Research Journal of Information Technology

ISSN 1815-7432

Academic Journals Inc.

www.academicjournals.com

Research Journal of Information Technology 6 (1): 46-57, 2014
ISSN 1815-7432 / DOI: 10.3923/rjit.2014.46.57

KM-NEU: An Efficient Hybrid Approach for Intrusion Detection System

[1]Mazyar Mohammadi Lisehroodi, [1]Zaiton Muda, [2]Warusia Yassin and [1]Nur Izura Udzir
[1]Faculty of Computer Science and Information Technology, University Putra Malaysia, UPM Serdang, 43400, Selangor, Darul Ehsan, Malaysia
[2]Faculty of Information and Communication Technology, University Technical Malaysia Melaka, Durian Tunggal, 76100, Melaka, Malaysia

Corresponding Author: Zaiton Muda, Faculty of Computer Science and Information Technology, University Putra Malaysia, 43400, UPM Serdang, Selangor Darul Ehsan, Malaysia Tel: +60-3-8947-1706 Fax: +60- 3-8946-6577

ABSTRACT

Due to the widespread use of Internet and communication networks, a reliable and secure network plays a crucial role for Information Technology (IT) service providers and users. The hardness of network attacks as well as their complexities has also increased lately. The anomaly-based Intrusion Detection Systems (IDS) are able to detect unknown attacks. Major task of this research is to increase detection rate and accuracy while keeping the false alarm at low rate. To overwhelm this challenge a new hybrid learning approach, KM-NEU is proposed by combination of K-means clustering and Neural Network Multi-Layer Perceptron (MLP) classification. The K-means clustering algorithm is engaged for grouping analogous nodes into k clusters using the similarity measures such as attack and non-attack, whereas the Neural Network Multi-Layer Perceptron classifies the clustered data into detail categories such as R2L, Probing, DoS, U2R and Normal. Performance of this hybrid approach is evaluated with standard knowledge discovery in databases (KDD Cup '99) dataset. The experimental results confirm that this approach has considerably increased in the detection rate and accuracy and reduce in false alarm rate compared to single neural network classifier.

Key words: Intrusion detection system, KM-NEU, K-means clustering, neural network classifier, multi-layer perceptron

INTRODUCTION

As the growing number of people who use computer network resources, this technology entered users' everyday lives. Due to the fact that the openness of network has posed some network security vulnerabilities with vast number of novel invasive technologies, the network security plays a vital role in terms of information accuracy and reliability.

As a result of having bugs and other drawbacks of software applications, firewalls and policies have been unable to prevent network intrusions. In addition, the number of new attacks broadcasting over the Internet is increasing daily. On the other hand, misbehavior of some employees can put the system in danger of intrusions from inside. A robust IDS which is able to detect and react to illegal access and anomalous activities, is likely to block such attacks (Chen *et al*., 2005).

Intrusion detection has emerged to gather and analyze a number of key points in computer systems and networks, to find if there are abnormal behaviors against the policy of system or violent sign in the network. The combination of software and hardware for detection intrusion is IDS (Zhao *et al.*, 2011).

Intrusion detection technologies aim to identify two major groups of attacks: Misuse detection and anomaly selection. Anomaly detection recognizes any variation from the defined patterns for users. Anomaly detection usually based on creation of monitored activity profiles. Misuse detection comprises the comparison of user's activities and the known behaviors of assailants to infiltrate a network (Cannady, 1998). Misuse detection method using a rule-based approach to detect known attacks by matching attack pattern to list of signatures, greatly similar to antivirus applications. The signatures should be updated regularly, because if the signature is not included in its library this type of IDS is unable to detect the unknown attacks. Contrasting misuse detection, anomaly based detection is involved monitoring user's activities to catch any deviation from normal behavior profile. Despite being able to detect unknown attacks, the probability of high false alarm is considerable (Muda *et al.*, 2011).

Many of recent researches of IDS have been proposed anomaly detection to detect novel attack (Patcha and Park, 2007; Hashemi *et al.*, 2013). Many of these approaches resulted in high detection rate and accuracy, however majority of them encounter high false alarm rates. As the result of falsely classification of normal connections as attack, authentic users cannot access to the network. Therefore, IDS research area is in desperate need of focusing on false alarm to properly identify such intrusions. In this study, a hybrid approach has been proposed using the combination of K-means clustering algorithm and Neural Network MLP classifier to improve anomaly based prior works in terms of detection rate, accuracy and reduce the false alarm rate. For evaluation of this work the KDD cup '99 benchmark data set has been used and the experimental results compared with single neural network classifier and previous findings.

LITERATURE REVIEW

IDS has become a significant area of research regarding safe and secured IT communication. Many of previous researches proposed unsupervised anomaly detection approaches with various classification algorithm (Aneetha and Bose, 2012). Most researches employed KDD cup '99 data set for evaluation of their proposed approaches. The hybrid learning approaches has been resulted in well detection rate and accuracy (Muda *et al.*, 2011). Although, detecting all kinds of attack, decreasing the false alarm rate is still a big issue.

It has been proved that clustering technique is suitable for huge datasets since its low computational requirements. Due to the fact that the time complexity of clustering algorithm is linear, it has been used commonly. The most well-known clustering algorithm is K-means clustering concerning its simplicity and being straightforward (Hartigan, 1975). K-means clustering is able to detect new types of attacks and group data based on their natural behaviors (Tsang *et al.*, 2007). The major weakness of K-means is that the result is highly dependent to initial cluster centroid which can lead to converge local optima (Selim and Ismail, 1984).

Related work based on hybrid learning approaches have been broadly discovered such as in Kavitha *et al.* (2012) and Li *et al.* (2012). In majority of these approaches, False Alarm (FA), True Positive (TP), False Positive (FP), False Negative (FN), Detection Rate (DR) and accuracy rate have been issued. Some approaches showed high number of detection but unable to improve false alarm rate. To boost the accuracy, a Fuzzy SVMs (FSVM) was proposed aiming to build a new training

set using centroids (Teng *et al*., 2010). FSVM is used for training the new set to gain a support vector. The experimental result shows a reasonable increase in the accuracy but still rooms to improve it.

Rough set (LEM2) algorithm and K-nearest neighbor (KNN) are used for intrusion detection. Although it has been unable to detect U2R and R2L attack in a high range but the feathers values in training dataset were completely different from the testing data set for these two attack types (Adetunmbi *et al*., 2008).

A multiple level classifier is suggested that employed the combination of unsupervised Bayesian clustering and supervised tree (Xiang *et al*., 2008). However this approach was able to detect high range of DoS, Probe and Normal types. It could detect only 71.43 and 46.97% of U2R and R2L, respectively and moderate amount of false alarm by 3.2%.

Due to the vast number of vulnerabilities of mobile and ad hoc networks in term of security, utilizing neural network as anomaly based intrusion detection system can be effective to touch near zero false positive and false alarm rates (Jabbehdari *et al*., 2012). It should be noted that despite acceptable improvement in false alarm rate, their approach has only covered DoS attack.

The combination of various neural network and clustering method has been proposed to improve anomaly detection for instance Self-organizing map (SOM) is modified to eliminate the drawbacks of the traditional SOM. In this method the network is allowed to be developed with the connection strength to recognize neighbor nodes. The results of modified SOM are grouped by K-means by natural behavior and centroids (Bose *et al*., 2012; Lee *et al*., 2011). Modification of SOM engaged with K-means clustering can enhance anomaly detection rate in a considerable range. However, 2% false alarm still is a big issue (Aneetha and Bose, 2012).

Many of previous works employed Artificial Neural Networks (ANN) to resolve difficult real-world problems. For instance, formal concept ANN (FC-ANN) approach used fuzzy clustering method alongside neural network to enrich anomaly detection rate (Wang *et al*., 2010). Training dataset is generated by various models of ANN and fuzzy clustering is used to collect the results. Though this model has been successful to detect R2L and U2R attack, it has been unable to show a reasonable rate in Probe detection.

SOM algorithm can be modified to overcome fixed architecture. To achieve this goal new neighborhood updating rules is included and the learning phase is done dynamically. As the primary step, algorithm starts with empty network and develops with the original data space. Distance threshold measure is used to create new nodes and their neighborhoods will be found using connection strength. The results claim 98% detection rate and 2% false alarm rate.

A new hybrid model applied C-means clustering, fuzzy neural network and radial basis function (RBF). This study defined four steps. First step for analysis, next C-means is used for data clustering. Then hybrid neural network and fuzzy (neuro-fuzzy) classifier related with the clusters to train each of the nodes. Finally, RBF-SVM classifies data to detect intrusions. Comparisons showing that the efficiency of this technique in the detection rate and F-measure but high percentage of the false alarm is a limitation (Chandrashekhar and Raghuveer, 2013). In this study, a hybrid approach is proposed to detect all types of attack (R2L, U2R, Probe, DoS) using the combination of K-means clustering and neural network MLP classifier. After training with KDD cup '99 training data set, 17 new types of attacks will come by testing data set. This system can detect such anomalies by distinguishing them from normal behaviors. The false positive and false alarm rate are near to zero while high rate of detecting new attacks.

MATERIALS AND METHODS

Hybrid learning approach: Accuracy and detection rate are mostly increasing but false alarm still is a big concern in IDS research area. Therefore, it has been decided in this study to combine K-means clustering algorithm with artificial neural network to decrease false alarm and increase accuracy and detection rates at the same time. This combination method called KM-NEU. The KM-NEU approach involves two modules. First, data being clustered based on their natural behavior using K-means as clustering component. Then clustered data are classified by neural network MLP algorithm.

K-means clustering module: K-means clustering is using to group data into attack and normal instances. A cluster is a collection of records that are similar to one another and dissimilar to records in other clusters. The similarity of the records within the cluster is maximized and the similarity to records outside this cluster is minimized. Standard classification of network intrusion fall into four major categories: DoS, Probe, U2R and R2L (Lippmann *et al*., 2000). K-means clustering partition raw dataset into k-cluster based on the initial value which called seed-points into each cluster's centers. Centroids are specified by the mean value of numerical data contain in each single cluster. K-means clustering module can be summarized as following pseudo code:

Initialize m_i, i = 1,..., k, for example, to k random x^t.

Repeat

For all $x^t \| X$:

$$b_i^t = \begin{cases} 1 \text{ if } \|x^t - m_i\| = \min_j \|x^t - m_j\| \\ 0 \text{ otherwise} \end{cases}$$

For all m_i, i = 1,..., k, for example, to k random x^t:

$$m_i \sum_t b^t x^t / \sum_t b^t$$

Until m_i converge.

Neural network classifier module: As the related works indicated, there are several researchers used the various clustering techniques like C-means, fuzzy clustering and K-means. Most of them were unable to differentiate between attack records and normal records appropriately. In this study regarding the advantages of neural networks which is able to characterize both nonlinear and linear functions and their ability to learn these relationships straight from the data being modeled, a combination of K-means clustering with neural network classifier has been employed.

Neural network divided into two architectures: Support Vector Machine (SVM), Multi-Layer Perceptron (MLP). In this study MLP is used as the classifier algorithm. In such neural network every neuron's input of the next layer is joined to neuron's output of the previous layer. MLP architecture consists of at least one hidden layer. Due to signal transition establishment through the network from input to output, this architecture is called feed forward.

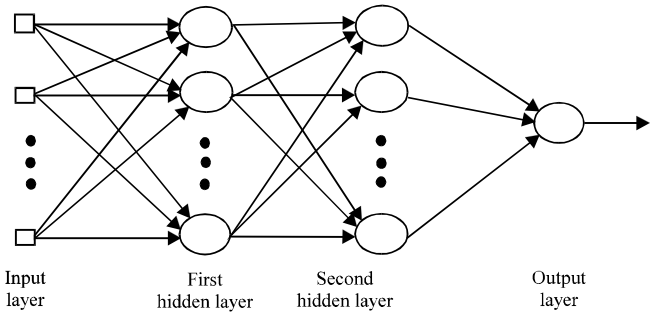

Fig. 1: Design of MLP with two hidden layers

MLP is known as feed forward neural network was initially provided for the non-linear XOR and was then effectively used to different combinatorial problems. MLP is mostly used for information managing and pattern recognition in prediction of seismic activities. It is incredibly used and analyzed with different problems such as in time series prediction and function approximation (Shah *et al*., 2012). Thus MLP can be used as a nonlinear model for regression as well as for classification. As the arriving information in the network could be failed randomly, these characteristics are vital in intrusion detection system. Moreover, as multiple attackers may target the system with a synchronized assault, being able to process data from different sources in a non-linear manner is crucial. Figure 1 shows the design of MLP with two hidden layers, one output layer and one input layer:

$$y_i = f_i\left(\sum_{i=1}^{n} w_{ij}x_i + b_i\right) \quad (1)$$

Equation 1 calculates y_i which is the output of the node, x_i stand for the ith input for the node while w_{ij} represents the connection weight between input and output node, b_i is threshold of the node and the node transfer function showed by f_i. The network error function summarized in Eq. 2:

$$E(w(t)) = \frac{1}{n}\sum_{j=1}^{n}\sum_{k=1}^{k}(Dk - Ot) \quad (2)$$

where, E(w(t)) is the error function of t th iteration and w(t) is the weight of connection in tth iteration. D_k is the wanted output node and O_t is the real value of tth output node's is the number of output node and n is the number of pattern and k is optimization goal to minimize the objective function by optimizing the weight of network w(t).

Comparing with single neural network classifier the proposed KM-NEU hybrid approach shows improvement in terms of accuracy, detection rate and low false alarm rate.

EXPERIMENTAL DESIGN

The previous learning methodologies offered the high range in accuracy and intrusion detection rate for unknown attacks. On the other hand, these approaches were unable to decrease the false alarm rate. In this research, a hybrid approach was proposed to satisfy both objectives in an

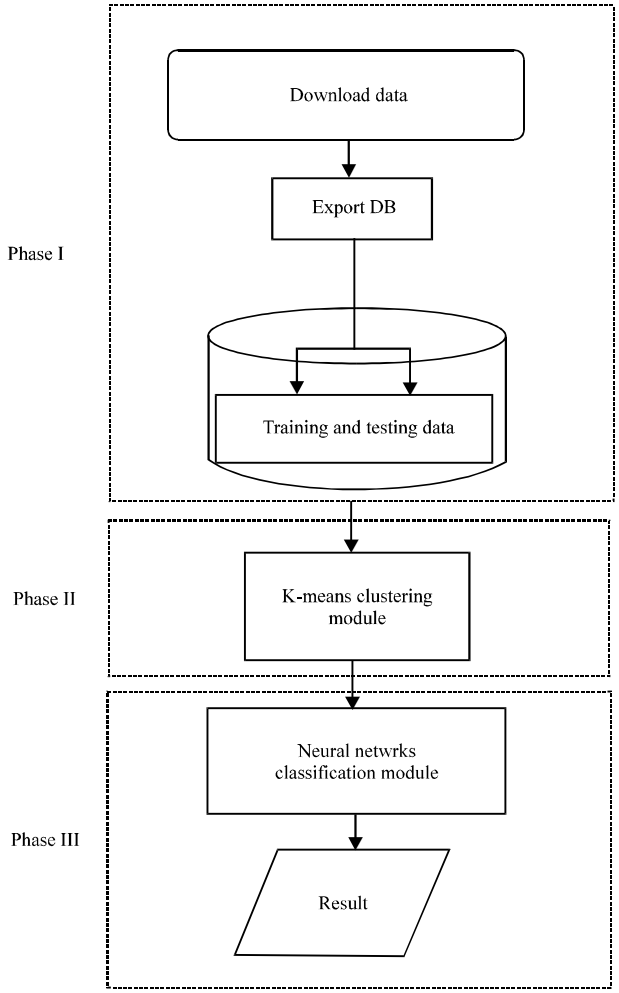

Fig. 2: Structural design of KM-NEU approach

acceptable range. Figure 2 illustrates the structural design of this approach for implementation of KM-NEU approach. Phase I is aimed for preparing data set while phase II and III designed for clustering and classification, respectively.

Phase I

Data preparation: In this phase, KDD Cup 99' (University of California, 1999) data set is downloaded from the website that mentioned in Fig. 2. Then the data is converted from the text format to comma separated value and will be uploaded to simulator. In this study, the training dataset contains 24 types of known attacks and testing set contained 14 additional types of unknown attacks. Training and testing datasets contain 494,020 and 311,029, respectively.

Phase II

K-means clustering: The data which provided in phase I is clustered by K-means clustering algorithm. As the result of grouping data into K number of clusters, the normal data is accurately separated from the attack data.

Table 1: Data distribution of the training and testing dataset

	No. of data		Percentage	
Class	Training dataset	Testing dataset	Training dataset	Testing dataset
Normal	97277	60593	19.69	19.400
Probe	4107	4166	0.83	1.330
Dos	391458	231455	79.24	74.400
U2R	52	88	0.01	0.028
R2L	1126	14727	0.23	4.730
Total	494020	311029	100.00	100.000

Phase III

Neural network classifier: Most of the previous works in this area used single classifiers like neural network, SVM, NB-Tree, GA and Zero-R. Due to the fact that, they have been unable to increase accuracy and detection rate while keep false alarm in low range, in this research the neural network MLP classifier is applied to the dataset just after the clustering phase. Neural network classifies the data into five specific categories which are Normal, Dos, U2R, Probe and R2L. This approach aim to reduce the false alarm while keeping accuracy and detection at high range.

In this research, the KDD Cup'99 is used as dataset which is generally accepted by means of a standard benchmark for evaluation of the intrusion detection system. This data set has been referred by many researchers (Wang *et al*., 2010). The "10% of KDD Cup'99" and "Corrected set (test)" from KDD Cup'99 are used to evaluate the KM-NEU as training and testing datasets correspondingly. The full KDD Cup'99 data set contain 41 feathers. In order to examine the ability of KM-NEU to detect different types of attacks, the training and testing dataset included all classes of intrusions like DoS, R2L, U2R and Probing. Table 1 illuminate the distribution of records in training and testing datasets regarding the categories.

Regarding the previous researches in IDS area, the performance of IDS is measured and evaluated by value of accuracy, detection rate and false alarm which defined in Eq. 3-5:

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \tag{3}$$

$$\text{Detection rate} = \frac{TP}{TP + FP} \tag{4}$$

$$\text{False alarm} = \frac{FP}{FP + TN} \tag{5}$$

- True positive (TP) when attack data detected as attack
- True negative (TN) when normal data detected as normal
- False positive (FP) when normal data detected as attack
- False negative (FN) when attack data detected as normal

RESULTS AND DISCUSSION

Two different experiments have been done in this research to compare the single classifier and hybrid approach using the training and testing datasets. In classification matter neural network

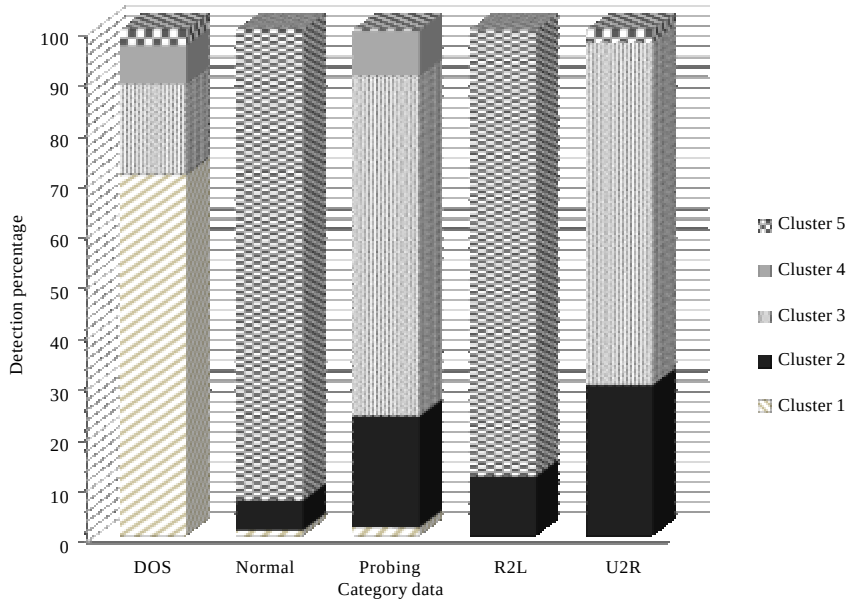

Fig. 3: Dispersion of four different types of attacks and normal data among five clusters

Table 2: Classification result for each type of data using testing dataset

Data	Normal (%)	Probe (%)	Dos (%)	U2R (%)	R2L (%)
Neural network	97.92	97.17	100.00	00.00	70.00
KM-NEU	99.99	99.97	99.99	99.99	99.98

MLP is selected as single classifier and K-means clustering pre-processing is combined with MLP to produce this approach as hybrid K-means and Neural Network (KM-NEU). Evaluation of this approach is based on the comparison of single ANN and hybrid approach in terms of accuracy, detection rate and false alarm. Moreover, KM-NEU approach is compared with the other related approaches which used the same KDD Cup'99 dataset (KDD Cup, 1999).

Figure 3 illustrates the dispersion of four different types of attacks and normal data among five clusters after applying K-means clustering pre-processing. From the Fig. 3 it can be perceived that a high percentage of DoS attack and normal data assigned to cluster 1 and 5 correspondingly. In addition, 60% of U2R and 70% of Probing attacks placed in cluster 3. This bundling prepares enhanced dataset which is useful to boost the neural network classification.

Table 2 represents how different types of data classified by Neural network and KM-NEU using the testing data set. Based on this table, KM-NEU outperformed the Neural Network single classifier in predicting Normal, Probe, DoS, U2R and R2L data types. Specifically there is a huge improvement in U2R type that amplified from 0-99.99%. However Single Neural Network detected 70% of R2L attacks, proposed KM-NEU increased this rate by 99.98.

As it observed in Table 3 Single Neural Network resulted in 1290 false positives and 1940 false negatives. On the contrary Table 3 also shows that the hybrid KM-NEU performs better than single Neural Network where none of normal data detected as attack and only 4 attacks were misclassified.

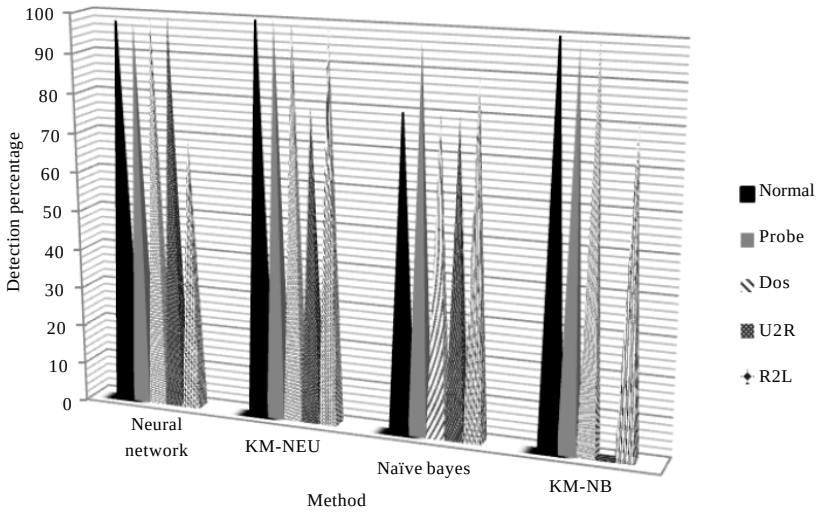

Fig. 4: Detection rate of KM-NEU and other approaches with five categories of attacks

Table 3: Detection results for the normal and attack classes using testing dataset

	Predicted normal		Predicted attack	
Actual	Single neural network	KM_NEU	Single neural network	KM-NEU
Normal	59327 or 97.9%	60592 or 99.9%	1290 or 2.13%	1 or 0.01%
Intrusion	1940 or 0.77%	4 or 0.001%	245379 or 99.23	250437 or 99.9%

Table 4: Detection rate for novel attacks using testing dataset

Name of attack	No. of vectors in test data set	Attack detection rate (%) single neural network	Attack detection rate (%) KM-NEU
Snmpgetattack	7741	0.02	100
Named	17	52.94	100
Xlock	9	55.55	100
Xsnoop	4	50.00	100
Sendmail	17	52.95	100
Saint	736	82.20	100
Xterm	13	61.54	100
Mscan	1053	7.50	100
Processable	759	1.45	100
Ps	16	81.25	100
Apache2	794	4.16	100
Udpstorm	2	100.00	0
Httptunnel	158	0.63	100
Worm	2	0.00	100
Mailbomb	5000	0.32	100
Sqlattack	2	100.00	100
Snmpguess	2406	0.04	100

Table 5: Summary of overall measurement using testing dataset

Measurements	Single neural network	KM-NEU	Improvement
Accuracy	99.98	99.99	+0.12
Detection rate	99.40	99.99	+0.95
False alarm	2.12	0.00	-2.12

The Corrected KDD (testing dataset) contains 17 new categories of attack which are 18729 data records. Table 4 shows the considerable improvement of proposed approach in contrast with single neural network classifier. Although KM-NEU was unable to detect any of UdpStorm attacks, the rest of attacks have been fully detected.

Table 5 summarizes the overall result for both single and hybrid classifiers. It is clear that KM-NEU improve the detection rate and accuracy for neural network, that shows +0.95, +0.12 and false alarm rate reached near zero by -2.12 reductions. Thus, KM-NEU performs much better in decreasing the misclassification constraints. It should be noted that employing the K-means clustering helped the classification process to get a better result on pre-processed dataset. Grouping similar data into 5 clusters boosted the hybrid approach to exceed the performance of neural network classifier.

Figure 4 compares the detection rates of four different classifiers with the proposed KM-NEU approach, divided into five categories. It can be seen from the Fig. 4 that, Neural network, KMNB and KM-NEU have detected almost all connections of DoS, Normal and Probe whereas, Naïve Bayes classifier shows poor results. Although, neural network was unable to detect any of U2R attacks, KM-NEU has improved it by 99.99 %. However, this hybrid approach has classified 99.99% percent of U2R but, the rest of techniques could not go further 90%.

CONCLUSION

Due to the related work about IDS, the challenges and gaps in this area are how to increase accuracy and detection rate while decrease the false alarm rate. In this work, KM-NEU is proposed which used K-means clustering to separate potentials attack from normal connections. Then, neural network MLP algorithm classified data into five specific categories namely: Dos, Probe, U2R, R2L and Normal. In comparison to single neural network, the hybrid approach can detect almost whole connections properly while decrease the false alarm from 2.2 to 0. In addition, proposed approach is able to detect almost all of novel attacks which single neural network could not detect them in an acceptable range. As the KM-NEU approach was unsuccessful to detect any of "Udpstorm" attacks, future work should concern it as weakness which can be improved.

REFERENCES

Adetunmbi, A.O., S.O. Falaki, O.S. Adewale and B.K. Alese, 2008. Network intrusion detection based on rough set and k-nearest neighbour. Int. J. Comput. ICT Res., 2: 60-66.

Aneetha, A.S. and S. Bose, 2012. The combined approach for anomaly detection using neural networks and clustering techniques. Comput. Sci. Eng. Int. J., 2: 37-46.

Bose, S., A.S. Aneetha and S. Revathi, 2012. Dynamic network anomaly intrusion detection system using modified SOM. Proceedings of 2nd International Conference of Computer Science, Engineering and Application, May 25-27, 2012, New York, pp: 27-34.

Cannady, J., 1998. Artificial neural networks for misuse detection. Proceedings of 21st National Information Systems Security Conference, October 5-8, 1998, Arlington, Virginia, USA., pp: 443-456.

Chandrashekhar, A. and K. Raghuveer, 2013. Fortification of hybrid intrusion detection system using variants of neural networks and support vector machines. Int. J. Network Security Appl., 5: 71-90.

Chen, W.H., S.H. Hsu and H.P. Shen, 2005. Application of SVM and ANN for intrusion detection. Comput. Oper. Res., 32: 2617-2634.

Hartigan, J.A., 1975. Data for Clustering Algorithms. John Wiley and Sons, New York, ISBN: 0-471-35645-X.

Hashemi, V.M., Z. Muda and W. Yassin, 2013. Improving intrusion detection using genetic algorithm. Inform. Technol. J., 12: 2167-2173.

Jabbehdari, S., S.H. Talari and N. Modiri, 2012. A neural network scheme for anomaly based intrusion detection system in mobile ad hoc networks. J. Comput., 4: 61-66.

KDD Cup, 1999. KDD cup'99: Computer network intrusion detection. http://www.kdd.org/kdd-cup-1999-computer-network-intrusion-detection

Kavitha, B., D.S. Karthikeyan and P.S. Maybell, 2012. An ensemble design of intrusion detection system for handling uncertainty using neutrosophic logic classifier. Knowl. Based Syst., 28: 88-96.

Lee, S., G. Kim and S. Kim, 2011. Self-adaptive and dynamic clustering for online anomaly detection. Expert Syst. Appl., 38: 14891-14898.

Li, Y., J. Xia, S. Zhang, J. Yan, X. Ai and K. Dai, 2012. An efficient intrusion detection system based on support vector machines and gradually feature removal method. Expert Syst. Appl., 39: 424-430.

Lippmann, R.P., D.J. Fried, I. Graf, J.W. Haines and K.R. Kendall *et al.*, 2000. Evaluating intrusion detection systems: The 1998 DARPA off-line intrusion detection evaluation. Proceedings of the 2000 DARPA Information Survivability Conference and Exposition (DISCEX), January 25-27, 2000, IEEE Computer Society Press, Los Alamitos, CA, pp: 12-26.

Muda, Z., W. Yassin, M.N. Sulaiman and N.I. Udzir, 2011. Intrusion detection based on K-means clustering and OneR classification. Proceedings of the 7th International Conference on Information Assurance and Security, December 5-8, 2011, Malacca, Malaysia, pp: 192-197.

Patcha, A. and J. Park, 2007. An overview of anomaly detection techniques: existing solutions and latest technological trends. Comput. Networks, 51: 3448-3470.

Selim, S.Z. and M.A. Ismail, 1984. K-means-type algorithms: A generalized convergence theorem and characterization of local optimality. IEEE Trans. Pattern Anal. Mach. Intell., 6: 81-87.

Shah, H., R. Ghazali and N.M. Nawi, 2012. Hybrid Ant Bee Colony Algorithm for Volcano Temperature Prediction. In: Emerging Trends and Applications in Information Communication Technologies, Chowdhry, B.S., F.K. Shaikh, D.M.A. Hussain and M.A. Uqaili (Eds.). Springer, USA, pp: 453-465.

Teng, S., H. Du, N. Wu, W. Zhang and J. Su, 2010. A cooperative network intrusion detection based on fuzzy SVMs. J. Networks, 5: 475-483.

Tsang, C.H., S. Kwong and H. Wang, 2007. Genetic-fuzzy rule mining approach and evaluation of feature selection techniques for anomaly intrusion detection. Pattern Recognition, 40: 2373-2391.

University of California, 1999. KDD Cup 99 KDD dataset. http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html

Wang, G., J. Hao, J. Ma and L. Huang, 2010. A new approach to intrusion detection using artificial neural networks and fuzzy clustering. Expert Syst. Appl., 37: 6225-6232.

Xiang, C., P.C. Yong and L.S. Meng, 2008. Design of multiple-level hybrid classifier for intrusion detection system using bayesian clustering and decision tree. Pattern Recognit. Lett., 29: 918-924.

Zhao, J., M. Chen and Q. Lou, 2011. Research of intrusion detection system based on neural networks. Proceedings of the IEEE 3rd International Conference on Communication Software and Networks, May 27-29, 2011, Xi'an, China, pp: 174-178.