EMITTER International Journal of Engineering Technology
Vol.2, No.1, June 2014
ISSN: 2443-1168

Reinforced Intrusion Detection Using Pursuit Reinforcement Competitive 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 Campus, Jalan Raya ITS, Sukolilo 60111, Indonesia
Email: indahyuliap@yahoo.com, {ridho, amang, trison}@eepis-its.edu

Abstract

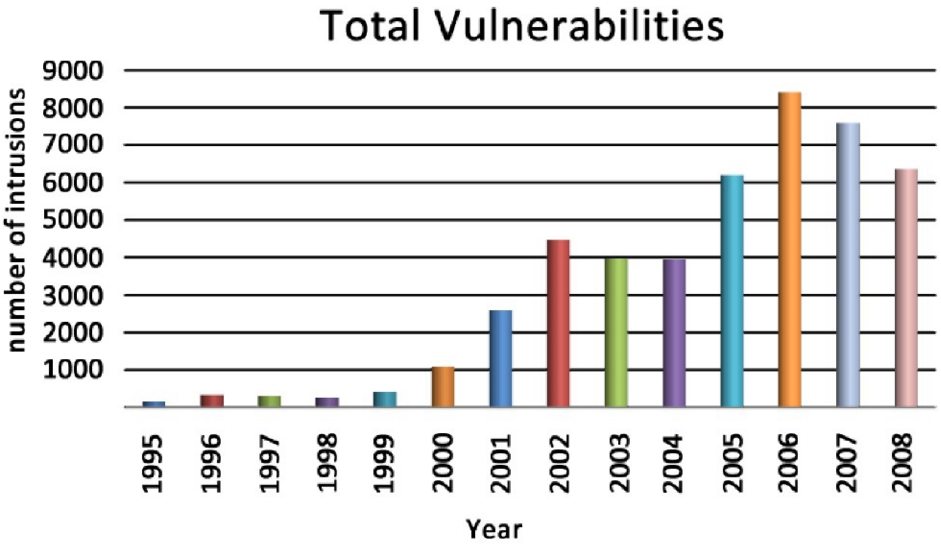
Today, information technology is growing rapidly,all information can be obtainedmuch easier. It raises some new problems; one of them is unauthorized access to the system. We need a reliable network security system that is resistant to a variety of attacks against the system. Therefore, Intrusion Detection System (IDS) required to overcome the problems of intrusions. Many researches have been done on intrusion detection using classification methods. Classification methodshave high precision, but it takes efforts to determine an appropriate classification model to the classification problem. In this paper, we propose a new reinforced approach to detect intrusion with On-line Clustering using Reinforcement Learning. Reinforcement Learning is a new paradigm in machine learning which involves interaction with the environment.It works with reward and punishment mechanism to achieve solution. We apply the Reinforcement Learning to the intrusion detection problem with considering competitive learning using Pursuit Reinforcement Competitive Learning (PRCL). Based on the experimental result, PRCL can detect intrusions in real time with high accuracy (99.816% for DoS, 95.015% for Probe, 94.731% for R2L and 99.373% for U2R) and high speed (44 ms).The proposed approach can help network administrators to detect intrusion, so the computer network security systembecome reliable.

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

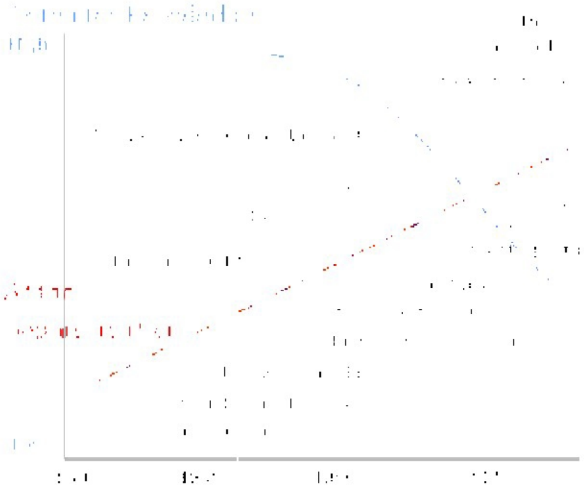
1. INTRODUCTION

Based on data compiled by CERT [11], the number of intrusions from year to year is increase. From 1995 to 2008, the total attack was summarized by CERT is 46.156, as illustrated in Figure 1.a.

Meanwhile, according to data analyzed by Carnegie Mellon University (2002) and Idaho National Laboratory (2005), intruder technical knowledge decreases, as illustrated in Figure 1.b.



a. The number of intrusions summarized by CERT[11]



b. Decreasing intruder technical knowledge[12]

Figure 1. The number of intrusions and intruder technical knowledge

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 [7]. Intrusion detection system consists of three categories, there are host-based, network-based and vulnerability assessment-based. Host-based where information is found on a single or multiple host systems. Network-based that examines the information captured from network communications. Vulnerability assessment-based identify vulnerabilities in internal networks and firewall. The functionality intrusion detection classified into two as anomaly detection and misuse detection.

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 [7]:

- 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.

2. RELATED 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 [7], “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. 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 [5], “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. The accuracy rate reaches 98.5% for DOS attack.

Prof. Dr. Kais Said Al-Sabbagh [6], “Development an Anomaly Network Intrusion Detection System Using Neural Network” (December, 2012) proposed Self Organizing Map (SOM) to improve payload anomaly detector (PAYL). 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.

Shaker Reyadh Namh Naoum and Zainab Al-Sultani [8], “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. 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[2], “Using Learning Vector Quantization in Alert Management of Intrusion Detection System” (2012) proposed a new alert management system by using Learning Vector Quantization (LVQ).

Reyadh Shaker Naoum and Zainab Namh Al-Sultani[3], “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. 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%.

Kyaw Thet Khaing [1], “Enhanced Features Ranking and Selection using Recursive Feature Elimination(RFE) and k-Nearest Neighbor Algorithms in Support Vector Machine for Intrusion Detection System” (June, 2010) proposed hybrid intrusion detection system which combining enhanced SVM, Recursive Feature Elimination (RFE) and k-Nearest Neighbor (KNN) to detect intrusion. The improvement precision is only 0.4% on average, but the improvement for false negative rate is between 16.2% and 28.8%. The experimental results are precision = 99.91%, false negative = 5.49%, time execution = 77.85 second.

Nitin Mohan Sharma, Tapan P. Gondaliya [9], “Enhance IDS False Alarm Filtering Using KNN Classifier” (May, 2013) proposed k-Nearest Neighbor

(KNN) classifier to reduce the number of false alarms. KNN classifier successfully reduces up to 93% of false alarms generated by famous IDS.

3. ORIGINALITY

Intrusion Detection System (IDS) is a software or hardware used to detect unauthorized access of acomputer system or network[4]. Many research have done using classification method. Classification methods have high precision, but need appropriate classification model and need long time to classify intrusions.

In this paper we propose a new reinforced approach for detecting intrusions using On-Line Clustering which can perform clustering in real-time with high accuracy in detecting intrusions. We usePursuit Reinforcement Competitive Learning (PRCL) [10] to perform On-Line Clustering.

PRCL proposed by Ali Ridho Barakbah & Kohei Arai [10], is expected to detect new attacks in realtime with higher speed and higher accuracy than previous research and can help network administrators to detect intrusion, so the computer network security system become reliable.

4. SYSTEM DESIGN

The proposed system consists of 3 phases: (1) Data pre-processing phase, (2) PRCL algorithm and (3) Performance evaluation phase.

Here is a Block Diagram System shown in Figure 2.

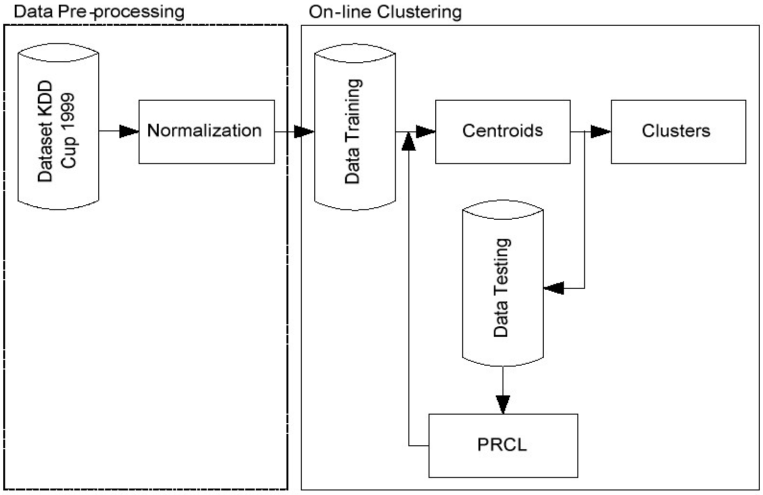


Figure 2. Block diagram of system

4.1. Data Pre-processing Phase

The proposed system will be trained using 10% KDD Cup 1999 dataset. The total dataset of 10% KDD Cup is 494.021 with composition (DOS=391.458, Normal=97.278, Probe=4.107, R2L=1.126, U2R=52). 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 [7].

4.2. PRCL Algorithm

In this phase, we use Pursuit Reinforcement Competitive Learning (PRCL) to detect intrusions. The algorithm of PRCL is described as follows [4]:

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

$$d_{i^*}=\text{argmin}_i\, d(x, w_i) \quad (1)$$

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

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

$$w_{i^*}=\text{arg max}_i\, r(x, w_i) \quad (3)$$

d. Update the weight vectors as follows:

$$\triangle w_{ij}= a\,(x_j- w_{ij})\text{if} i =i^*$$

and $\triangle w_{ij}=0$ if$i \neq i^*$ (4)

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

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 1.a explains the confusion matrix. Table 1.b explains the definition of TP, TN, FP, FN.

Table 1. Confusion matrix and definition [1]

a.Confusion matrix

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

b. Definition

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 performance of a binary classification test is statistically measured by precision and recall. The proportion of actual positives which are correctly recognized is calculated by recall. The overall accuracy is calculated by using precision, recall and F-measure which are generally used to estimate the rare class prediction. It is advantageous to achieve a high recall devoid of loss of precision. Harmonic mean of precision and recall is called as F-measure. The equation used for Recall, Precision, F-measure and overall Accuracy is described as follows [7]:

$$Accuracy=(TN+TP)/(TN+TP+FN+FP) \qquad (5)$$

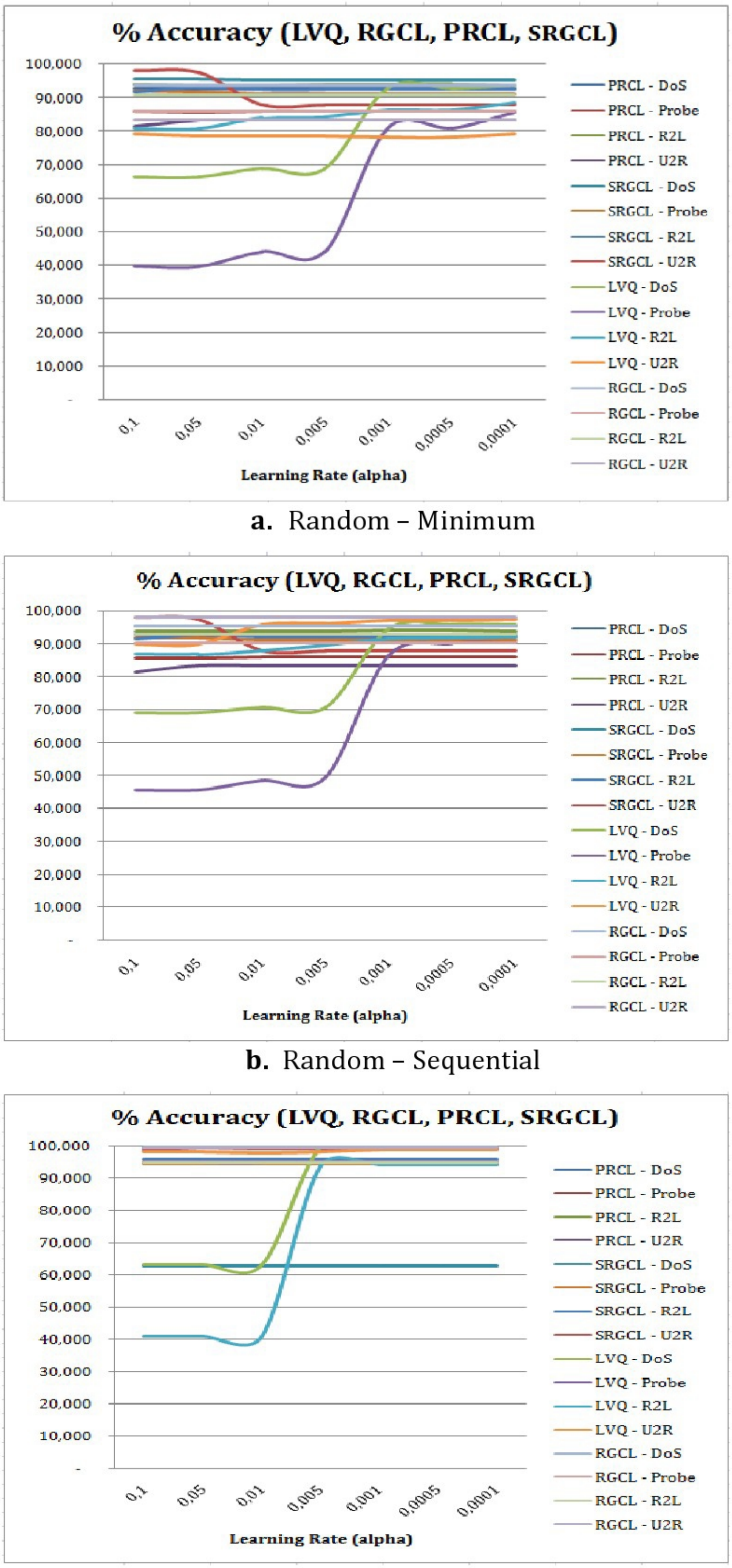
5. EXPERIMENT AND ANALYSIS

In this paper we compare PRCL with Learning Vector Quantization (LVQ), Reinforcement Guided Competitive Learning (RGCL), and Sustained Reinforcement Guided Competitive Learning (SRGCL). Vector quantization is one example of competitive learning [4]. Vector quantization is a method used to have the network "discover" structure in the data by finding how the data is clustered.Reinforcement Guided Competitive Learning (RGCL), proposed by A. Likas, is a new method to solve on-line clustering problem using Reinforcement Learning [10].

Sustained RGCL is the modification of RGCL that employs the above weight update scheme. It will be called the SRGCL algorithm (Sustained RGCL) [10]. PRCL, LVQ, RGCL, SRGCL, and SVM 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).

PRCL, LVQ, RGCL, SRGCL, and SVMwill be tested using learning rate (alpha) = 0.1, 0.05, 0.01, 0.005, 0.001, 0.0005, and 0.0001.The following are the results of an experiment of PRCL, LVQ, RGCL, and SRGCL using learning rate (alpha) = 0.1, 0.05, 0.01, 0.005, 0.001, 0.0005, 0.0001 and data composition = Random-Minimum, Sequential, Random-Maximum. The accuracy of intrusions detection between LVQ, RGCL, PRCL, and SRGCL with data composition (Random–Minimum, Sequential, Random–Maximum) illustrated in Figure 3.

The experimentalresults of random - minimum explain that almost all algorithms stable when alpha = 0.0001 (Figure 3.a). The experimentalresults of random - sequential explain that almost all algorithms stable when alpha = 0.0001, 0.0005 (Figure 3.b). The experimental results of random – maximum explain that almost all algorithms stable when alpha = 0.0001, 0.0005, 0.001 (Figure 3.c). The experimental results of random – minimum, random – sequential, random - maximum explain that the smaller learning rate (alpha), the accuracy will be better.



a. Random – Minimum

b. Random – Sequential

c. Random – Maximum

Figure 3. Accuracy of intrusions detection betweenLVQ, RGCL, PRCL, and SRGCL

The accuracy of intrusions detection using PRCL is higher than SRGCL but SRGCL more stable than PRCL. PRCL stable when beta=0.0001 and learning rate=0.0005, 0.0001, while SRGCL stable when beta=0.0001 and learning rate=0.001, 0.0005, 0.0001. The accuracy of intrusions detection using PRCL almost same with LVQ, but PRCL more stable than LVQ when learning rate=0.0005, 0.0001.The accuracy of intrusions detection using PRCL is almost same with RGCL but RGCL more stable than PRCL. PRCL stable whenlearning rate (alpha)=0.0005, 0.0001, while RGCL stable when learning rate (alpha)=0.01, 0.005, 0.001, 0.0005, 0.0001.

The following are the results of a comparison between LVQ, RGCL, SRGCL, PRCL, SVM with data composition = Random-Maximum illustrated in Table 2.

Table 2. Comparison accuracy and processing time measurement (ms) of intrusions detection between LVQ, RGCL, SRGCL, PRCL, and SVM

Technique	**DoS (%)**	**Probe (%)**	**R2L (%)**	**U2R (%)**	**Time (ms)**
LVQ (On-Line Clustering)	99.843	95.038	94.174	98.847	39
RGCL (On-Line Clustering)	99.844	95.042	94.659	99.373	60
SRGCL (On-Line Clustering)	62.946	94.424	95.974	99.263	83
PRCL (On-Line Clustering)	99.816	95.015	94.731	99.373	44
SVM (Classification)	99.996	99.804	99.690	99.836	5050

The experimental results shown in Table 2 explain that smaller learning rate (alpha), the accuracy of LVQ, RGCL, SRGCL, PRCL will be better.PRCL achieves high accuracy (99.816% for DOS, 95.015% for Probe, 94.731% for R2L and 99.373% for U2R)when learning rate (alpha) = 0.0001, beta=0.001, 0.0005, 0.0001 and data composition=Random-Maximum.SRGCL achieves high accuracy(62.946% for DOS, 94.424% for Probe, 95.974% for R2L and 99.263% for U2R)when learning rate (alpha)=0.0001, beta=0.0001 and data composition=Random-Maximum.LVQachieves high accuracy (99.843% for DOS, 95.038% for Probe, 94.174% for R2L and 98.847% for U2R)when learning rate (alpha)=0.0001 and data composition=Random-Maximum.RGCL achieves high accuracy(99.844% for DOS, 95.042% for Probe, 94.659% for R2L and 99.373% for U2R)when learning rate (alpha)=0.0001 and data composition=Random-Maximum. SVM achieves high accuracy (99.996% for DOS, 99.804% for Probe, 99.690% for R2L, and 99.836% for U2R).

The result of a comparison explains that :

- ✓ The accuracy of intrusions detection using PRCLalmost same with LVQ but PRCL more stable than LVQ, besideLVQfaster than PRCL.

- ✓ The accuracy of intrusions detection using PRCL almost same with RGCL but PRCL faster than RGCL.
- ✓ The accuracy of intrusions detection using PRCLhigher and faster than SRGCL.
- ✓ Theaccuracy of intrusions detection using PRCL lower than SVM butPRCL faster than SVM.

6. CONCLUSION

This paper presents a new reinforced approach to detect intrusion using On-Line Clustering which can perform clustering in real-time with high accuracy in detecting intrusions. We use Pursuit Reinforcement Competitive Learning (PRCL) to perform On-Line Clustering.

This proposed approach was examined with KDD Cup dataset. From experimental study, the proposed approach achieves high accuracy (99.816% for DOS, 95.015% for Probe, 94.731% for R2L and 99.373% for U2R) and high speed (44ms) when learning rate (alpha) = 0.0001, beta=0.001, 0.0005, 0.0001.SRGCL achieves high accuracy(62.946% for DOS, 94.424% for Probe, 95.974% for R2L and 99.263% for U2R) and high speed (83 ms)when learning rate (alpha)=0.0001, beta=0.0001. LVQachieves high accuracy (99.843% for DOS, 95.038% for Probe, 94.174% for R2L and 98.847% for U2R) and high speed (39 ms) when learning rate (alpha)=0.0001.RGCL achieves high accuracy(99.844% for DOS, 95.042% for Probe, 94.659% for R2L and 99.373% for U2R) and high speed (60 ms)when learning rate (alpha)=0.0001. SVM achieves high accuracy (99.996% for DOS, 99.804% for Probe, 99.690% for R2L, and 99.836% for U2R) and low speed (5050 ms). Data composition of all algorithms=Random–Maximum.

The accuracy of intrusions detection using PRCL is higher than SRGCL but SRGCL is more stable than PRCL. The accuracyof intrusions detection of LVQ almost is same with RGCL but RGCL more stable than LVQ.The accuracy of intrusions detection PRCL is almost same with LVQ but PRCL more stable than LVQ.In this paper, we also compare PRCL (On-Line Clustering) with SVM (Classification). The experimental results explain that the accuracy of intrusions detection using PRCLlower than SVM butPRCL faster than SVM.In this paper our proposed reinforced approach to detect intrusion with PRCL shows high performance in speed and accuracy comparing to the other algorithm.

REFERENCES

[1] Kyaw Thet Khaing, **Enhanced Features Ranking and Selection using Recursive Feature Elimination(RFE) and k-Nearest Neighbor Algorithms in Support Vector Machine for Intrusion Detection System**, *International Journal of Network and Mobile Technologies,* Vol. 1, Issue 1, pp. 1832-6758, June 2010.

[2] 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.

[3] 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, pp. 105-109, 2012.

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

[5] 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, pp. 37-46, August, 2012.

[6] 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, pp. 1325-1334, December, 2012.

[7] 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, pp. 71-90, January, 2013.

[8] 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.

[9] Nitin Mohan Sharma, Tapan P. Gondaliya, **Enhance IDS False Alarm Filtering Using KNN Classifier**, International Journal of Emerging Research in Management & Technology, Vol. 2, Issue 5, pp. 2278-9359, May 2013.

[10] Ali Ridho Barakbah, Kohei Arai, **Pursuit Reinforcement Competitive Learning,***Information and Communication Technology Seminar (ICTS)*, 2006.

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

[12] www.cert.org/archive/pdf/CERTCC_**Vulnerability_Discovery**.pdf [accessed on July28th, 2013].