HYBRID MACHINE LEARNING TECHNIQUE FOR INTRUSION DETECTION SYSTEM

Hatim Mohamad Tahir[1], Wael Hasan[2], Abas Md Said[3], Nur Haryani Zakaria[4], Norliza Katuk[5], Nur Farzana Kabir[6], Mohd Hasbullah Omar[7], Osman Ghazali[8], and Noor Izzah Yahya[9]

[1,2,4,5,6,7,8,9]*Universiti Utara Malaysia, Malaysia,* hatim@uum.edu.my
[3]*Universiti Teknologi PETRONAS, Malaysia,* abass@utp.edu.my

ABSTRACT. The utilization of the Internet has grown tremendously resulting in more critical data are being transmitted and handled online. Hence, these occurring changes have led to draw the conclusion that the number of attacks on the important information over the internet is increasing yearly. Intrusion is one of the main threat to the internet. Various techniques and approaches have been developed to address the limitations of intrusion detection system such as low accuracy, high false alarm rate, and time consuming. This research proposed a hybrid machine learning technique for network intrusion detection based on combination of K-means clustering and support vector machine classification. The aim of this research is to reduce the rate of false positive alarm, false negative alarm rate and to improve the detection rate. The NSL-KDD dataset has been used in the proposed technique. In order to improve classification performance, some steps have been taken on the dataset. The classification has been performed by using support vector machine. After training and testing the proposed hybrid machine learning technique, the results have shown that the proposed technique has achieved a positive detection rate and reduce the false alarm rate.

Keywords: intrusion detection, hybrid intelligent technique, K-means, SVM, NSL-KDD

INTRODUCTION

In recent decades, computer networks (internet) have become broadly used. A lot of sensitive information and services passes through various kinds of computer and mobile devices . Such these changes have led to increase number of threats on important information over the network systems. Hence, the network security has become a significant issue to prevent dangerous threats and to protect sensitive data over the network. Intrusion is one of the broad types of threats over the Internet.

In order to recognize the attacks with high accuracy, different techniques have been applied and suggested over the last few years. Most recent methods for processing of detecting network system attack have been utilizing machine learning techniques for automating the detection process (Upadhyaya & Jain, 2013; Wankhade, Patka, & Thool, 2013) Machine learning performs a major role in intrusion detection via decreasing and categorizing the data according to the clusters. This research has proposed a hybrid machine learning technique for network intrusion detection based on combination of K-Means clustering and support vector

machines (SVM) classification to overcome the mentioned limitation in existing hybrid intelligent approaches.

INTRUSION DETECTION SYSTEM

Intrusion detection system(IDS) is a dynamic security system which can provide effective defense to the information stored in the network systems. The main objective of deploying the IDS is to recognize abuse, illegitimate use and misuse of network system attacks and to prevent them from carrying out their attacks. On other hand, IDS performs three main security tasks which are monitoring the activities of networks users, detecting and responding to malicious actions respectively for both two types of attacks (Anantvalee & Wu, 2007; Brutch & Ko, 2003).

In general, intrusion detection system (IDS) can be categorized into two broad approaches come under this classification and they are misuse and anomaly approach. Misuse approach is the ability for detecting attacks depending on predefined signatures of malicious activities. Systems store patterns or signatures of known attacks and use them to compare with the actual activities or captured data. For signature detection method, the IDSs analyze the data which are collected and compared to attacks pattern, which are saved in the big database of known attacks (Albers et al., 2002; Anantvalee & Wu, 2007). Anomaly detection approach depends on defining a network behavior (profile) and trying to detect traffic on deviation created by normal network behavior. For anomaly method, the system administrators determine the normal profile (baseline) for the traffic of the network, protocols and typical package size, breakdown (Farhan, Zulkhairi, & Hatim, 2008).

DESIGN OF PROPOSED HYBRID TECHNIQUE

The proposed hybrid machine learning technique applies clustering on all data by dividing and labeling into the corresponding group. A clustering algorithm which used K-means divides and labels the data for the corresponding groups before applying a classifier technique. A Support Vector Machine (SVM) is a technique used for classification purpose. Figure 1 shows the proposed hybrid technique model.

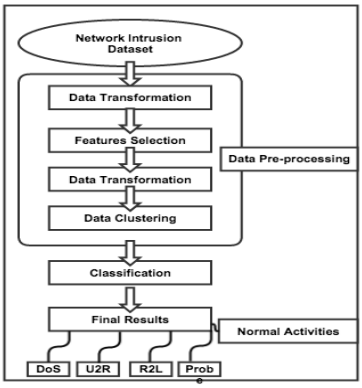

Figure 1. Proposed Hybrid Technique Model

K-Means Clustering

Data clustering is a popular technique for intrusion detection. Labelling and grouping of dataset are important and natural patterns in the K-means clusters (Jain, Sharma, & Sisodia, 2011; Jaisankar & Kannan, 2011). The manual labeling of dataset is expensive and time consuming because of the huge amount of network data available. Clustering is the process of

grouping, labeling the data and determining it into sets of similar objects (Chapke Prajkta & Raut, n.d.). Every set is named as cluster.

K-means is one of well-known data mining clustering algorithms. K-means has been performed in an attempt to detect abnormal network user behavior in a network traffic. The difficulty of recognizing among normal and intrusion behavior in network systems is a major challenge using clustering techniques because of the overlapping in data monitoring. The detection processing causes true and false alarms in the intrusion detection system. The main aim of applying the K-Means clustering algorithm is to separate the set of normal and abnormal data that behave similarly for different partitions which are known as K-th cluster centroids (Joshi & Pimprale, 2013; Mohammad, Sulaiman, & Khalaf, 2011).

Support Vector Machine Classification

Support Vector Machine (SVM) Classification is a machine learning techniques that deals with every instance of data set and classifies it to a specific class. Classification process consists of two steps. The first step is learning by training phase and the second step is by classification. In the learning step, a classifier is formed and in the classification step that model is used to predict the class labels for a given data (Neethu, 2012) .

Nowadays, SVM technique is mature enough to apply for different domain classification problems (Jain et al., 2011). It plots the training vectors in high dimensional feature space assign each vector by its class. It classifies data by determining a set of support vectors which are the members of the set of training inputs that outline a hyper plane in the feature space. SVMs provide a generic mechanism to fit the surface of the hyper plane to the data via the use of a kernel function.

EXPERIMENTS

For the purpose of running the experiment, a simulation environment has been selected due to the ease of varying different parameters of the environment and observing the results. The fully functional WEKA machine learning software is an open source tool. The results will be presented in two different methods namely Confusion Matrix and Receiver Operating Characteristic curve (ROC). A ROC curve is to help us decide where to draw the line between 'normal' and 'not normal' behaviour. In addition, the process of evaluation was done and shown by comparing with the existing intelligent approach for network intrusion detection.

Dataset Description

The experiments for training and testing of the proposed hybrid intelligent approach for network intrusion detection is applied by using a real dataset stream named as intrusion detection dataset. These datasets contain a standard set of data to be audited and the datasets include a wide variety of intrusion types simulated in a network environment. Validating the efficiency and accuracy of the proposed hybrid technique, NSL-KDD intrusion dataset was used. It is a new version of KDD'99 dataset (Tavallaee, Bagheri, Lu, & Ghorbani, 2012, 2009). NSS-KDD dataset has some advantages over KDD'99 dataset. It has solved several inherent problems of the KDD'99 dataset and it is considered as the standard benchmark dataset for intrusion detection evaluation (Chapke Prajkta & Raut, n.d.)(Jain et al., 2011).

Dataset Pre-processing

Pre-processing of original NSL-KDD intrusion data set is an important phase to make it as an appropriate input for classification phase. The main objective of preprocessing phase is to reduce ambiguity and provide accurate information to detection engine. The preprocessing phase cleans the network data by grouping, labeling and it handles the missing or incomplete dataset. The dataset pre-processing is achieved by applying the following stages sequentially.

Transformation

There are many symbolic attributes like flag, services types and protocol types. These attributes have nominal values such as RSTOS0 and ICMP in the dataset. Under this step, some outlier data will be filtered and modified. Hence, one needs to transform these nominal values to numeric values beforehand and to make it suitable input for classification phase using SVM. In Table 1, shows the transformation of all the nominal values of dataset features into the numeric values. For instance, the flag type of "OTH" is transformed to 1, "REJ" is transformed to 2 and so on.

Table 1. Transformation Table

Type	Feature	Numeric Value
Attack or Nor-	Normal	0
	Attack	1
Protocol Type	TCP	1
	UDP	2
	ICMP	3
Flag	OTH	1
	REJ	2
	RSTO	3
	RSTOS0	4
	RSTR	5
	S0	6
	S1	7
	S2	8
	S3	9
	SF	10
	SH	11
Services	All Services	1 to 70

Feature Selection

Features selection is the most critical stage in building a hybrid intrusion detection models and is equally important to improve the efficiency of data mining algorithms. In general, the input data to classifiers is in a high dimension feature space but not all of the features are relevant to the classes to be classified. Some of the data includes irrelevant, redundant or noisy features. In this case, irrelevant and redundant features can introduce noisy data that distract the learning algorithm. It decreases the number of attributes, eliminates irrelevant, noisy or redundant features and brings about effects on applications such as speeding up a data mining algorithm, improving learning accuracy and leading to better model comprehensibility. During this step, the set of attributes or features deemed to be the most effective attributes which are extracted in order to construct suitable detection system.

The goal of features selection increases the detection rate and decreases the false alarm rate in network intrusion detection. WEKA 3.7 which is a machine learning tool has been used to compute the features selection subsets for SVM classifier to test the classification performance on each of these feature sets.

The ClassifierSebsetEvel and BestFirst algorithms have been applied to select specific features from the dataset and remove those features which are irrelevant before clustering and classification phases. All the training dataset and 10-fold cross validation are used for this purpose. A 10-fold cross validation is a technique on how to use the dataset. In this case, the dataset will be classified into 10 sub-datasets and apply the above algorithms on all the 10

sub-datasets. Table 2 and Table 3 shows the result of feature selection operation before and after transformation.

Table 2. The Original NSL-KDD Dataset Before Transformation

0, tcp, netbios_ns, S0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 96, 16, 1.00, 1.00, 0.00, 0.00, 0.17, 0.05, 0.00, 255, 2, 0.01, 0.06, 0.00, 0.00, 1.00, 1.00, 0.00, 0.00, neptune
0, tcp, http, SF, 300, 13788, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 8, 9, 0.00, 0.11, 0.00, 0.00, 1.00, 0.00, 0.22, 91, 255, 1.00, 0.00, 0.01, 0.02, 0.00, 0.00, 0.00, 0.00, normal

Table 3. The NSL-KDD Dataset After Transformation

0, 1, 1, 6, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 96, 16, 1.00, 1.00, 0.00, 0.00, 0.17, 0.05, 0.00, 255, 2, 0.01, 0.06, 0.00, 0.00, 1.00, 1.00, 0.00, 0.00, 1
0, 1, 2, 10, 300, 13788, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 8, 9, 0.00, 0.11, 0.00, 0.00, 1.00, 0.00, 0.22, 91, 255, 1.00, 0.00, 0.01, 0.02, 0.00, 0.00, 0.00, 0.00, 0

Dataset Normalization

Dataset normalization is a preprocessing type which plays an important role in classification. Normalizing the input data will help speed up the learning phase and to enhance the performance of intrusion detection system when datasets are too large. Min-Max Normalization applies in a linear transformation on the original dataset X into the specified interval. This method scales the data from (X_{min}, X_{max}) to (New_{min}, New_{max}) in proportion. The advantage of this method is that it preserves all relationships of the data values. The Min-Max in **(1)** is as follow:

(1)

$$\boldsymbol{Xnew} = \frac{(\boldsymbol{X} - \boldsymbol{Xmin})}{(\boldsymbol{Xmax} - \boldsymbol{Xmin})}$$

K-Means

K-Means is an unsupervised approach to overcomes the problem of training datasets in intrusion detection system. After an initial random assignment of a sample to K clusters, the centers of clusters are computed and the sample are assigned to the clusters with the closest centers. The process is repeated until the cluster centers do not significantly change. When the cluster assignment is fixed, the mean distance of the element to cluster centers is used as the score. A set of n vectors X_j where j = (1,…, n) are to be partitioned into C groups G_i where i = (1,...,c). The function based on the Euclidean distance between a vector X_j in group J and the corresponding cluster centre C_i can be defined in Eq. **(2)**

(2)

$$\boldsymbol{J} = \sum_{\boldsymbol{i=0}}^{\boldsymbol{c}} \boldsymbol{Ji} \sum_{\boldsymbol{i=1}}^{\boldsymbol{c}} \Big[\sum_{\boldsymbol{k,x \in Gi}}^{\boldsymbol{c}} \|\boldsymbol{Xk} - \boldsymbol{Ci}\|^{\boldsymbol{2}} \Big]$$

By applying the K-means clustering algorithm, two clusters were specified and created for each output class. As the algorithm iterates through the training data, each cluster's architecture is updated. In updating the clusters, elements are deleted from one cluster and transferred to another. The updating of clusters causes the values of the centroids to modify. This change is a reflection of the current cluster elements. When there are no changes to any cluster, the clustering of the K-Means algorithm becomes complete.

The algorithms are as follow:

1. Initialize K clusters (randomly select K elements from the data).
2. Initialize the K cluster centroids. This can be done by arbitrarily dividing all objects into K clusters, computing their centroids, and verifying that all centroids are different from each other. Alternatively, the centroids can be initialized to k arbitrarily chosen different object.
3. Iterate over all data points in the data set and compute the distances to the centroids of all clusters. Assign each data point to the cluster with the nearest centroid.
4. Recalculate "k" new centroids as per centers of the clusters resulting from the previous step.
5. Repeat step 3 until the centroids do not change any more. In Figure 2 shows the result of clustering for NSL-KDD dataset.

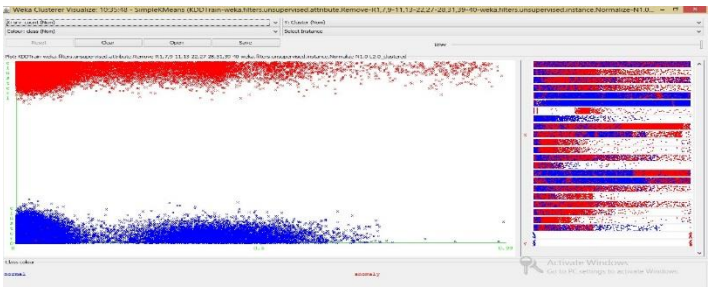

Figure 2. The Result of Clustering for NSL-KDD Dataset

Support Vector Machine

A classification based IDS will classify all the network traffic into normal or intrusion behavior and assign each attack to its specific category. The network attacks fall into four categories namely DoS, U2R, R2L and Probing. The processed data from previous phase are classified as normal or attack and are assign every attack to its type. SVM classifies data by determining a set of support vectors which are the members of the set of training inputs that outline a hyper plane in the feature space. SVMs provide a generic mechanism to fit the surface of the hyper plane to the data via the use of a kernel function. In the standard supervised learning, we are given n training samples (x_i, y_i), i = 1,2,…,n where x_i ε X denotes the input vector and yi ε Y , yi ε {+1,-1} denotes the corresponding output.

Performance Evaluation

The confusion matrix method was used to present the classification results. Each row of the matrix represents the instances in a predicted class. On the other hand, each column represents the instances in an actual class. The following factors are often use to evaluate the detection accuracy and false alarm rate of IDS in confusion matrix as shown in Table 4.

Table 4. Confusion Matrix

Actual	Predicated	
	Attack	Normal
Attack	True Positive (TP)	False Negative (FN)
Normal	False Positive (FP)	True Negative (TN)

The performance have been evaluated in terms of Accuracy (A) as in Eq.**(3)**. In Eq. **(3)** indicates the total number of connections that are correctly classified including normal and intrusive connections. Detection Rate (DR) as in Eq. **(4)** is the amount of attack detected when it is actually attack over the amount of attack sample and false alarm rate. False Alarm Rate (FAR) in Eq. **(5)** which is the amount of attack detected when it is actually normal over the amount of normal sample.

$$A = (TP+TN) / (TP+TN+FP+FN) \quad (3)$$

$$DR = (TP) / (TP+FP) \quad (4)$$

$$FAR = (FP) / (FP+TN) \quad (5)$$

RESULTS AND DISCUSSION

The proposed technique detect anomaly activities with significant improvement in terms of high detection rate and low false positive rate. It has achieved 96.26 percentage in detection rate and 3.7 percentage as a false alarm rate. The proposed technique has detected 95.76 percentage as attack from 71,463 real attack connection records. While, the other 4.23 percentage as normal. Nevertheless, the full number of normal connections of records in the NSL-KDD dataset which is 75,984 have been classified as 96.28 percentage as normal and 3.71 percentage of the connection as an attack.

Table 5.Table 5 shows the confusion matrix which has been obtained from the classification of the proposed hybrid machine learning technique using the full NSL-KDD intrusion dataset.

Table 5. Confusion Matrix Result

Actual	Predicated	
	Attack	Normal
Attack	95.766% (TP)	4.237% (FP)
Normal	3.715% (FN)	96.284% (TN)

The details of detection for the proposed technique have shown that the higher the detection for DoS, R2Land Probing attacks. In spite of the highly assigning rate for last three categories, it shows a less rate in U2R attack detection. In Figure 3, shows the detection rate for every category of attack as well as the normal network behavior.

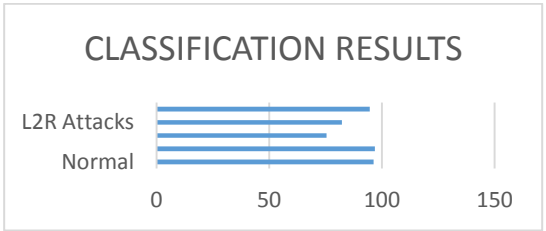

Figure 3. Detection Rate for Attack Categories

The details of detection for the proposed technique have shown that, the higher the detection for DoS, R2Land Probing attacks. In spite of the highly assigning rate for last three categories, it shows a less rate in U2R attack detection. In Figure 4 below shows the detection rate for every category of attack as well as the normal network behavior.

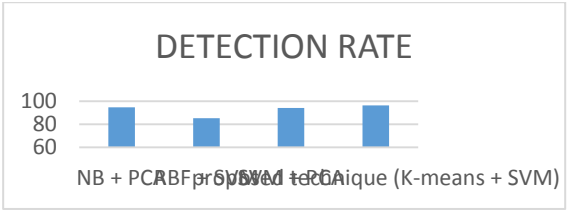

Figure 4. Detection Rate for Attack Categories

CONCLUSION

Network security has recently become a domain of great interest in the scientific, academic and industrial arenas alike. The impact of a successful attack on an institution can have disastrous consequences. Due to the increasing incidents of network attacks have heightened concerns for network security and we have proposed the hybrid intelligent technique.

The proposed hybrid intelligent approach for network intrusion detection has managed to address the existing intrusion detection approaches such as accuracy and false detection rate. The proposed approach is done by integrating two machine techniques namely K-Means clustering and SVM classifier for intrusion detection. The result indicates an encouraging approach.

ACKNOWLEDGMENTS

The authors would like to express our gratitude to the Ministry of Education (MoE), Malaysia under FRGS 2014-2 grant, UUM Research & Innovation Management Center (RIMC), Universiti Utara Malaysia (UUM) and to the School of Computing (SoC), UUM.

REFERENCES

Albers, P., Camp, O., Percher, J. M., Jouga, B., Mé, L., & Puttini, R. (2002). Security in ad hoc networks: A general intrusion detection architecture enhancing trust based approaches. In *Proceedings of the First International Workshop on Wireless Information Systems (WIS-2002)*, 1–12.

Anantvalee, T., & Wu, J. (2007). A survey on intrusion detection in mobile ad hoc networks. *Wireless Network Security*, 159–180.

Brutch, P., & Ko, C. (2003). Challenges in intrusion detection for wireless ad-hoc networks. In *Proceedings of the Symposium on Applications and the Internet Workshops*, 368–373.

Chapke Prajkta, P., & Raut, A. B. (n.d.). Hybrid Model For Intrusion Detection System.

Farhan, A. F., Zulkhairi, D., & Hatim, M. T. (2008). Mobile agent intrusion detection system for mobile ad hoc networks: A non-overlapping zone approach. In *4th IEEE/IFIP International Conference on Internet, 2008. ICI 2008*, 1–5.

Jain, A., Sharma, S., & Sisodia, M. S. (2011). Network Intrusion Detection by Using Supervised and Unsupervised Machine Learning Techniques: A Survey. *International Journal of Computer Technology and Electronics Engineering*, *1*.

Jaisankar, N., & Kannan, A. (2011). A Hybrid Intelligent Agent Based Intrusion Detection System. *Journal of Computational Information Systems*, *7*(8), 2608–2615.

Joshi, S. A., & Pimprale, V. S. (2013). Network Intrusion Detection System (NIDS) based on Data Mining. *International Journal of Engineering Science and Innovative Technology (IJESIT)*, *2*.

Mohammad, M. N., Sulaiman, N., & Khalaf, E. T. (2011). A novel local network intrusion detection system based on support vector machine. *Journal of Computer Science*, *7*(10), 1560.

Neethu, B. (2012). Classification of intrusion detection dataset using machine learning approaches. *International Journal of Electronics and Computer Science Engineering*, 1044–1051.

Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2012). Nsl-kdd dataset. *Http://www. Iscx. ca/NSL-KDD*.

Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A.-A. (2009). A detailed analysis of the KDD CUP 99 data set. In *Proceedings of the Second IEEE Symposium on Computational Intelligence for Security and Defence Applications 2009*.

Upadhyaya, D., & Jain, S. (2013). Hybrid Approach for Network Intrusion Detection System Using K-Medoid Clustering and Na{ï}ve Bayes Classification. *International Journal of Computer Science Issues (IJCSI)*, *10*(3).

Wankhade, K., Patka, S., & Thool, R. (2013). An Overview of Intrusion Detection Based on Data Mining Techniques. In *International Conference on Communication Systems and Network Technologies (CSNT)*, 626–629.