A Novel Combined Method for Network Intrusion Detection Systems Aimed at Detecting Novel Attacks

Mohammad Mehdi Masoumi
M.Sc. Student
Shiraz University of Technology

Marzieh Ahmadzadeh
Assistant Professor Shiraz University of Technology

Reza Javidan
Assistant Professor Shiraz University of Technology

ABSTRACT
Intrusion Detection Systems are important tools in computer networks security. To date, many practical methods have been proposed using data mining techniques, however, presence of novel is not considered in most of the proposed method. As the presence of novel attacks in the real world is unavoidable, proposing methods that consider novel attacks is crucial in this area of research. In this paper, a combined method has been presented for Network Intrusion Detection Systems using K-NN and K-Means clustering algorithm. A threshold has been used for detection of novel attacks. The proposed method is superior to a hybrid method in the literature that does not consider novel attacks, in which K-means clustering algorithm and K-Nearest Neighbor(K-NN) algorithm have been combined, in terms of accuracy, detection rate, and false alarm rate.

Keywords
Network Intrusion Detection, Hybrid Learning, Network Security, Data Mining

1. INTRODUCTION
Computer networks are vulnerable to security violation from inside and outside intruders. A Network Intrusion Detection System (NIDS) is a system that aimed at detecting suspicious activities in a network, in the second line of defense [1]. Actually, NIDSs play a vital role in providing a secure network environment. The first major challenge in designing an effective IDS is detecting suspicious activities as accurately as possible [2]. Therefore, researchers are trying to employ data mining techniques in this area of research to differentiate between suspicious activities and normal activities [3].

Distance-based data mining techniques such as K-Nearest Neighbors and K-Means clustering algorithm, have been used widely in the area of IDSs [4]. The simple assumption of distance-based techniques is that suspicious behaviors are far enough from normal behaviors that can be differentiated from normal behaviors [4]. In other words, discerning of suspicious behaviors is based on the distance of normal and anomalous behaviors.

Considering the methods of differentiating between normal and suspicious behaviors, NIDSs can be categorized into three categories, namely signature-based NIDS, anomaly-based NIDS, and hybrid NIDS [2, 5]. However, some of the previous works do not count hybrid methods as the third category, they just categorize NIDSs into two categories [1, 6, 7]. One of the major goals of this paper is providing a combined method and take advantage of the potential characteristics of combined methods, it is crucial to know the characteristics of combined NIDSs and consider hybrid NIDSs as a distinct category.

Signature-based NIDSs have the potential ability of detecting attacks with high detection rate and low false alarm rate, on the other hand these methods are not able to detect novel attacks or zero-days attacks. Novel attacks are previously unseen attacks, which are unavoidable in a real network environment, since, network environments are inherently dynamic environments and it is impossible to find the patterns of all attacks in designing phase [5]. Furthermore, with the tremendous growth of the Internet, networks are accessible for outside intruders, this makes detection of novel attacks a non-trivial issue. In comparison with signature-based NIDSs, anomaly-based NIDSs have the ability of detecting novel attacks, however their detection rate is relatively low, and their false alarm rate is relatively high[8].

To circumvent the drawbacks of signature-based NIDSs and anomaly-based-NIDSs, hybrid NIDSs have been employed in literature [9, 10]. In other words, hybrid NIDSs are trying to obtain high detection rate and low false alarm rate and detect novel attacks as well. However, there are many research papers that combine different data mining techniques as a hybrid method in order to improve detection rate and false alarm rate and do not take novel attacks as an issue [11, 12]. As detection of novel attacks is a major part of the proposed method, this research is categorized as a hybrid NIDS.

The remainder of the paper is organized as follows. Section 2 presents existing related works in the area of hybrid methods for network intrusion detection and also describes the contribution of this paper. Section 3 presents the proposed method, which has two general steps, training and testing. Section 4 explains the data that has been used for the evaluation of the proposed method. Experimental design and performance evaluation metrics are presented in section 5. The results of the simulation are presented in Section 6. Finally, Section 7 concludes the work and describes the system potentialities and future works.

2. RELATED WORKS
Hybrid IDSs have multiple goals. The first goal and the most obvious goal of hybrid approaches is to use potential advantages of various algorithms to detect suspicious behaviors as accurately as possible [11, 13-15]. Many researchers have combined supervised and unsupervised algorithms to detect attacks with high detection rate and keep false alarm rate low.

K-Means clustering algorithm is an algorithm that partitions data into K user defined clusters. The idea behind K-Means algorithm is to cluster similar data points in the same cluster. With the idea of clustering similar data in the same clusters

and predicting normal and suspicious activities subsequently. K-means clustering algorithm has been used in hybrid methods in combination with predictive algorithms. In [13-16], researchers have combined K-Means clustering algorithm with other predictive algorithms such as Naïve Bayes and OneR classification. Evaluating the results of the proposed methods show that clustering similar data in the same clusters can improve the detection rate and accuracy of NIDS effectively in comparison with single classifiers. In fact, the idea behind all these research papers is almost the same, however, different predictive algorithms have been used, and also performance evaluation methods are slightly different.

Using the same idea, for the improvement of IDSs in terms detection rate and false alarm rate, ID3 algorithms is employed for classification of clustered data, but a distinct model is constructed for each cluster using ID3 algorithm [17]. In a similar way, K-Means clustering algorithm is employed to cluster the data and predict the attacks with multiple classifiers subsequently [18]. Data points in each cluster are classified by a distinct classifier in order to take the potential advantage of each classifier in data classification.

In [10], the authors have shown that unsupervised algorithms have lower detection rate, accuracy and higher false alarm rate in comparison with supervised algorithms, on the other hand, unsupervised algorithms have the potential ability of detecting novel attacks. To take the advantage of the potential abilities of unsupervised algorithms in novel attacks detection and obtaining high detection rate, accuracy and low false alarm rate, researchers combine supervised and unsupervised algorithms as hybrid methods [11]. Although it is important to obtain high detection rate, accuracy and low false rate, it is important to take novel attacks into consideration. Since, in the real world and network environments novel attacks are unavoidable. Actually, many researchers are trying to use hybrid approaches in order to obtain high detection rate, accuracy, low false alarm rate and detect novel attacks as well. Detecting novel attacks is an important issue because the real network environments consist unseen attacks as well as previously seen attacks.

With the aim of detecting novel attacks, in [11] the authors proposed a hybrid method with combination of K-Means clustering algorithm and Random Forest. In the proposed method, the authors used Random Forest for the detection of known attacks and K-Means clustering algorithm for the detection of unknown attacks. In an almost similar manner, in [19], the researchers used Random Forest for the detection of known and unknown attacks. In the proposed method, the data points that have significant are considered as outliers.

Researchers in the area of network IDS are trying to improve the detection rate and accuracy of IDSs as effectively as they can. Using the same idea that is presented in [9], this paper tries to find novel attacks, in addition to improvement of performance evaluation metrics. In [9], the proposed method does the prediction with 1-dimensional data (plus class variable). As mentioned in [9], the primary purpose is to present a feature that would be a good representative feature and classification can be done based on the representative feature. In this paper, the same idea has been used to make a representative feature, also, the idea of nearest and farthest neighbors has been presented for novel attack detection.

The most primary distinction of this paper and related works is in using of farthest nearest neighbor. To our knowledge, to date, the idea of farthest neighbor has not been used in the area of IDS. The novelty of the presented idea is that in addition to nearest neighbor, farthest neighbor can be employed to contribute to better prediction of data, which is also the main distinction between the proposed method and the method presented in [9] and other related works.

2.1 Contribution to network IDS

The aim of this paper is twofold. The first is to present a hybrid intrusion detection method with combining of K-Means clustering algorithm and K-Nearest Neighbors in order to improve the performance of IDSs in terms of detection rate, accuracy and false alarm rate. The second is to detect previously unseen attacks using the theory of IDSs and the concept of farthest and nearest neighbor. In other words, the proposed method tries to provide high accuracy and detection rate as well as low false alarm rate. It also considers novel attack as an inevitable challenge in the real world and tries to detect novel attacks.

3. THE PROPOSED METHOD

Intuitively, the simple idea behind the proposed method is considering the nearest neighbor and farthest neighbor of each test data point. In other words, if a test data point is a normal data, the closest data point to the test data in the train set has to be a normal data. Since, in theory, normal activities have some characteristics and close enough to normal activities. That is why algorithms such as K-NN are applicable in the area of IDS. On the other hand, the farthest data point to a normal activity has to be an attack data point. Since, in the theory of anomaly detection techniques, attack data points deviate significantly from normal activities, enough to be detectable [1, 2].

Using the above-mentioned theory, in the proposed method, the idea of nearest and farthest neighbors has been used in order to detect novel attacks. If the closest data point to a test data point is a normal data point, the farthest data point has to be an attack, as discussed earlier. If the farthest data point would be a normal data point and it is far enough from the test point, this could be considered as a novel attack and a mis-prediction.

In addition to the idea of farthest and nearest neighbors, similar to CANN algorithm, in the proposed method n-dimensional data set is transformed into 1-dimentional data set. As mentioned in CANN algorithm [9], the goals of transforming data set into 1-dimentional data set are computation efficiency and representative feature. Actually, representative feature means that the action of intrusion detection can be done by the value of one feature. As a result, CANN algorithm uses 1-dimensional data to differentiate between attacks and normal data. However, as discussed earlier, the proposed method considers novel attacks, which CANN algorithm does not pay attention to. The presence of novel attacks is inevitable in the real world.

3.1 Training phase of the proposed algorithm

The proposed methods spits the data into 5 clusters because the dataset contains 5 different activities, namely DoS, U2R, R2L, probe, and normal activities. Also, in the literature 5 clusters has been used widely, because of the same reason [13, 14, 16, 17].

The steps of the training phase of the proposed algorithm are as follows:

1. Split the train set into 5 distinct clusters using K-Means clustering algorithm.
2. Find the nearest neighbor of each data point in the cluster that the data point is belonging to it.
3. Make the representative feature: Add up the distance between each data point to 5 cluster centroids and the distance between the data point and its closest neighbor within the cluster.

In sum, up to this stage, the training data have been clustered and the representative feature for the training data has been created.

3.2 Testing Phase of the Proposed Algorithm

The main difference between the proposed algorithm and CANN is in the test phase. This phase can be considered as online phase and novel attacks are detected based on nearest, farthest neighbors and a predefined threshold. The steps of the test phase of the proposed algorithm are as follows. These steps are executed for each test point in the test set.

For each test point:

1. Find the cluster of the test point, based on the cluster centroids in the training phase.
2. Make the representative feature for each test point: Add up the distance between the test point to 5 cluster centroids and the distance between the test point and its closest neighbor.
3. Classify the test point based on its closest neighbor

3.1. If the test point is classified as a normal data, the test point can be a novel attack, find the farthest neighbor of the test point.

3.1.1. If the farthest data point to the test point is a normal data (the farthest data point has to be an attack data point, because, in theory, attack data points deviate significantly from normal data, so they are differentiable [1, 2]) and the distance of the farthest data point to the test data point is greater than a predefined threshold, classify the data point as an attack. Else, classify the data point as a normal data point.

In the first step of the proposed combined method, the training phase the train set is clustered using K-Means clustering algorithm. Subsequently, in the testing phase, the distance of each data point is calculated with all K cluster centroids and K nearest neighbors (Using K-Nearest Neighbor algorithm).

The proposed method is analogous to the hybrid method that has been proposed in [9], however, the major differences between the proposed algorithm in this paper with CANN algorithm are considering of novel attacks and farthest and nearest neighbors.

It is worth noting that the proposed methods uses K-Means clustering algorithm and nearest neighbor to make the representative feature. Afterwards, using nearest neighbor (K-NN) and farther neighbor the task of prediction is done.

4. DATA DESCRIPTION

There are two popular data sets in the area of NIDS, namely KDDcup99 and NSL-KDD [20]. Most of the researchers use KDDcup99 as a benchmark to test the performance and efficiency of their methods. However, in [20] it is proved that KDDcup99 data set has some inherent problems such as redundancy and duplicate records. The most tangible difference between KDDcup99 and NSL-KDD is duplicate records. NSL-KDD does not have any duplicate records, which is consistent with novel attack detection that is the major goal of this research paper. Also, the testing set in NSL-KDD data set consists novel attacks that are not exist in the training set.

In NSL-KDD data set each record has 41 features plus a class label. The class labels can be categorized into 5 classes: normal, Denial of Service (DoS), Unauthorized Access from a Remote Machine (R2L), User to Root (U2R) and probing. More details of NSL-KDD data set and number of novel attacks is available in [20].

5. EXPERIMENTAL DESIGN

The proposed algorithm is compared with CANN algorithm. The proposed and CANN algorithm are executed 10 times on the same data with different seeds for the random number generator, which means that the training set and the testing set had been changed in each repetition. In each repetition of the algorithms 30000 records of the data have been chosen for the training set and 10000 of the data for the testing set. As Euclidean distance metric [4, 21] is used as the distance metric in the proposed algorithm and CANN, the data set has been normalized based on Min-Max normalization method [22].

From the 41 features of the NSL-KDD data 13 features are used in the experimental design [23]. The other features have been eliminated, since, they do not have any useful information and are redundant features.

As mentioned earlier, the number of clusters for K-Means clustering algorithm is 5. This is because the data set contains 4 categories of attacks and normal activities [13-15]. The value of the threshold of the proposed algorithm is 5.5, based on experimental results in the training phase, 5.5 provides promising results, therefore, 5.5 has been used as the value of the threshold.

5.1 Performance Evaluation Metrics

The performance evaluation metrics have been described in this section. There are three measurements metrics which have been used for calculating the efficiency of algorithms in this paper:

$$\text{Accuracy} = \frac{(TP+TN)}{(TP+TN+FP+FN)} \quad (1)$$

$$\text{Detection Rate} = \frac{(TP)}{(TP+FP)} \quad (2)$$

$$\text{False Alarm Rate} = \frac{(FP)}{(FP+TN)} \quad (3)$$

- True positive (TP): Number of samples which are correctly classified as attacks.
- True negative (TN): Number of normal samples that are correctly classified as normal.
- False positive (FP): Number of normal samples which are incorrectly classified as attacks.
- False negative (FN): Number of samples that are incorrectly classified as attacks.

To report the performance of the proposed method and CANN algorithm in terms of detection rate, accuracy and false alarm rate as a single number, the performance metrics are presented using 90% confidence interval[24].

6. RESULTS

The accuracy of the proposed algorithm and CANN algorithm are shown in Fig.1. As it is shown in Fig.1, the accuracy of the proposed algorithm in all repetitions is superior to the accuracy of CANN algorithm. The accuracy of the proposed algorithm with 90% is between 97.19% and 98.37% and the accuracy of CANN algorithm with 90% is between 95.24% and 97.00%. This means that the accuracy of the proposed method is significant and superior to CANN algorithm with.

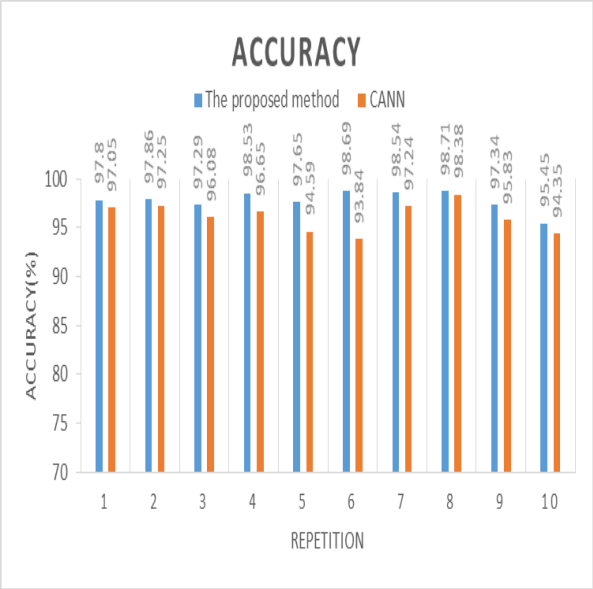

Fig.1: The accuracy of the proposed algorithm and CANN algorithm in ten repetitions.

The detection rate of the proposed algorithm and CANN algorithm for ten repetition are shown in Fig.1. Based on the equation of detection rate, the proposed algorithm performs better in the detection of attacks. The detection rate of the combined proposed algorithm with 90% confidence interval is between 96.91% and 98.21%, on the other hand, the detection rate of CANN algorithm is between 94.83% and 96.62%, which means that the difference between the detection rate of the proposed algorithm and CANN algorithm is significant.

Finally, the false alarm rate of the proposed method with 90% confidence interval is between 2.45% and 4.00%. The false alarm rate of CANN algorithm is between 3.99% and 6.64%.

Fig.2: The detection rate of the proposed algorithm and CANN algorithm in ten repetitions.

7. CONCLUSIONS AND FUTURE WORKS

In this paper, a new hybrid method has been proposed for NIDSs. The main advantages of the proposed method in comparison with other methods is twofold. Firstly, in the proposed method a new hybrid method has been presented with the employment of farthest neighbor and nearest neighbor. Secondly, the proposed method has taken novel attacks into consideration and a threshold has been defined for the detection of novel attacks.

The experimental results show that the proposed method is superior to CANN algorithm in terms of accuracy, detection rate, and false alarm rate. It means that the proposed method can detect attacks more effectively and raise less false alarms.

Finally, for the future works, other feature selection methods can be considered for the improvement of performance evaluation metrics. Also, other distance metrics can be used for better nearest and farthest neighbors query.

8. REFERENCES

[1] B. Morin and L. Mé, "Intrusion detection and virology: an analysis of differences, similarities and complementariness," Journal in computer virology, vol. 3, pp. 39-49, 2007.

[2] A. Patcha and J.-M. Park, "An overview of anomaly detection techniques: Existing solutions and latest technological trends," Computer networks, vol. 51, pp. 3448-3470, 2007.

[3] S. V. Farrahi, M. K. Sarvestani, and M. Ahmadzadeh, "A Novel Supervised Algorithm for Network Intrusion Detection with the Ability of Zero-day Attacks Identification," International Journal of Computer Applications, vol. 121, 2015.

[4] D. J. Weller-Fahy, B. J. Borghetti, and A. A. Sodemann, "A survey of distance and similarity measures used within network intrusion anomaly detection," Communications Surveys & Tutorials, IEEE, vol. 17, pp. 70-91, 2015.

[5] S. Agrawal and J. Agrawal, "Survey on Anomaly Detection using Data Mining Techniques," Procedia Computer Science, vol. 60, pp. 708-713, 2015.

[6] P. Garcia-Teodoro, J. Diaz-Verdejo, G. Maciá-Fernández, and E. Vázquez, "Anomaly-based network intrusion detection: Techniques, systems and challenges," computers & security, vol. 28, pp. 18-28, 2009.

[7] E. Biermann, E. Cloete, and L. M. Venter, "A comparison of intrusion detection systems," Computers & Security, vol. 20, pp. 676-683, 2001.

[8] M. Ahmed, A. N. Mahmood, and J. Hu, "A survey of network anomaly detection techniques," Journal of Network and Computer Applications, vol. 60, pp. 19-31, 2016.

[9] W.-C. Lin, S.-W. Ke, and C.-F. Tsai, "CANN: An intrusion detection system based on combining cluster centers and nearest neighbors," Knowledge-based systems, vol. 78, pp. 13-21, 2015.

[10] P. Laskov, P. Düssel, C. Schäfer, and K. Rieck, "Learning intrusion detection: supervised or unsupervised?," in Image Analysis and Processing–ICIAP 2005, ed: Springer, 2005, pp. 50-57.

[11] R. M. Elbasiony, E. A. Sallam, T. E. Eltobely, and M. M. Fahmy, "A hybrid network intrusion detection framework based on random forests and weighted k-means," Ain Shams Engineering Journal, vol. 4, pp. 753-762, 2013.

[12] F. Kuang, W. Xu, and S. Zhang, "A novel hybrid KPCA and SVM with GA model for intrusion detection," Applied Soft Computing, vol. 18, pp. 178-184, 2014.

[13] Z. Muda, W. Yassin, M. Sulaiman, and N. I. Udzir, "A K-Means and Naive Bayes learning approach for better intrusion detection," Information technology journal, vol. 10, pp. 648-655, 2011.

[14] Z. Muda, W. Yassin, M. Sulaiman, and N. Udzir, "Intrusion detection based on K-Means clustering and Naïve Bayes classification," in Information Technology in Asia (CITA 11), 2011 7th International Conference on, 2011, pp. 1-6.

[15] S. K. Sharma, P. Pandey, S. K. Tiwari, and M. S. Sisodia, "An improved network intrusion detection technique based on k-means clustering via Naïve bayes classification," in Advances in Engineering, Science and Management (ICAESM), 2012 International Conference on, 2012, pp. 417-422.

[16] Z. Muda, W. Yassin, M. N. Sulaiman, and N. I. Udzir, "Intrusion detection based on k-means clustering and OneR classification," in Information Assurance and Security (IAS), 2011 7th International Conference on, 2011, pp. 192-197.

[17] Y. Yasami and S. P. Mozaffari, "A novel unsupervised classification approach for network anomaly detection by k-Means clustering and ID3 decision tree learning methods," The Journal of Supercomputing, vol. 53, pp. 231-245, 2010.

[18] S. V. Farrahi and M. Ahmadzadeh, "KCMC: A Hybrid Learning Approach for Network Intrusion Detection using K-means Clustering and Multiple Classifiers," International Journal of Computer Applications, vol. 124, 2015.

[19] J. Zhang and M. Zulkernine, "A hybrid network intrusion detection technique using random forests," in Availability, Reliability and Security, 2006. ARES 2006. The First International Conference on, 2006, p. 8 pp.

[20] M. Tavallaee, E. Bagheri, W. Lu, and A.-A. Ghorbani, "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, 2009.

[21] H. NASOOTI, M. AHMADZADEH, M. KESHTGARY, and S. VAHID, "The Impact of Distance Metrics on K-means Clustering Algorithm Using in Network Intrusion Detection Data."

[22] G. W. Milligan and M. C. Cooper, "A study of standardization of variables in cluster analysis," Journal of classification, vol. 5, pp. 181-204, 1988.

[23] V. Rampure and A. Tiwari, "A Rough Set Based Feature Selection on KDD CUP 99 Data Set," International Journal of Database Theory and Application, vol. 8, pp. 149-156, 2015.

[24] R. Jain, The art of computer systems performance analysis: John Wiley & Sons, 2008.