VISUALIZE NETWORK ANOMALY DETECTION BY USING K-MEANS CLUSTERING ALGORITHM

A. M. Riad[1], Ibrahim Elhenawy[2] ,Ahmed Hassan[3] and Nancy Awadallah[1]

1Faculty of Computer Science and Information Systems, Mansoura University, Egypt
amriad2000@yahoo.com
rarecore2002@yahoo.com

2Faculty of Computer Science and Information Systems ,Zagazig University, Egypt
henawy2000@yahoo.com

3Faculty of Engineering Mansoura University , Egypt
arwaahmed1@gmail.com

ABSTRACT

With the ever increasing amount of new attacks in today's world the amount of data will keep increasing, and because of the base-rate fallacy the amount of false alarms will also increase. Another problem with detection of attacks is that they usually isn't detected until after the attack has taken place, this makes defending against attacks hard and can easily lead to disclosure of sensitive information.

In this paper we choose K-means algorithm with the Kdd Cup 1999 network data set to evaluate the performance of an unsupervised learning method for anomaly detection. The results of the evaluation showed that a high detection rate can be achieve while maintaining a low false alarm rate .This paper presents the result of using k-means clustering by applying Cluster 3.0 tool and visualized this result by using TreeView visualization tool .

KEYWORDS

Intrusion detection, Clustering, K-means, Kdd Cup 99, Cluster 3.0, Visualization, TreeView

INTRODUCTION

Network Intrusion Detection System (NIDS) is one that scans the network activities in a computer environment ,and detect the intrusions or attacks. Then, the system administrator may be alerted to the take the corrective actions. Network intrusion detection approaches are : signature-based and anomaly detection. The oldest method in practice is the signature-based method which depends on a signature database of previously known attacks. A model-based supervised method is misuse detection which trains a classifier with labeled patterns to classify new unlabeled patterns. To detect abnormal behaviors in patterns, anomaly detection approaches can make use of supervised or unsupervised methods. [1] Intrusion detection evaluation problem and its solution usually affect the choice of the suitable intrusion detection system for a particular environment depending on several factors. The false alarm rate and the detection rate are the most

basic of these factors; they are calculated from the main four instances True Positive (TP), True Negative (TN), False Positive(FP) and False Negative (FN) .[22]

Grouping objects into meaningful subclasses is clustering method . For classifying log data and detecting intrusions, clustering methods can be useful .

The most important unsupervised learning process in data mining is clustering, it used to find the structures or patterns in a collection of unlabeled data. There are two main types of clustering algorithms ,it can be categorized into: partitioning algorithm, hierarchical algorithm.

Four major categories of attacks are found on KDD dataset : Probing attacks (information gathering attacks), Denial of-Service (DoS) attacks (deny legitimate requests to a system), user-to-root (U2R) attacks (unauthorized access to local super-user or root), and remote-to-local (R2L) attacks (unauthorized local access from a remote machine). Each labeled record in KDD dataset is consisted of 41 attributes (features) and one target value. [20]

Section 2 presents researcher's previous studies in this field, section 3. Presents clustering methods, section 4 describes k-means algorithm, section 5 describes KDD cup 99 dataset and section 6. Presents proposed work.. The paper presents the result of using k-means clustering algorithms by using Cluster 3.0 tool and visualized this result by using TreeView visualization tool.

2. RELATED WORK

Jose F. Nieves , presented a comparative study with more emphasis on the unsupervised learning methods for anomaly detection. K-means algorithm with KDD Cup 1999 network data set are used to evaluate the performance of an unsupervised learning method for anomaly detection. High detection rate can be achieve while maintaining a low false alarm rate is the results of this work evaluation .[1]

L. Portnoy et all , presented clustering-based intrusion detection algorithm, which trains on unlabeled data in order to detect new intrusions. Different types of intrusions are detect by their method, while a low false positive rate is maintained as verified over the KDD CUP 1999 dataset.[2]

E.Eskin et all , presented algorithms that are designed to process unlabeled data ,they presented a new geometric framework for unsupervised anomaly detection. [3]

K. Nyarko et all, presented network visualization techniques for intrusion detection on small and large-scale networks. They showed that haptic technologies can provide another dimension of information critical to the efficient visualization of network intrusion data. [4]

K.Labib, V. Vemuri , presented the S Language as a tool for the implementation of intrusion detection systems. Anomaly-based detection selected the two type of attacks such as Denial-Of-Service (DoS) and Network Probe attacks are schemed for detecting from the 1998 DARPA. [5]

P. Ren et all, presented IDGraphs as an interactive visualization system for intrusion detection. using the Histographs technique is used to summarize a stack of thousands of these traces, which maps data frequency at each pixel to brightness. [6][26][27][28][30][31][32]

P. Laskov et all , presented a new technique for visualization of anomaly detection based on prediction sensitivity. Its application enables an expert (a) to interpret the predictions made by anomaly detection and (b) to select informative features in order to improve detection accuracy. [7]

A. Mitrokotsa, C. Douligeris , proposed an approach that detects Denial of Service attacks using Emergent Self-Organizing Maps. The approach is based on classifying "normal" traffic against "abnormal" traffic in the sense of Denial of Service attacks. The approach permits the automatic classification of events that are contained in logs and visualization of network traffic. Extensive simulations show the effectiveness of this approach compared to previously proposed approaches regarding false alarms and detection probabilities. [8]

J. Peng et all, presented a hybrid intrusion detection and visualization system that influence the advantages of signature-based and anomaly detection methods. When intrusion is detected it is protecting the system from internal and external attacks and autonomous agents will automatically take actions against misuse and abuse of computer system. [9]

X.Cui et all, the swarm based visual data mining approach (SVDM) is a technique developed to help user gain insight into the alert event data of the intrusion detection system. The SVDM can help administrators detect anomaly behaviors of malicious user. The output visual representation exploits the ability to recognize patterns and utilizes it to help security administrators understand the relationship between the discrete security breaches. [10]

A.Frei, M. Rennhard , proposed Histogram Matrix (HMAT) which is a novel log file visualization technique. It visualizes the content of a log file to enable administrator to spot anomalies. The system uses a combination of graphical and statistical techniques and allows even non-experts to interactively search for anomalous log messages. The system allows to automatically generating security events if an anomaly is detected. Researchers introduced HMAT, demonstrate its functionality using log files from a variety of services in real environments, and identify strengths and limitations of the technique. [11]

L. Dongxia and Z. Yongbo , an intrusion detection module based on honeypot technology presented are presented ,which utilizes IP Traceback technique. By using honeypot technology, this module traces the intrusion source farthest.[12]

M. Jianliang et all , K-means algorithm to cluster and analyze the data of KDD-99 dataset. This algorithm can detect unknown intrusions in the real network connections. The simulations results that run on KDD-99 data set showed that the K-means method is an effective algorithm for partitioning large data set. [13]

B. K. Kumar and A. Bhaskar , presented an approach for identifying network anomalies by visualizing network flow data which is stored in weblogs. Various clustering techniques can be used to identify different anomalies in the network. Here, they present a new approach based on

simple K-Means for analyzing network flow data using different attributes like IP address, Protocol, Port number etc. to detect anomalies. By using visualization, they can identify which sites are more frequently accessed by the users. In their approach they provide overview about given dataset by studying network key parameters. In this process they used preprocessing techniques to eliminate unwanted attributes from weblog data [14].

3. CLUSTERING METHODS

The task of cluster analysis is grouping a set of objects in a way that objects in the same group which called (cluster) are more similar to each other than to those in other groups (clusters).

Clustering algorithms fall into two categories hierarchical and partitioning algorithms.

A. Hierarchical Algorithms:

In this type of clustering data are not gets clustered at ones instead stepwise procedures is followed for clustering the datasets. [1]

Hierarchical clustering can be classified as:

- **Division clustering**

Whole data point is considered as a single cluster and formation of new clusters starts from the whole data point to single datapoint. It starts form root to leave.

- **Agglomerative Clustering**

Formation of the clusters starts by combining two instances based upon the certain criteria. It starts form leave to root. [5][16]

B. Partitioning Algorithms:

It divides the data set into k clusters, where the integer k needs to be specified. The algorithm is run for a range of k values.

- **K-Mean Clustering**

In this method, assignment of the data points to clusters is depending upon the distance between cluster centroid and data point.

There are three variation of k-mean clustering, **k-mean:** which is used for numerical data sets,

k-mediod : which is used for categorical datasets and **k-prototype:** is used for numerical and categorical dataset .[1][16]

- **Fuzzy C Mean Clustering**

This algorithm concerned with the distance calculation, membership of the data points with the cluster are also considered.[15]

- **QT Clustering**

It groups datapoint into clusters. By finding large cluster whose diameter does not exceed a given user-defined diameter threshold value the quality is ensured. [16]

4. K-MEANS CLUSTERING

The observations in this algorithm are classified as belonging to one of k groups. By calculating the centroid for each group and assigning each observation to the group with the closest centroid Group membership is determined.

Number of cluster centers is choosed to minimize the within-class sum of squares of the vectors for those centers. K-means algorithm uses Euclidean distance.

The general steps for the K-means algorithm were the following:

1. Number of clusters (K) are choosed
2. Centroids Initialization
3. Each pattern Assigned to the cluster with closest centroid
4. Means of each cluster is calculate to be its new centroid
5. Repeat step 3 until stopping criteria is met
6. The best clustering solution was chosen after repeating this procedure 10 times. [1][13]

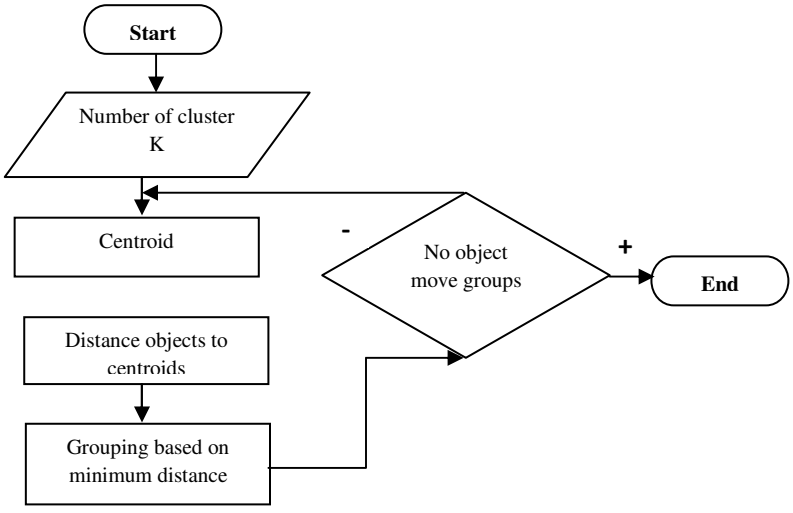

Figure 1. K-means clustering process [17]

4.1 Distance Calculation

A distance function is required to compute the distance between two objects. The Euclidean is the most commonly used distance function, it is one which is defined as: Formula

$$d(x, y) = \sqrt{\sum_{i=1}^{m} (x_i - y_i)^2} \quad \textbf{(1)}$$

In previous equation two input vectors are with m quantitative features where x = (x1;:; xm) and y = (y1;:; ym) .In the Euclidean distance function, all features contribute equally to the function value.

5. KDD CUP 99 DESCRIPTION DATASET

The KDD-99 (Knowledge Discovery in Databases) [18] dataset is a standard set of data that can be used in order to evaluate proposed approaches in the area of intrusion detection. Four major categories of attacks found in KDD dataset are: Probing attacks which related to (information gathering attacks), the attack (deny legitimate requests to a system) is Denial-of-Service (DoS) attacks user-to-root (U2R) attacks (unauthorized access to local super-user or root), and remote-to-local (R2L) attacks (unauthorized local access from a remote machine) [8][19]. KDD dataset is composed of labeled and unlabeled records. Each labeled record consisted of 41 attributes (features) which are:

Fundamental Properties: the basic properties are obtained from differential of packet without the investigation of useful load for transmission.

Content: knowledge in this case is used for evaluation of useful load for transmission in TCP packets and involves failed attempts to log in system.

Traffic property based on time: these features are designed to get properties that are happened in more than two seconds continuously. A sample of these features shows the number of connections to the host.

Traffic property based on the host: It uses historical window to estimate the number of connections instead of time. Also, it is designed to assess the extent attacks that are happened in more than two seconds. In international knowledge discovery and data mining only 10% KDD of dataset is used for training purposes. [20]

6. VISUALIZE INTRUSION DETECTION USING K-MEANS CLUSTERING

In previous sections the clustering techniques are presented such as K-Means ,also the KDD dataset and its features are explained .In this section, the proposed work is presented; it will improve and comprehend the result of clustering technique through visualization.

The proposed work contains 3 stages after entering corrected KDD dataset. The first stage is to fragment the 37 attacks which are founded in this dataset into four general categories (DOS, Probe, R2L, and U2R).

The second stage is to use Cluster 3.0 tool for apply k-means technique to cluster attacks. And last stage is to use TreeView visualization tool to visualize k-means result.

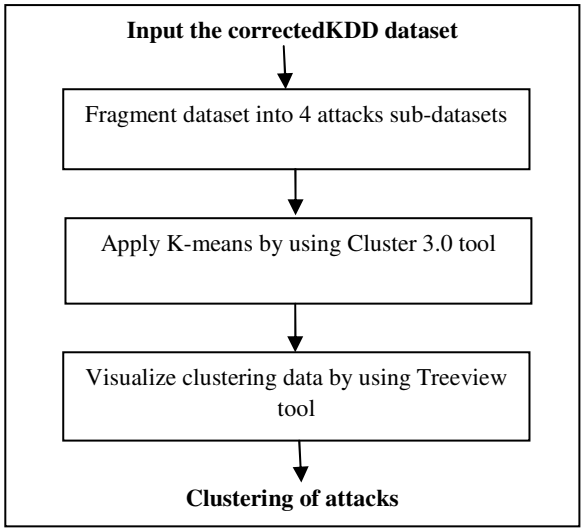

Figure 2. : Architecture of the proposed system

6.1 KDD Fragmentation

The KDD cup 99 intrusion detection consists of three components, which are detailed in Table 1. There are only 22 attack types in "10% KDD" dataset and they are mostly of denial of service category. different statistical distributions in "Corrected KDD" dataset compared to "10% KDD" or "Whole KDD". It contains 37 types of attacks. Table 1 gives number of records in each attack category. [22][23]

TABLE 1. THE KDD 99 Intrusion Detection Datasets Characteristics In Terms of Number Of Samples [22][23]

Dataset	DoS	Probe	U2R	R2L	Normal
"10%KDD"	391458	4107	52	1126	97277
"CorrectedKDD"	229853	4166	70	16347	60593
WholeKDD"	3883370	41102	52	1126	972780

The KDD Cup 1999 data contains a wide variety of intrusions .Each sample in the data is a record of extracted features from a network connection gathered during the simulated intrusions. [33]

A connection is a sequence of TCP packets to and from various IP addresses. A connection record consists of 41 fields. Basic features about TCP connection as duration, protocol type, number of bytes transferred, domain specific features as number of file creation, number of failed login attempts, and whether root shell was obtained. [33]
The Corrected KDD is used for proposed experiment. There are 37 types of attacks (as showed in figure 4) in the dataset which are classified into four categories (Probe, Dos, U2R, R2L) are shown in Table 2.

TABLE 2. Attack Types With Their Corresponding Categories [23]

Category	Types Of Attack
Probe	Satan, nmap, portsweep, mscan, ipsweep, saint
DoS	udpstorm apache, mailbomb, back, neptune ,land, smurf, teardrop, processtable , pod
U2R	xterm ,buffer_overflow, rootkit, ps, loadmodule, perl, sqlattack,
R2L	Httptunnel, ftp_write, worm, imap, xlock, multihop, warezmaster, named, snmpguess, phf, , snmpgetattack, xsnoop, guess_password ,sendmail

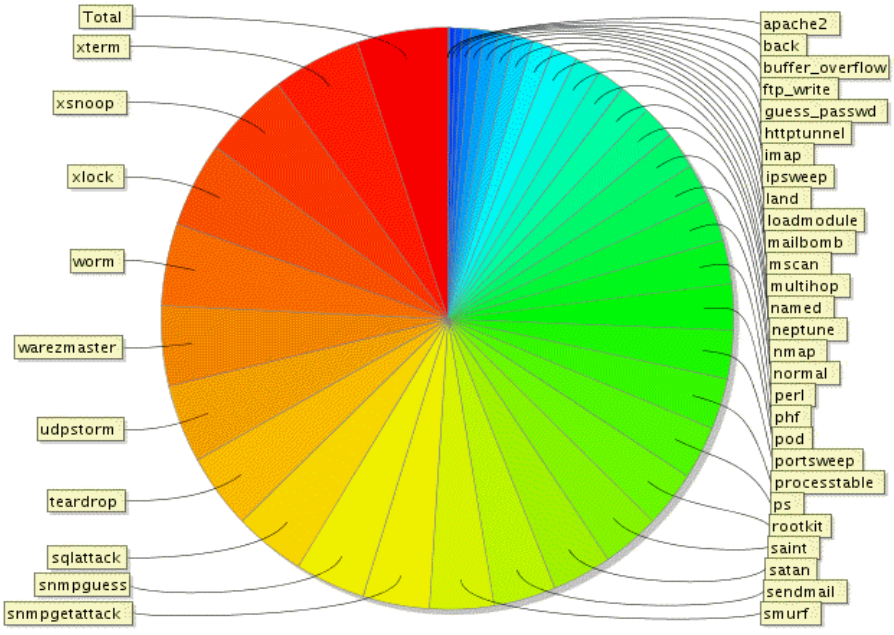

Figure 3.: The 37 types of Attack founded in corrected KDD

In the next figure the classification of 37 attack types into four categories (DoS , Probe, U2R, R2L).Figure 3.,4. are extracted from RapidMiner program.

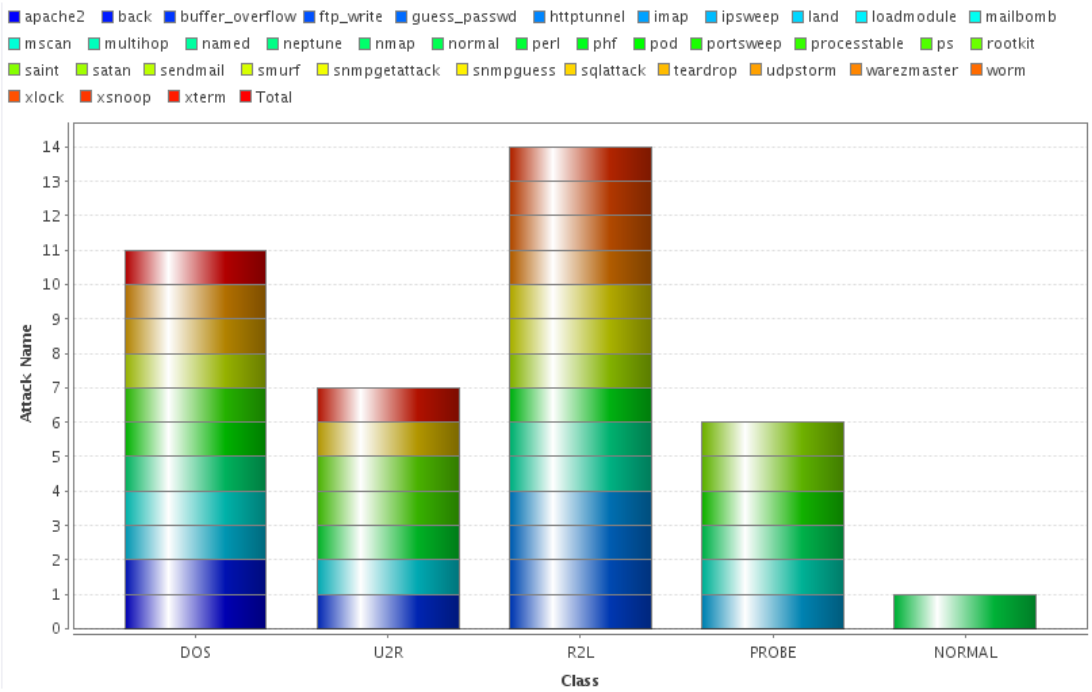

Figure 4: Bar stacked between Class and Attack name

6.2 Apply K-means by Using Cluster 3.0 tool

The following criteria were used: detection rate and false alarm rate. The number of attacks detected divided by the total number of attacks is defined as (detection rate). The number of 'normal' patterns classify s attacks divided by the total number of 'normal' patterns is defined as (false alarm rate). [1]

The number of malicious correctly classified as malicious: **True Positives (TP)**;
The number of benign programs correctly classified as benign is called: **True Negatives (TN);**
The number of benign programs falsely classified as malicious is called: **False Positives (FP);**
The number of malicious falsely classified as benign is called: **False Negative (FN)** [21]

May be defines as follows:

Detection Rate (DTR) = TP / (TP + TN) [24]
False Alarm Rate (FPR) = FP / (TN + FP) [21][25]

The total number of ‘normal’ patterns: 60593
The total number of 'attacks' patterns: 250436
The total number of all detection: 311029

TABLE 3. Experiment Results Of K-Means

Clustering Technique		DOS	Probe	U2R	R2L
K-Means K=4	**Detection rate**	0.9993	0.0656	0.00005	0.064
	False Alarm	0.001	0.004	0.00007	0.0001
K-Means K=5	**Detection rate**	0.9766	0.0659	0.00061	0.381
	False Alarm	0.003	0.013	0.0004	0.0022
K-Means K=6	**Detection rate**	0.9643	0.0654	0.00099	0.4997
	False Alarm	0.004	0.026	0.008	0.001

The experiment results show that K-means when k=4 is the best as detection rate is high and false alarm rate is less than others.

The next figure illustrates the detection rate and false alarm for the four categories of attacks (DOS, Probe, R2L, U2R) with different clusters (k=4, 5, 6)

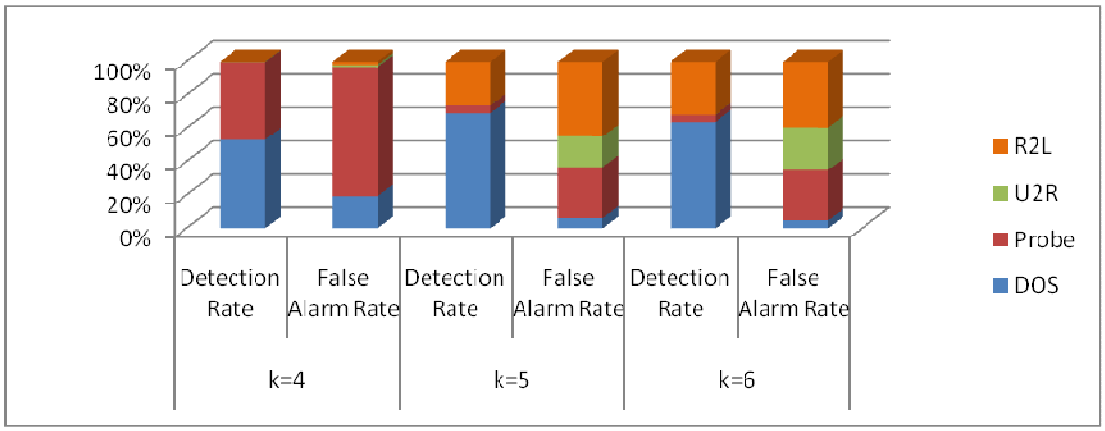

Figure 5. : Detection Rate & False Alarm with different K clusters

6.2.1 Cluster 3.0 tool

To provide a computational and graphical environment for analyzing data from genomic datasets Cluster and TreeView programs are used. Organizing and analyzing the data in a number of different ways is the responsibility of Cluster program. To allow the organized data to be visualized and browsed TreeView program is used. [34]

Load data file option under the File menu is used for loading data to be into Cluster. The functions that provided for adjusting and filtering the loaded data are accessed via the Filter Data and Adjust Data tabs.

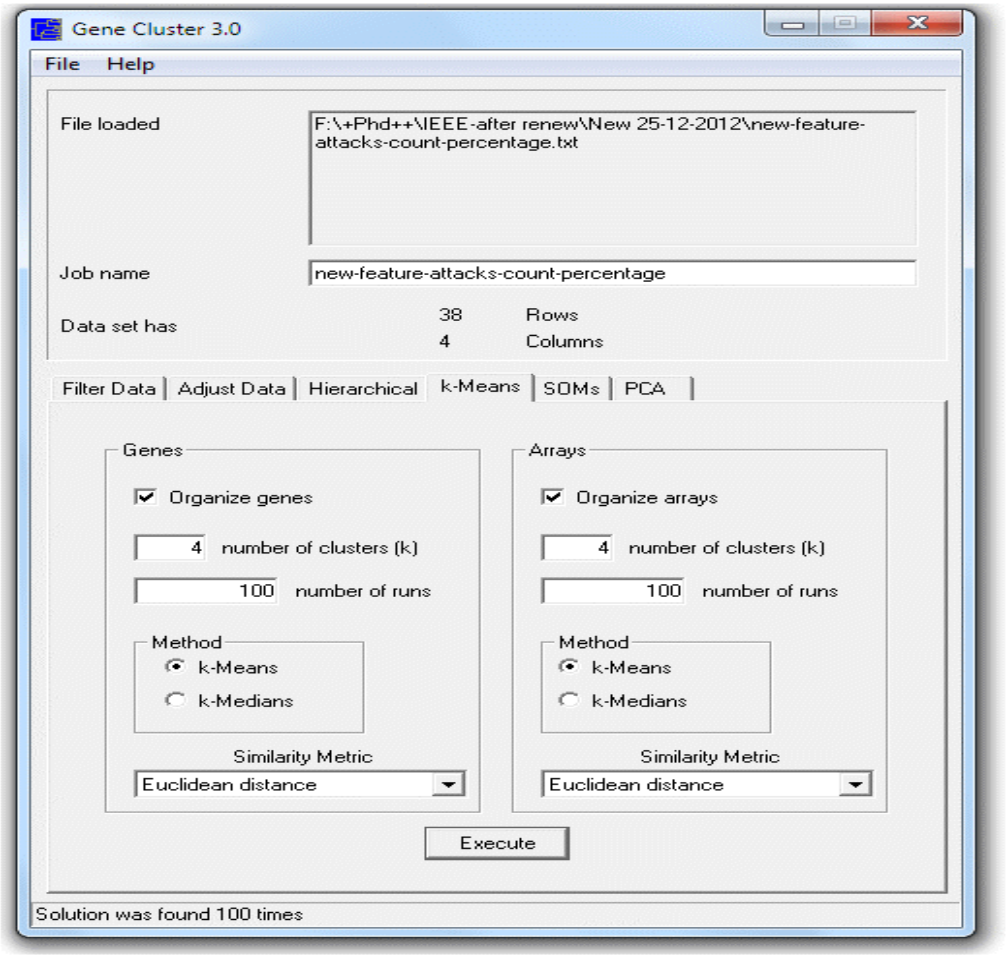

Figure 6: Using K-means in Cluster 3.0 tool

In the previous figure illustrated how K-means clustering implemented in Cluster 3.0 allows any of the eight distance measures to be used; it had recommended using the Euclidean distance or city-block distance instead of the distance measures based on the Pearson correlation. To use k-means clustering with a distance measure based on the Pearson correlation, Researcher in this experiment first normalize the data appropriately (using the "Adjust Data" tab) before running the k-means algorithm.

Cluster 3.0 tool deals with attached data, applying k-means technique for clustering. This tool enables users to choose the number of clusters which are (4) clusters, and the numbers of runs which are (100). Also similarity metric which be used is Euclidean distance function which illustrated in section 4.1.

An assignment of items to a cluster is the output simply. The output data file is 'new-feature-attacks-count-percentage_KG4_A4.CDT', where '_KG4' point to items were organized, and '_A4' point to arrays were organized.

6.3 Visualize Clustering Data by Using TreeView Tool

After applying k-means algorithm by using clustering tool which called (Cluster 3.0), the result will be entered to TreeView program to visualize clustering data. TreeView is a program for viewing the results of expression clustering performed by the associated program Cluster 3.0. TreeView reads in matching *.CDT and *.GTR files produced by Cluster 3.0. A thumbnail image is generated along with a view of the tree. The next figure illustrated TreeView visualization tool result .

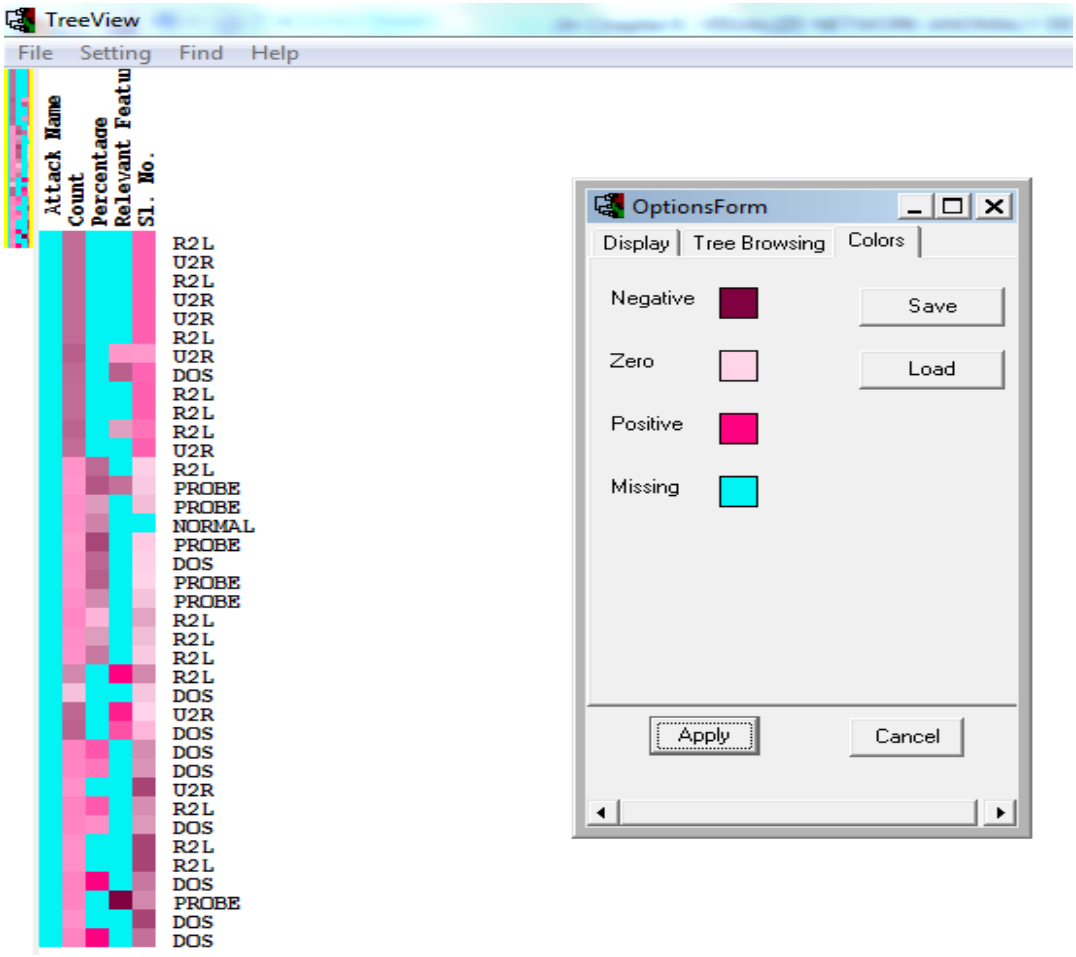

Figure 7: Visualized clustering data via TreeView

This tool working with the result of k-means technique which be extracted from Cluster 3.0 tool 'new-feature-attacks-count-percentage_KG4_A4.CDT'.There are general four attacks categories (DOS, Probe, R2L, and U2R) visualized from applying .

7. CONCLUSION

In this paper we presented an approach for visualizing network attacks data using clustering. It is an easy, simple and fast way of analyzing the flow data. By the help of clustering we can predict the type of flow i.e. attacks or normal by performing some clustering on the particular attributes. We present the K-means algorithm for intrusion detection and apply it by using Cluster 3.0. Results on a subset of KDD-99 dataset showed accuracy of the algorithm. To visualize clustering data we use TreeView visualization tool.

ACKNOWLEDGEMENTS

The authors would like to thank all the people and institutions that have allowed them to use many of the figures present in this paper.

REFERENCES

[1] J. F. Nieves ,"Data Clustering for Anomaly Detection in Network Intrusion Detection " ,Research Alliance in Math and Science , August, pp.1-12, 2009 .

[2] L. Portnoy , E. Eskin , S. Stolfo , " Intrusion detection with unlabeled data using clustering", In Proceedings of ACM CSS Workshop on Data Mining Applied to Security (DMSA-2001) , Philadelphia , PA,USA ,2001.

[3] E.Eskin, A.Arnold, , M. Prerau, L.Portnoy, S. Stolfo, "A geometric framework for unsupervised anomaly detection: Detecting intrusions in unlabeled data", Applications of Data Mining in Computer Security(2002), Norwell, MA, USA, Dec., pp. 78–100,2002.

[4] K. Nyarko, T. Capers, C. Scott, K. Ladeji-Osias," Network Intrusion Visualization with NIVA, an Intrusion Detection Visual Analyzer with Haptic Integration", IEEE, 2002.

[5] K.Labib, V. R. Vemuri, "Anomaly Detection Using S Language Framework: Clustering and Visualization of Intrusive Attacks on Computer Systems". Fourth Conference on Security and Network Architectures, SAR'05, Batz sur Mer, France, June 2005

[6] P. Ren , Y. Gao , Z. Li , Y. Chen and B. Watson , "IDGraphs: Intrusion Detection and AnalysisUsing Histographs" ,IEEE , 2005 .

[7] P. Laskov, K. Rieck, C. Schäfer, K.R. Müller, "Visualization of anomaly detection using prediction sensitivity", Proc.of Sicherheit, April 2005, 197- 208.

[8] A. Mitrokotsa, C. Douligeris ," Detecting Denial of Service Attacks Using Emergent Self-Organizing Maps" , Signal Processing and Information Technology, 2005. Proceedings of the Fifth IEEE International Symposium , pp. 375 – 380 ,IEEE,2005.

[9] J. Peng, C. Feng, J.W. Rozenblit , "A Hybrid Intrusion Detection and Visualization System" , Engineering of Computer Based Systems, 2006. ECBS 2006. 13th Annual IEEE International Symposium and Workshop , , pp. – 506, IEEE ,2006.

[10] X.Cui, J.Beaver, T. Potok and L.Yang , "Visual Mining Intrusion Behaviors by Using Swarm Technology" , System Sciences (HICSS), 2011 44th Hawaii International Conference , pp. 1 – 7, IEEE 2011.

[11] A.Frei, M. Rennhard ," Histogram Matrix: Log File Visualization for Anomaly Detection", IEEE , 2007 .

[12] L. Dongxia , Z. Yongbo ," An Intrusion Detection System Based on Honeypot Technology" ,Computer Science and Electronics Engineering (ICCSEE), 2012 International Conference on IEEE, Vol.1,2012 .

[13] M. Jianliang , S. Haikun, B. Ling, "The Application on Intrusion Detection Based on K-means Cluster Algorithm" , IFITA '09 Proceedings of the 2009 International Forum on Information , Technology and Applications – Vol.1,pp. 150-152,IEEE ,2009.
[14] B. K. Kumar , A. Bhaskar , "Identifying Network Anomalies Using Clustering Technique in Weblog Data", International Journal of Computers & Technology, Vol. 2 No. 3, June, 2012.
[15] S. Akbar , K.Nageswara Rao , J.A.Chandulal ," Intrusion Detection System Methodologies Based on Data Analysis",International Journal of Computer Applications ,Vol. 5 , No.2 , August 2010.
[16] K.Bharti, S. Shukla, S. Jain ,"Intrusion detection using clustering", IJCCT, Vol.1 , 2010
[17] S.Jain , M. Aalam , M.Doja , " K-means clustering using weka interface" , Proceedings of the 4th National Conference; INDIACom, Computing For Nation Development, 2010.
[18] The Third International Knowledge Discovery and Data Mining Tools Competition, May 2002,Available from http://kdd.ics.uci.edu/databases/kddcup99.kddcup99.html.
[19] M. Sabhnani ,G. Serpen, "Application of Machine Learning Algorithms to KDD Intrusion Detection Dataset within Misuse Detection Context ", In Proceedings of the International Conference on Machine Learning, Models, Technologies and Applications (MLMTA 2003), Vol. 1, (2003).
[20] F.S.Gharehchopogh, Neda Jabbari, Zeinab Ghaffari Azar ,"Evaluation of Fuzzy K-Means And K-Means Clustering Algorithms In Intrusion Detection Systems" , International Journal of Scientific & Technology Research ,Vol. 1, issue 11, December 2012.
[21] M. E. Elhamahmy, H. N. Elmahdy , I. A. Saroit ,"A New Approach for Evaluating Intrusion Detection System" , International Journal of Artificial Intelligent Systems and Machine Learning, Vol. 2, No 11, November 2010 .
[22] Dr.S.Siva Sathya, Dr. R.Geetha Ramani and K.Sivaselvi. "Discriminant Analysis based Feature Selection in KDD Intrusion Dataset ", International Journal of Computer Applications 31(11):1-7, October 2011.
[23] P. G.Jeya , M. Ravichandran and C. S. Ravichandran ," Efficient Classifier for R2L and U2R Attacks. International Journal of Computer Applications 45(21):29-32, May 2012 .
[24] F. N. M. Sabri, N. M.Norwawi, K. Seman," "Identifying False Alarm Rates for Intrusion Detection System with Data Mining", International Journal of Computer Science and Network Security, VOL. 11 No. 4, April 2011
[25] P. Divya , R. Priya," Clustering Based Feature Selection and Outlier Analysis ",International Journal of Computer Science & Communication Networks, Vol 2(6), pg.647-652.
[26] C.Ahlberg, B. Shneiderman ," Visual information seeking: tight coupling of dynamic query filters with starfield displays" , In proceeding of: Conference on Human Factors in Computing Systems, CHI 1994, Boston, Massachusetts, USA, pp. 313-317,April 24-28, 1994.
[27] S. Noel , M. Jacobs , P. Kalapa , S. Jajodia "Multiple Coordinated Views for Network Attack Graphs", Visualization for Computer Security,.(VizSEC 05). IEEE Workshop on, 99-106,2005
[28] http://www.researchgate.net/publication/27521564_The_Information_Mural_A_Technique_for_ Displaying_and_Navigating_Large_Information_Spaces
[29] http://www.ukessays.com/essays/information-technology/intrusion-detection-system-methodologies-data-analysis-information-technology-essay.php
[30] http://dl.acm.org/citation.cfm?id=1106724
[31] http://www.computer.org/csdl/proceedings/vizsec/2005/2782/00/27820005-abs.html
[32] http://dl.acm.org/citation.cfm?id=1106719
[33] Ms. P. K. Karmore and MS. S. T. Bodkhe ,"A Survey on Intrusion in Ad Hoc Networks and its Detection Measures" , International Journal on Computer Science and Engineering (IJCSE) ,3(5),pp.1896-1903,May 2011 .
[34] http://bonsai.hgc.jp/~mdehoon/software/cluster/cluster3.pdf - Last visiting at 21.06.2013.