no.1, pp.60-67, 2010.

[19] Iftikhar Ahmad, Azween B. Abdullah, Abdullah S. Alghamdi, "Towards the designing of robust IDS through an optimized advancement of neural networks", Advances in Computer Science and Information Technology, LNCS, Vol.6059, Springer Berlin / Heidelberg, , 2010, pp.597-602.