A Novel Supervised Algorithm for Network Intrusion Detection with the Ability of Zero-day Attacks Identification

S. Vahid Farrahi
M.Sc student
Shiraz University of Technology
Shiraz, Iran

Mahsa Kamali Sarvestani
M.Sc student
Shiraz University of Technology
Shiraz, Iran

Marzieh Ahmadzadeh
Assistant Professor
Shiraz University of Technology
Shiraz, Iran

ABSTRACT
In this paper, a new algorithm has been proposed for network intrusion detection. The proposed algorithm operates in a simple but efficient manner. It uses labeled data in the training phase, which means that our algorithm is a supervised algorithm. In the training phase of the algorithm, the data are categorized based on their class label values. Then, the algorithm compute a center point for each category of the class label. A center point is a mean of all samples that belong to the same category. Finally, in the testing phase, the algorithm uses Euclidean distance metric to label the test data based on their distances to the center points. In other words, each test data assigns to the nearest center point. However, a pre-defined threshold has been used in the testing phase in order to deal with zero-day attacks. If a test data point is closer to the normal center it will be assign to the normal class but in this case the algorithm checks the pre-defined threshold. If the distance to the normal center was greater than the pre-defined threshold the test data point will be classify as an attack, else it will be assign to the normal class. Experimental results show that the proposed algorithm is superior to single Naïve Bayes classifier. The detection rate of the proposed algorithm with 95% confidence is between 95.88 ± 0.11 and the detection rate of Naïve Bayes algorithm with the same confidence is between 90.03 ± 0.31.

Keywords
Data Mining, Network Intrusion Detection, Zero-day Attacks Identifying, Supervised Learning, Anomaly Detection

1. INTRODUCTION
Nowadays by developing of the Internet, the data are more reachable and accessible for unauthorized entities. Accordingly, information security is necessary to be maintained in three parts namely privacy, integrity, and availability. Security mechanisms can be defined in a two level structure [1, 2]. The first level uses security mechanisms such as access control, identification, and cryptology. Intrusion detection systems (IDS) and antivirus tools stay in the second level of defense [1].

Formally, IDSs can be divided two main categories considering the method that they analyze the input data [3]: Anomaly-based Intrusion Detection Systems (AIDS) and Signature-Based Intrusion Detection Systems (SIDS).

The main difference between these two methods is in the definition of attacks and anomalies. In an AIDS, the main issue is about the definition of normal profile for the normal network traffics. On the other hand, a SIDS looks for the sequence of operations and events that cause an attack, called attack patterns [4]. A SIDS keeps the attack patterns in the signature-base in order to use them for intrusion detection.

Generally, statistical methods and clustering techniques are used in AIDS. AIDS have less accuracy than SIDS but they have the ability to identify "zero-day" attacks [5]. SIDS generally use classification algorithms and rule based classifiers. SIDS are more accurate than AIDS because they have the patterns of well-known attacks in the signature-base. On the other hand, they are not able to detect zero-day attacks [5].

The paper is amid to propose a supervised algorithm for network intrusion detection systems in order to achieve higher accuracy and also keep the ability of detecting new attack in the proposed algorithm. Although the proposed algorithm is a supervised algorithm, it has the ability of detecting new attacks.

The remainder of this paper organized as follows: Section 2 presents related works .Section 3 explains the goals of this paper based on the experimental design in supervised and unsupervised algorithms .Section 4 presents the proposed algorithm. Section 5 describes the dataset that has been used in our experiments. Section 6 explains the experimental design for the evaluation of our proposed algorithm. Finally, section 7 presents the results and section 8 concludes the paper and explains the future works.

2. RELATED WORKS
In [6] the authors reduced the number of input features in order to propose an efficient and effective IDS. They reduced the features using four different feature selection methods and used Naïve Bayes classification algorithm as the classifier to evaluate the results.

In [7] the authors evaluated the effect of different feature selection methods on decision tree using in network intrusion detection data.

In [8] some experiments had been done in order to evaluate the performance of Naïve Bayes algorithm with decision tree. The experimental results show that Naïve Bayes provides very competitive results with decision tree. Also [9] compared Naïve Bayes algorithm with two decision tree algorithms.

In [10] authors compared supervised and unsupervised algorithm for network intrusion detection. The problem of using supervised algorithm in network intrusion detection is that the performance of the supervised algorithms degrade when the data contain unknown attacks. On the other hand, the performance of unsupervised algorithms do not change

significantly in the presence of unknown attacks in the data [10].

Previous works that had been reviewed in this section used supervised algorithm and tried to achieve higher performance with their idea in the preprocessing step. Therefore, they achieved higher performance metrics but they did not consider the issue of unknown attacks. Obviously, in the real world new attacks will happen. An efficient IDS must has the ability to detect the new attacks.

This paper, tries to use labeled data in the training phase in order to achieve higher performance and consider the issue of detecting unknown attacks using a pre-defined threshold.

3. GOAL STATEMENT

Experimental results in [10] prove that supervised algorithms perform more accurately in network intrusion detection systems in detecting known attacks than unsupervised algorithms but the accuracy of the supervised algorithms degrade significantly, when unknown attacks are available in the test set. On the other hand, the accuracy of unsupervised algorithms do not degrade significantly in the presence of unknown attacks [10]. The authors concluded that the problem of IDS in detecting unknown attacks and keeping its performance at high simultaneously could not be solved by purely supervised or unsupervised algorithm [10].

To solve this problem a new supervised distance-based algorithm has been proposed in this paper. The idea behind of our proposed algorithm is based on K-means clustering algorithm. K-means is an unsupervised distance-based clustering algorithm [11] that has been used widely in many data mining applications as well as network intrusion detection [12].

In the proposed algorithm, K-means clustering algorithm is modified to a distance-based supervised algorithm. In other words, the proposed algorithm works with labeled data in the training phase. Although the proposed algorithm is a supervised algorithm but it still has the ability of detecting unknown attacks if they would be available in the test set.

Therefore, the main goal of this paper is to propose a supervised algorithm for network intrusion detection systems in order to achieve higher accuracy and detection rate (by using labeled data in the training phase of the algorithm) and keep the ability of zero-day attack identification in the proposed algorithm, simultaneously.

4. THE PROPOSED SUPERVISED ALGORITHM

In the following section, the proposed algorithm is described. The proposed algorithm has two phases, the training phase and testing phase.

4.1 Training Phase of the Proposed Algorithm

In the training phase, the data are categorized based on their class label values. Consider that n is the number of records in the dataset and d is the dimensionality of the records. Accordingly, m is the number of data that have been selected for the training set. The training set have c distinct class values where n_j is the number of records that belong to the j^{th} class value in the training set and s_{ij} is the i^{th} attribute value of record s in the training set with class label j .

The steps of proposed algorithm during the training phase have been shown in the following two steps:

Step (1): categorize the m records in the training set based on their class values into c categories (distinct number of the class labels).

Step (2): Make a center point for each category of the value of the class labels. The center point P_j is the average of all samples, which belong to category c_j. Formally:

$$P_j = \frac{1}{n_j}\sum_{j=1}^{n_c} s_{ij} \quad \text{for i} = 1,2,\ldots,\text{d} \qquad (1)$$

4.2 Testing Phase of the Proposed Algorithm

The proposed algorithm uses Euclidean distance metric to label the test data based on their distances to the center points. When a new network traffic data receives, the algorithm operates as follows to label the new data as normal or anomaly:

Step (1): Compute the distances between new data and all center points with Euclidean distance metric.

Step (2-a): Assign the data to the closest center point.

Step (2-b): If the data is closer to the normal center point and the distance between the new data and normal center point is greater than a predefined threshold, classify it as an attack data instead of normal.

The proposed algorithm is simple but efficient since, it considered the presence of new attacks in data. In fact, in real world new attack are available in the data. Therefore, the most important advantage of the proposed algorithm in comparison of previous works is the detection of new attacks through a simple method.

5. DATA DESCRIPTION

The dataset that has been used in our experiments is NSL-KDD labeled dataset [13]. NSL-KDD dataset has been produced based on KDD cup99 which is benchmark in network intrusion detection. NSL-KDD dataset suggested for solving some of the inherent problems of the KDD cup99 dataset. The dataset contains 25,192 records labeled as anomaly or normal.

One of the advantage of NSL-KDD over KDD cup99 is that it does not contain of redundant records that may cause the biased results of classifiers towards more frequent records [13].

Captions should be Times New Roman 9-point bold. They should be numbered (e.g., “Table 1” or “Figure 2”), please note that the word for Table and Figure are spelled out. Figure’s captions should be centered beneath the image or picture, and Table captions should be centered above the table.

6. EXPERIMENTAL DESIGN

The proposed algorithm has been compared with Naïve Bayes (NB) classification algorithm. The proposed algorithm is 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 [14]. In addition, Naïve Bayes algorithm has been executed 10 times using the same dataset with different seeds of the random number generator. In each repetition of the algorithms, 70% of the data have been chosen for the training set and 30% of the data for the testing set. Since, Euclidean distance metric [11] was used as the distance metric in the

proposed algorithm, it is necessary to normalize the dataset. Therefore, Min-Max normalization method was used for data normalization [15]. Finally, the value of the threshold for the proposed algorithm is 6. It means that if the distance between a test data is closer to the normal center point than the anomaly center point but the distance is greater than 6, the data will be label as an anomaly instead of normal.

6.1 Performance Evaluation Metrics

The performance metrics that have been used for the evaluation of the proposed algorithm with Naïve Bayes classifier are as following:

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

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

- True positive (TP): The number of attacks that are correctly classified as intrusions.
- True negative (TN): The number of normal data that are correctly classified as normal.
- False positive (FP): The number of normal data that are incorrectly classified as attacks.
- False negative (FN): The number of attacks that are incorrectly classified as normal.

7. RESULTS

The detection rates of the proposed algorithm and Naïve Bayes algorithm, which are obtained from each repetition, are shown in Table1. The proposed algorithm performs better in term of detection rate in all of the repetitions. The detection rates of the proposed algorithm is compared to Naïve Bayes algorithm in each repetition and are shown have been shown Fig. 1. As, it is shown in Fig. 1 the detection rate of the proposed algorithm is superior to Naïve Bayes algorithm in all of the repetitions. Considering the detection rate equation it means that, the proposed algorithm is able to detect more attacks than Naïve Bayes classifier. So, it is stated with 95% confidence that the detection rate of the proposed algorithm is between 95.88 ± 0.11 and the detection rate of Naïve Bayes algorithm with 95% confidence is between 90.03 ± 0.31. In other words, the proposed algorithm is significantly superior to Naïve Bayes classifier in term of detection rate.

Additionally, the proposed algorithm and Naïve Bayes have been evaluated in term of false alarm rate. The false alarm rate of the proposed algorithm and Naïve Bayes algorithm are shown in Table1. As it is shown in Table 1, the false alarm rate of the proposed algorithm is better than Naïve Bayes algorithm in all of the repetitions, which means that the proposed algorithm raises less false alarms in comparison of Naïve Bayes. The false alarm rate of the proposed algorithm with 95% confidence is between 3.04 ± 0.08 and the false alarm rate of Naïve Bayes with the same confidence is between 8.51 ± 0.34. In addition, false alarm rate performance metric indicate that the proposed algorithm is significantly better than Naïve Bayes algorithm. Therefore, the proposed algorithm detects more attacks than Naïve Bayes classifier and also reduce the false alarm an IDS raises.

Table 1. The Detection Rates (DR) and False Alarm Rates (FAR) of the proposed algorithm and Naïve Bayes algorithm in each repetition.

Repetition NO.	1st	2nd	3rd	4th	5th	6th	7th	8th	9th	10th
DR of the proposed algorithm (%)	95.74	o95.93	95.91	95.9	96.19	95.8	95.59	96.11	95.82	95.93
The DR of NB algorithm (%)	89.95	89.41	90.62	90.12	89.29	89.84	90.2	90.7	90.2	89.72
The FAR of the proposed algorithm (%)	3.02	3.1	3.03	3.08	2.89	3.17	3.21	2.82	3.11	2.97
The FAR of NB algorithm (%)	8.49	8.71	8.07	8.69	9.35	8.52	8.61	7.8	8.38	8.41

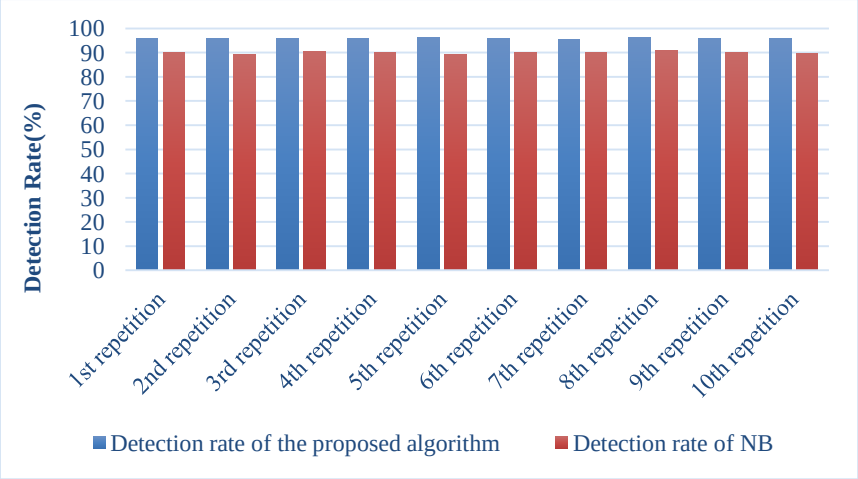

Fig. 1: Comparison of the detection rates of the proposed algorithm and Naïve Bayes classifier.

8. CONCLUSIONS AND FUTURE WORKS

In this paper, a novel distance-based supervised algorithm for network intrusion detection has been proposed. The proposed algorithm uses labeled data in the training phase but it also has the ability of zero-days attack identification. As, the proposed algorithm uses a distance metric it is able to handle the unknown attacks. Based on the experimental results the proposed algorithm is superior to Naïve Bayes algorithm in terms of detection rate and false alarm rate.

In this paper, we leave the algorithm intact without any preprocessing. In the future works preprocessing techniques such as feature selection, weighted Euclidean distance metric can be used in order to improve the performance metrics. In addition, other distance metrics can be used in the future works in order to evaluate the effect of different distance metrics on the proposed algorithm.

9. REFRENCES

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

[2] 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.

[3] P. Kabiri and A. A. Ghorbani, "Research on Intrusion Detection and Response: A Survey," IJ Network Security, vol. 1, pp. 84-102, 2005.

[4] 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.

[5] 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.

[6] S. Mukherjee and N. Sharma, "Intrusion detection using naive Bayes classifier with feature reduction," Procedia Technology, vol. 4, pp. 119-128, 2012.

[7] B. M. Bidgoli, M. Analoui, M. H. Rezvani, and H. S. Shahhoseini, "Performance Evaluation of Decision Tree for Intrusion Detection Using Reduced Feature Spaces," in Trends in Intelligent Systems and Computer Engineering, ed: Springer, 2008, pp. 273-284.

[8] N. B. Amor, S. Benferhat, and Z. Elouedi, "Naive bayes vs decision trees in intrusion detection systems," in Proceedings of the 2004 ACM symposium on Applied computing, 2004, pp. 420-424.

[9] M. Panda and M. R. Patra, "A comparative study of data mining algorithms for network intrusion detection," in Emerging Trends in Engineering and Technology, 2008. ICETET'08. First International Conference on, 2008, pp. 504-507.

[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] A. K. Jain, M. N. Murty, and P. J. Flynn, "Data clustering: a review," ACM computing surveys (CSUR), vol. 31, pp. 264-323, 1999.

[12] M. Jianliang, S. Haikun, and B. Ling, "The application on intrusion detection based on k-means cluster algorithm," in Information Technology and Applications, 2009. IFITA'09. International Forum on, 2009, pp. 150-152.

[13] 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.

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

[15] 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.