Intrusion Detection with On – line Clustering Using Reinforcement Learning

Indah Yulia Prafitaning Tiyas, Ali Ridho Barakbah, Tri Harsono, Amang Sudarsono
Postgraduate Applied Engineering of Technology
Division of Information and Computer Engineering, Department of Information and Computer Engineering, Electronic Engineering Polytechnic Institute of Surabaya (EEPIS)
EEPIS Campus, Jalan Raya ITS, Sukolilo 60111, Indonesia
Telp :+62(31)5947280, Fax:+62(31)5946114
indahyuliap@yahoo.com, ridho@eepis-its.edu, trison@eepis-its.edu, amang@eepis-its.edu

Abstract

Today, information technology is growing rapidly, we can obtain all the information much easier. Almost all the important information can be accessed by the users. These conditions raise some new problems, one of them is unauthorized access to the system. We need a reliable network security system that is resistant to a variety of attacks against the system. Therefore, Intrusion Detection System (IDS) required to overcome the problems of intrusions. Many researches have been done on intrusion detection using classification methods. Classification method has high precision, but to get a high precision required a determination of the proper classification model. In this paper, we propose a new approach to detect intrusion with On-line Clustering using Reinforcement Learning. Based on the experimental result, our proposed technique can detect intrusions with high accuracy (99.996% for DoS, 99.939% for Probe, 99.865% for R2L and 99.948% for U2R) and high speed (65 ms).

Keywords: Intrusion Detection System, On-Line Clustering, Reinforcement Learning, Unsupervised Learning.

1. Introduction

Based on data compiled by the CERT [8], the number of intrusions from year to year is increase. From 1995 to 2008, the total attack as summarized by CERT is 46.156, as illustrated in figure 1:

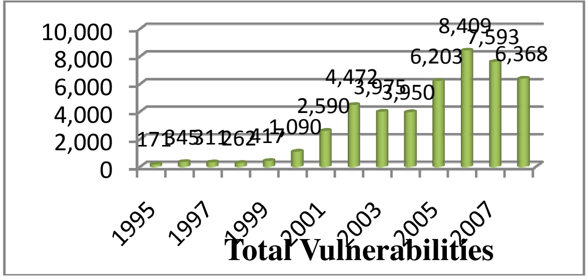

Figure 1. The number of intrusions summarized by CERT[8]

Meanwhile, according to data analyzed by Carnegie Mellon University (2002) and Idaho National Laboratory (2005), intruder technical knowledge decreases, as illustrated in figure 2:

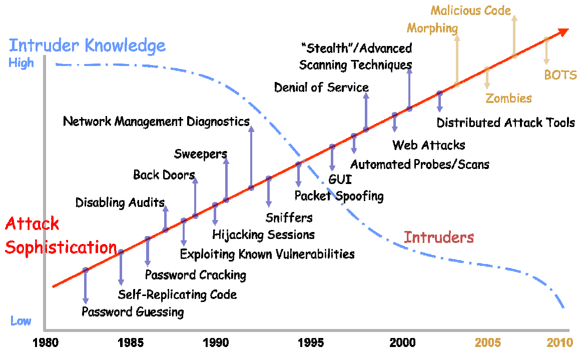

Figure 2. Decreasing Intruder Technical Knowledge[9]

Therefore, Intrusion Detection System (IDS) required to overcome the problems of intrusion. The system that detects and logs illegal access is called as intrusion detection system [1]. There are three categories of intrusion detection systems which are host-based where information is found on a single or multiple host systems, network- based that examines the information captured from network communications and vulnerability assessment-based that identifies vulnerabilities in internal networks and firewall, whereas based on the functionality intrusion detection can be classified into two as anomaly detection and misuse detection [1].

Misuse detection is a system that works by comparing the packet traffic on the computer network with signature database. The weakness of misuse detection is not able to detect any new attacks because the attack was not found in the signature database such that late in detecting the attack. In addition, the administrator must manually update signature database. Anomaly detection is a system that comparing the packet traffic on the computer network with a normal traffic pattern, but it has the disadvantage of sending a lot of false positives and can be fooled by the actual attack. Anomaly detection will identify how much bandwidth, protocol, ports that are normally used. If the system detects an abnormal, it will send alerts to the administrator.

There are four categories of attacks, namely Denial Of Service (DOS), Remote to local (R2L), User to Root (U2R) and Probe with the following explanation [1]:

- Denial of Service (DOS) Attacks: DOS attack is an attack where as the attacker creates a few calculations or memory resource completely engaged or out of stock to handle authentic requirements, or reject justifiable users the right to utilize a machine.
- User to Root (U2R) Attacks: These are a category of attack where an attacker begins by accessing normal user account in the system (maybe attained by hunting the passwords, by social engineering or by attacking dictionary) and get advantage of several vulnerability to accomplish root entrée to the system.
- Remote to local (R2L) Attacks: R2L attack occurs when an intruder who has the potential to send packets to a system/machine over a network without having an account in that system/machine, makes use of a few vulnerability to accomplish local access as a client of that system/machine.
- Probes (PROBE) Attack: Probing is a collection of attacks where an attacker scrutinizes a network to gather information or to conclude prominent vulnerabilities.

Many researchs in intrusion detection have been done using various techniques, and some of them have inspired us to take up this research. A. M. Chandrashekhar and K. Raghuveer [1] proposed hybrid intrusion detection system which combining Fuzzy C-Means, Neuro-Fuzzy Classifier (NF), SVM Vector Generator and Radial Basis Function (RBF) SVM. The accuracy rate reaches 98.94% for DOS attack and 97% for the other attack types (Probe, U2R, R2L). A.S. Aneetha and Dr S. Bose [2] proposed hybrid intrusion detection system which combining Self Organizing Map (SOM that has been modified) with Fuzzy K-Means Clustering. The accuracy rate reached 98.5% for DOS attack. Prof. Dr. Kais Said Al-Sabbagh [3] proposed Self Organizing Map (SOM) which can reduce false positives from 44.676% to 5.176%. Shaker Reyadh Namh Naoum and Zainab Al – Sultani [4] proposed a hybrid intrusion detection system that combines methods Learning Vector Quantization (LVQ) and Enhanced Resilient Backpropagation Artificial Neural Network. The accuracy rate reached 98.4 % for DoS , 99.59 % for Probe , 96.4 % for R2L , 70.3 % for U2R. Amir Azimi Alasti Ahrabi, Kaveh Feyzi, Zahra Atashbar Orang, Hadi Bahrbegi, and Elnaz Safarzadeh[5] proposed a new alert management system by using Learning Vector Quantization (LVQ). The results of the proposed system are compared to GA based techniques. The comparison shows that in contrast of GA based systems LVQ algoritm can be used in active alert management systems. Reyadh Shaker Naoum and Zainab Namh Al-Sultani[6] proposed hibrid intrusion detection system which combining Learning Vector Quantization artificial neural network with k-Nearest Neighbor approach to detect intrusion. The experiments and evaluations of the proposed method have been performed using the NSL-KDD 00 intrusion detection dataset. Hybrid (LVQ-kNN) was able to classify the datasets into five classes at learning rate 0.09 using 23 hidden neurons with classification rate about 89%.

Many research have done using classification method. Classification method have high precision but needed appropriate classification model. We propose new approach for detecting intrusions with On-Line Clustering which can perform clustering in real-time with high accuracy in detecting intrusions. Method of On-Line Clustering that used in this research is Reinforcement Learning. Reinforcement Learning is a learning machine that is able to be smart after interacting with the environtment, the more interaction, the more smart. The technique is expected to detect new attacks in realtime with higher speed and higher accuracy than previous research and can help network administrators in detecting intrusion in a computer network.

2. Previous Works

Many researches in intrusion detection have been done using various techniques. A brief description of some researches that inspire us, such as:

A. M. Chandrashekhar and K. Raghuveer [1], “Fortification of Hybrid Intrusion Detection System Using Varians of Neural Networks and Support Vector Machines” (January, 2013) proposed hybrid intrusion detection system which combining Fuzzy C-Means, Neuro-Fuzzy Classifier (NF), SVM Vector Generator and Radial Basis Function (RBF) SVM. In the first step, Fuzzy C-Means Clustering is performed to classify the KDD Cup 1999 dataset into various types of attacks (i.e., DOS, Probe, U2R, R2L) and normal data. Furthermore, each data trained by using Neuro-Fuzzy Classifier according to its cluster. Then, the vector for SVM classification is produced by the SVM Vector Generator. For the formation of vectors, each of the data is passed through all of ‘K’ trained neural networks. Each data receive ‘K’ attribute value after passing through ‘K’ neural networks. Value of the membership function of the data is discovered and added to the list of attributes in order to reduce the errors and improve results. And in the last step, the classification using the RBF-SVM was performed to detect intrusion. The accuracy rate reaches 98.94% for DOS attack and 97% for the other attack types (Probe, U2R, R2L).

A. S. Aneetha and Dr S. Bose [2], "The Combined Approach for Anomaly Detection using Neural Networks and Clustering Techniques" (August, 2012) proposed hybrid intrusion detection system which combining Self Organizing Map (SOM that has been modified) with Fuzzy K-Means Clustering. SOM is used to map the multi-dimensional nonlinear data into two dimensional data as output. In the modified SOM, the weakness of the SOM can be improved by allowing the network to grow with the distance threshold, and also by using the connection strength to identify the neighbourhood nodes. In the Fuzzy K-Means Clustering, nodes that have been created by the SOM are grouped into K clusters based on the distance, with their weight vector values as seed points. The accuracy rate reaches 98.5% for DOS attack.

Prof. Dr. Kais Said Al-Sabbagh [3], "Development an Anomaly Network Intrusion Detection System Using Neural Network" (December, 2012) proposed Self Organizing Map (SOM) to improve payload anomaly detector (PAYL). By combining two stages with the PAYL detector, it gives good detection ability and acceptable ratio of false positive. The proposed system improve the models recognition ability in the PAYL detector, for a filtered unencrypted HTTP subset traffic of DARPA 1999 dataset, from 55.234% in the PAYL system alone to 99.94% in the proposed system. In addition, SOM decreases the ratio of false positive from 44.676% in the PAYL stand alone system to 5.176% in the proposed system. The proposed system provides 80% detection ability of smart worms that are meant to invade the PAYL detector in the PAYL stand alone system, due to the existence of the randomization stage in the proposed system.

Shaker Reyadh Namh Naoum and Zainab Al-Sultani [4], "Hybrid System of Learning Vector Quantization and Enhanced Resilient Back-propagation Artificial Neural Network Classification for Intrusion" (February, 2013) proposed a hybrid intrusion detection system that combines methods Learning Vector Quantization (LVQ) and Enhanced Resilient Back-propagation Artificial Neural Network. Learning Vector Quantization is a method to train a supervised competitive layer . LVQ greatly affected by how many patterns that correspond to each major class. After the training process, LVQ ready to classify the test dataset. LVQ to classify the dataset into 5 classes (Normal , DoS, U2R , R2L and Prob) . Then the results of LVQ will be combined with the results of the method Enhanced Resilient Back-propagation Artificial Neural Network to provide the maximum level of classification. The level of accuracy reached 98.4 % for DoS , 99.59 % for Probe , 96.4 % for R2L , 70.3 % for U2R.

Amir Azimi Alasti Ahrabi, Kaveh Feyzi, Zahra Atashbar Orang, Hadi Bahrbegi, and Elnaz Safarzadeh[5], "Using Learning Vector Quantization in Alert Management of Intrusion Detection System" (2012) proposed a new alert management system by using Learning Vector Quantization (LVQ). It classifies the generated alerts based on attack type of alerts, detects false positive alerts, high speed classification to use with alert generation in IDSs. The proposed system uses some technique of previous work techniques such as alert filtering, alert preprocessing, and alert filtering to improve accuracy of the results. The system solved some problem of IDSs such as generating high amount of alerts and false positive alert. The system could classify true positive alert and could identify false positive ones. The system identifies and dramatically reduces the number of false positive alerts. The results of the proposed system are compared to GA based techniques. The comparison shows that in contrast of GA based systems LVQ algorithm can be used in active alert management systems.

Reyadh Shaker Naoum and Zainab Namh Al-Sultani[6], "Learning Vector Quantization (LVQ) and k-Nearest Neighbor for Intrusion Classification" (2012) proposed hybrid intrusion detection system which combining Learning Vector Quantization artificial neural network with k-Nearest Neighbor approach to detect intrusion. A supervised Learning Vector Quantization (LVQ) was trained for the intrusion detection system; it contains a specific number of neurons which are the sub attack types and the main attack types respectively. k-Nearest Neighbor (kNN) as a machine learning algorithm was implemented using different distance measures and different k values, but the results demonstrates that using the first norm instead the second norm and using k=1 gave the best results among other possibilities. The experiments and evaluations of the proposed method have been performed using the NSL-KDD 00 intrusion detection dataset. Hybrid (LVQ-kNN) was able to classify the datasets into five classes at learning rate 0.09 using 23 hidden neurons with classification rate about 89%.

3. Originality

An Intrusion Detection System (IDS) is a software or hardware tool used to detect unauthorized access of a computer system or network[10]. Many research have done using classification method. Classification method have high precision but needed appropriate classification model.

We propose new approach for detecting intrusions using On-Line Clustering which can perform clustering in real-time with high accuracy in detecting intrusions. Method of On-Line Clustering that used in this research is Reinforcement Learning. Reinforcement Learning is a learning machine that is able to be smart after interacting with the environtment, the more interaction, the more smart. The technique is expected to detect new attacks in realtime with higher speed and higher accuracy than previous research and can help network administrators in detecting intrusion in a computer network.

4. System Design

In this research, we propose new approach to detect intrusion using On-Line Clustering. The proposed system will be trained using 10% KDD Cup 1999 dataset. We use 100000 data points with composition: normal=25000 and intrusion=75000 (DoS=69715, Probe=4107, R2L=1126, U2R=52). The number of cluster=5 (0=Normal, 1=DoS, 2=Probe, 3=R2L, 4=U2R). The proposed system divided into 3 phases: data pre-processing phase, on-line clustering phase and performance evaluation phase.

Here is a Block Diagram System shown in figure 3:

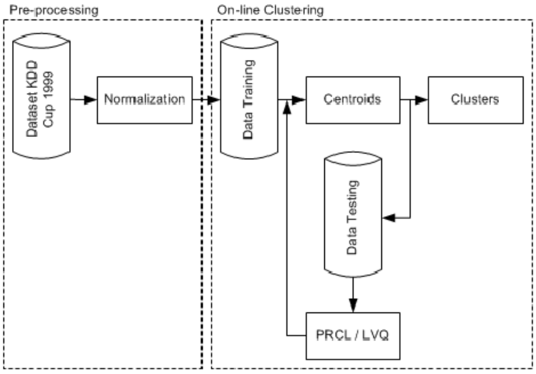

Figure 3. Block Diagram System

4.1. Data Pre-processing Phase

KDD Cup 1999 dataset consists of moderately around 5 million vectors single correlation vectors, where each single connection vector consisting of 41 features and is marked as a normal or an attack, through accurately one particular attack type [1].

Features columns 2, 3, 4 (symbolic) transformed to numeric values using transformation table. Table A, B, C in appendix explains the transformation table.

Label (column 42) contains label of normal and attack. Table D in appendix explains the transformation table for label.

4.2. On-line Clustering Phase

We use Pursuit Reinforcement Competitive Learning (PRCL) which compared with Learning Vector Quantization (LVQ). We utilized the pursuit algorithm in Reinforcement Learning to select the winning weight factors. Therefore, we call as Pursuit Reinforcement Competitive Learning (PRCL) [7].

The algorithm of PRCL is described as follows [7]:

a. First of all, we determine the winning unit i* from:

$$d_{i*} = \arg\min_i d(x, w_i) \qquad (1)$$

b. Update the reward track of x for all weights, as follows:

$$r(x, w_{ij}) = r(x, w_{ij}) + \beta\ (1 - r(xj, w_{ij}))\ \text{if } i = i*$$

and $r(x, w_{ij}) = r(x, w_{ij}) + \beta\ (0 - r(xj, w_{ij}))\ \text{if } i \neq i*$ (2)

c. Select the winning i* from maximizing the reward as :

$$w_{i*} = \arg\max_i r(x, w_i) \qquad (3)$$

d. Update the weight vectors as follows:

$$\varnothing w_{ij} = a\ (x_j - w_{ij}) \quad \text{if } i = i*$$

and $\varnothing w_{ij} = 0 \quad \text{if } i \neq i*$ (4)

where a is learning rate, β is reward rate, d is distance, r is reward, x is data.

Vector quantization is one example of competitive learning. The goal here is to have the network "discover" structure in the data by finding how the data is clustered. The results can be used for data encoding and compression. One such method for doing this is called vector quantization [7].

Algorithm of Vector Quantization can be described as follows [7]:

a. Choose the number of clusters M

b. Initialize the prototypes $w_{1*} \ldots w_{m*}$ (one simple method for doing this is to randomly choose M vectors from the input data)

c. Repeat until stopping criterion is satisfied:
   - Randomly pick an input x
   - Determine the "winning" node k by finding the prototype vector that satisfies
     $| w_{m*} - x |\ £\ | w_{i*} - x |$ (for all i) (5)
   - Update only the winning prototype weights according to
     $w_{k*} = w_{k*} + m\ (x - w_{k*})$ (6)

4.3. Performance Evaluation Phase

We use accuracy to evaluate the performance of the proposed system. Firstly, we calculate confusion matrix, such as: True Positive (TP), False Negative (FN), True Negative (TN) and False Positive (FP). The table 6 explains the confusion matrix. Table 7 explains the definision of TP, TN, FP, FN.

Table 6. Confusion Matrix[1]

Confusion Matrix			
		Predicted Class Intrusion	
		Yes	No
Actual Class Intrusion	Yes	True Positive	False Negative
	No	False Positive	True Negative

Table 7. Definisions[1]

Definitions
TP and TN: True Positive and True Negative are correct classifications.
FP: False Positive occurs when the result is envisaged as positive when it is actually negative.
FN: False Negative occurs when the result is envisaged as negative when it is actually positive.

The equation of accuracy is described as follows:
Accuracy=(TN+TP)/(TN+TP+FN+FP)[1] (7)

4. Experiment and Analysis

In this research, PRCL and LVQ will be trained using 10% KDD Cup 1999 dataset. We use 100000 data points with composition: normal=25000 and intrusion= 75000 (DoS=69715, Probe=4107, R2L=1126, U2R=52). The number of cluster=5 (0=Normal, 1=DoS, 2=Probe, 3=R2L, 4=U2R). Testing in this research using learning rate (alpha) = 0.1, 0.05, 0.01, 0.005, 0.001, 0.0005, and 0.0001.

Table 8. Accuracy of PRCL

Learning Rate	DoS (%)	Probe (%)	R2L (%)	U2R (%)
0.1	99.970	99.852	99.684	99.844
0.05	99.987	99.931	99.838	99.928
0.01	99.988	99.935	99.842	99.920
0.005	99.988	99.931	99.842	99.920
0.001	99.989	99.931	99.846	99.924
0.0005	99.989	99.931	99.846	99.924
0.0001	99.996	99.939	99.865	99.948

Table 9. Accuracy of LVQ

Learning Rate	DoS (%)	Probe (%)	R2L (%)	U2R (%)
0.1	99.960	99.858	99.692	99.852
0.05	99.936	99.811	99.634	99.796
0.01	99.957	99.851	99.688	99.852
0.005	99.970	99.852	99.685	99.852
0.001	99.990	99.920	99.845	99.928
0.0005	99.995	99.935	99.861	99.944
0.0001	99.996	99.939	99.865	99.948

Table 8 illustrates the accuracy of the proposed technique (PRCL). While, table 9 illustrates the accuracy of LVQ technique.

Figure 4 illustrate the Accuracy of DOS (PRCL Vs LVQ)

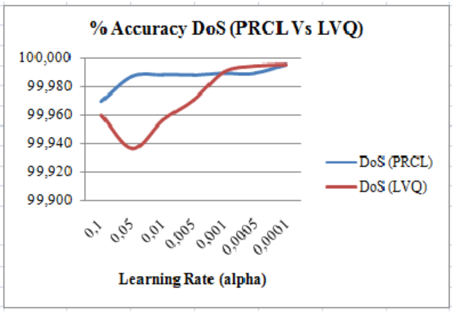

Figure 4. Accuracy of DOS (PRCL Vs LVQ)

Figure 5 illustrate the Accuracy of Probe (PRCL Vs LVQ)

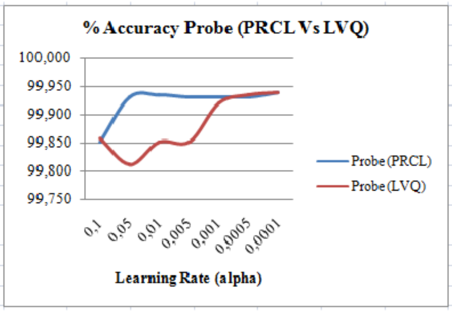

Figure 5. Accuracy of Probe (PRCL Vs LVQ)

Figure 6 illustrate the Accuracy of R2L (PRCL Vs LVQ)

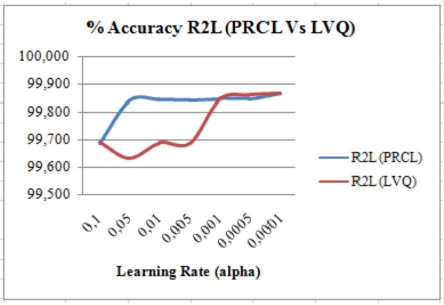

Figure 6. Accuracy of R2L (PRCL Vs LVQ)

Figure 7 illustrate the Accuracy of U2R (PRCL Vs LVQ).

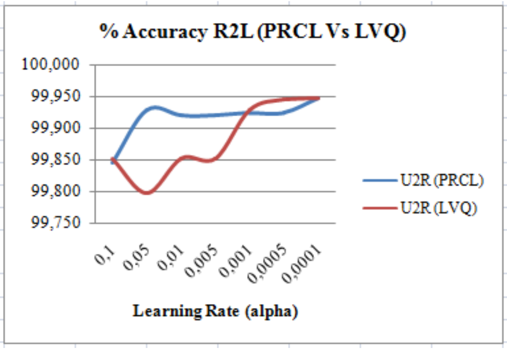

Figure 7. Accuracy of U2R (PRCL Vs LVQ)

The experimental results explain that smaller learning rate (alpha), the accuracy will be better. The proposed technique (PRCL) achieve high accuracy when learning rate=0.0001 (99.996% for DoS, 99.939% for Probe, 99.865% for R2L and 99.948% for U2R). As well as LVQ achieve high accuracy when learning rate=0.0001 (99.996% for DoS, 99.939% for Probe, 99.865% for R2L and 99.948% for U2R). The accuracy of the proposed technique (PRCL) same with LVQ technique, but the proposed technique (PRCL) more stable when learning rate=0.001, 0.0005, 0.0001.

Table 10 and figure 8 illustrate the time required by PRCL and LVQ technique for on-line clustering.

Table 10. Time (PRCL Vs LVQ)

Learning Rate	Time of PRCL (ms)	Time of LVQ (ms)
0.1	86	54
0.05	83	58
0.01	80	59
0.005	77	59
0.001	77	55
0.0005	72	53
0.0001	65	49

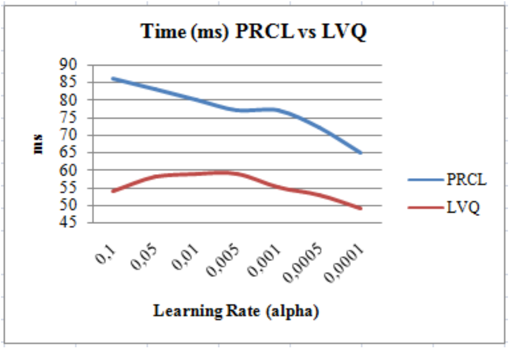

Figure 8. Time (PRCL Vs LVQ)

The experimental results explain that smaller learning rate (alpha), the time required by PRCL and LVQ for on-line clustering will be faster.

So, we can conclude that smaller learning rate (alpha), the accuracy will be better and the time required for on-line clustering will be faster.

5. Conclusion

This paper presents new approach to detect intrusion using On-Line Clustering. The On-Line Clustering method which used in this research is Pursuit Reinforcement competitive Learning (PRCL). The experimental results explain that smaller learning rate (alpha), the accuracy will be better and the time required for on-line clustering will be faster. And based on experiment results, LVQ achieve high accuracy when learning rate=0.0001 (99.996% for DoS, 99.939% for Probe, 99.865% for R2L and 99.948% for U2R) and high speed (49 ms). The proposed technique (PRCL) achieve high accuracy (99.996% for DoS, 99.939% for Probe, 99.865% for R2L and 99.948% for U2R) and high speed (65ms) when learning rate=0.0001. So, the proposed technique (PRCL) can detect intrusions with high accuracy and high speed.

Our future works is to improve the accuracy and speed in detecting intrusions.

References

[1] A. M. Chandrashekhar, K. raghuveer, Fortification of Hybrid Intrusion Detection System Using Variants of Neural Networks and Support Vector Machines, International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.1, January, 71-90, 2013.

[2] A. S. Aneetha and Dr. S. Bose, The Combined Approach for Anomaly Detection using Neural Networks and Clustering Techniques, Computer Science & Engineering An International (CSEIJ), Vol.2, No.4, August, 37-46, 2012 [2]

[3] Prof. Dr. Kais Said Al-Sabbagh, Assist. Prof. Hamid M. Ali, Elaf Sabah Abbas, Development an Anomaly Network Intrusion Detection System Using Neural Network, Journal of Engineering, Vol. 18, No. 12, December, 1325-1334, 2012.

[4] Reyadh Shaker Naoum, Zainab Namh Al-Sultani, Hibrid System of Learning Vector Quantization and Enhanced Resilient Backpropagation Artificial Neural Network for Intrusion Classification, International Journal of Research and Reviews in Applied Sciences (IJRRAS), Vol. 14, No. 2, February 2013.

[5] Amir Azimi Alasti, Kaveh Feyzi, Zahra Atashbar Orang, Hadi Bahrbegi, Elnaz Safarzadeh, Using Learning Vector Quantization in Alert Management of Intrusion Detection System, International Journal of Computer Science and Security, (IJCSS), Vol. 6, Issue. 2, 2012.

[6] Reyadh Shaker Naoum, Zainab Namh Al-Sultani, Learning Vector Quantization (LVQ) and k-Nearest Neighbor for Intrusion Classification, World of Computer Science and Information Technology Journal (WCSIT), Vol. 2, No. 3, 105-109, 2012.

[7] Ali ridho Barakbah, Kohei Arai, Pursuit Reinforcement Competitive Learning, Informatiion and Communication Technology Seminar (ICTS), 2006.

[8] http://www.cert.org/stats/ [accessed on July 28th, 2013]

[9]www.cert.org/archive/pdf/CERTCC_**Vulnerability_Discovery**.pdf [accessed on July 28th, 2013]

[10] Manoj Sharma, Keshav Jindal, Ashish Kumar, Intrusion Detection System using Bayesian Approach for Wireless Network, International Journal of Computer Applications (0975 – 888), Volume 48– No.5, June 2012

Appendix

Table A. Protocol Type Column Transformation

Protocol Type (column 2)	Value
Icmp	1
Tcp	2
Udp	3

Table B. Service Column Transformation

Service (column 3)	Value
ecr_i	1
Private	2
http	3
Smtp	4
Other	5
domain_u	6
ftp_data	7
eco_i	8
ftp	9
Finger	10
urp_i	11
telnet	12
ntp_u	13
Auth	14
pop_3	15
Time	16
csnet_ns	17
remote_job	18
Gopher	19
imap4	20
Discard	21
Domain	22
Systat	23
iso_tsap	24
Echo	25
Shell	26
Rje	27
sql_net	28
Whois	29
Printer	30
Courier	31
nntp	32
netbios_ssn	33
Sunrpc	34
Mtp	35
Bgp	36
uucp_path	37
Uucp	38
Klogin	39
Vmnet	40
Ssh	41
Nnsp	42
Supdup	43
Login	44
Hostnames	45
Daytime	46
Efs	47
Link	48
netbios_ns	49
pop_2	50
Ldap	51
netbios_dgm	52
Exec	53
http_443	54
Name	55
Kshell	56
Ctf	57
Netstat	58
Z39_50	59
IRC	60
urh_i	61
X11	62
tim_i	63
tftp_u	64
pm_dump	65
red_i	66

Table C. Flag Column Transformation

Flag (column 4)	Value
SF	1
S0	2
REJ	3
RSTR	4
RSTO	5
SH	6

Flag (column 4)	Value
S1	7
S2	8
RSTOS0	9
S3	10
OTH	11

Table D. Attack Label Transformation

Sub Attack Label (column 42)	Label	Value
normal.	normal	0
smurf.	dos	1
neptune.	dos	1
back.	dos	1
teardrop.	dos	1
pod.	dos	1
land.	dos	1
satan.	probe	2
ipsweep.	probe	2
portsweep.	probe	2
nmap.	probe	2
warezclient.	r2l	3
guess_passwd.	r2l	3
warezmaster.	r2l	3
imap.	r2l	3
ftp_write.	r2l	3
multihop.	r2l	3
phf.	r2l	3
spy.	r2l	3
buffer_overflow.	u2r	4
rootkit.	u2r	4
loadmodule.	u2r	4
perl.	u2r	4