A Novel Intrusion Detection Method

ShengYi Jiang [1], QingHua Li [2],Hui Wang[3]

Computer School, Huazhong University of Science & Technology,430074,Hubei,wuhan,China
[1]Jiangshengyi@163.com,[2]Liqh@263.net,[3]Wh621004@yahoo.com

Abstract. It is an important issue for the security of network that how to detect new intrusions attack. This paper investigates unsupervised intrusion detection method. A distance definition for mixed attributes, a simple method calculating cluster radius threshold, a outlier factor measured deviating degree of a cluster, and a novel intrusion detection method are proposed in this paper. The experimental results show that the method has promising performance with high detection rate and low false alarm rate, also can detect new intrusion.

1. Introduction

The signature-based detection methods and supervised anomaly detection methods can only detect previously known intrusion, at same time signature database and labeled data has to be manually processed. To upper flaws, unsupervised anomaly detection methods have been addressed recently [1-4]. However, existing unsupervised methods have some problems: (1)They cannot deal with categorical attributes or deal with categorical attributes too complicatedly. (2)The results of detection are sensitive to the parameter, and it is difficult to select the parameter. (3) It isn't reasonable that the objects in the small clusters are labeled anomalous. This paper is mainly concerned with these problems.

2. Notation and definition

Suppose dataset D is featured by m attributes(m_C categorical and m_N continuous), categorical attributes before continuous attribute, D_i is the set of i-th attribute value.

Definition 1: Given a cluster C and $a_i \in D_i$, then the support of a_i in C with respect to D_i is defined as $Sup_{C|D_i}(a_i) = \left|\{object \middle| object \in C, object.D_i = a_i\}\right|$.

Definition 2: Given a cluster C, the cluster summary information (*CSI*) for C is defined as: $CSI = \{kind, n, Summary\}$, *kind* for the type of the cluster C with 'normal' or 'attack', n for the size of the cluster C, $Summary$ describes the frequency information for categorical attribute value and the centroid of numerical attributes.

$$Summary = \{< Stat_i, Cen > \left| Stat_i = \{(a_j, Sup_{C|D_i}(a_i)) \right| a_j \in D_i\}, 1 \le i, j \le m_C, Cen = (p_{m_C+1}, p_{m_C+2}, \cdots p_{m_C+m_N})\}$$

Definition 3:Given clusters C, C_1, C_2 and objects $p = \{p_i | i \in [1,m]\}$, $q = \{q_i | i \in [1,m]\}$

(1) The distance between objects *p* and cluster *C* is defined as $d(p,C) = (d_C + d_N)/m$, where $d_C = m_C - \sum_{i=1}^{m_C} Sup_{C|D_i}(p_i)/|C|$, $d_N = \sqrt{\sum_{i=m_C+1}^{m_C+m_M} |p_i - c_i|^2}$.

(2) The distance between clusters C_1 and C_2 is defined as $d(C_1, C_2) = (d_C + d_N)/m$,

$d_C = m_C - \frac{1}{|C_1| \cdot |C_2|} \sum_{i=1}^{m_C} \sum_{p \in C_1} Sup_{C_1|D_i}(p_i) \cdot Sup_{C_2|D_i}(p_i) = m_C - \frac{1}{|C_1| \cdot |C_2|} \sum_{i=1}^{m_C} \sum_{q \in C_2} Sup_{C_1|D_i}(q_i) \cdot Sup_{C_2|D_i}(q_i)$,

$d_N = \sqrt{\sum_{i=m_C+1}^{m_C+m_M} |c_i^{(1)} - c_i^{(2)}|^2}$.

Definition 4: Let $C = \{C_1, C_2, \cdots, C_k\}$ is the result of clustering on training data *D*, The outlier factor of cluster C_i is defined as harmonic means of distances between cluster C_i and other clusters: $OF(C_i) = (k-1) / \sum_{j \ne i} \frac{1}{d(C_i, C_j)}$.

3. The clustering-based intrusion detecting method

3.1 Clustering

We use the least distance principle to cluster dataset into hyper spheres with almost the same radius [3]. The details about the clustering are described as follows.

Step 1: Initialize the set of clusters, S, to the empty set, read a new object *p*.

Step 2: Create a cluster with the object *p*.

Step 3: If no objects are left in the database then turn to step 6, else read a new object *p*, find the cluster *C* in S that is closest to the object *p*. In other words, find a cluster *C* in *S*, such that for all C' in S, $d(p,C) \le d(p,C')$.

Step 4: If $d(p,C) > r$ turn to step 2, where *r* is threshold.

Step 5: else merge object *p* into cluster *C* and, modify the *CSI* of cluster *C*.

Step 6: Stop.

3.2 The intrusion detection method

Our intrusion detection method is composed of modeling and detecting module.

(1) Setting up model

Step 1,**Clustering**:Cluster training set T_1 and produce clusters $C = \{C_1, C_2, \cdots, C_k\}$.

Step 2, **Labeling clusters**: Sort clusters $C = \{C_1, C_2, \cdots, C_k\}$ and make them meet $OF(C_1) \le OF(C_2) \le \cdots \le OF(C_k)$. Search the smallest b_1, which satisfies $\sum_{i=1}^{b_1} |C_i| / |T_1| \ge \varepsilon$, and then label clusters $C_1, C_2, \cdots, C_{b_1}$ with 'normal' while $C_{b_1+1}, C_{b_1+2}, \cdots, C_k$ with 'attack'.

Step 3, **Producing model**: The model is made up of the cluster summary information and the radius threshold r.

(2) Detecting attack

For any object p in testing set T_2, find a cluster C_{i_0} which is closest to p, if $d(p, C_{i_0}) \le r$ then classify p by the label of C_{i_0}, else regard p as new attack.

3.3 Tuning parameters

(1) **Selecting threshold r**

According to the process of clustering, threshold r should greater than inter-cluster distance and less than intra-cluster. So we guess logically that r should be close to average distance of any pair's objects. The details are described as follows:

①Choosing randomly N0 pairs of objects in the dataset D.

②Computing the distances between each pair objects.

③ Computing the average EX and standard deviation DX of distances from ②.

④ Selecting r in the range of [EX -0.25DX,EX].

(2) **Selecting parameter** ε

$1-\varepsilon$ is the approximation ratio of outlier to whole dataset. A rule of thumb in statistics is that the proportion of contaminated data in a dataset is usually less than 5% and almost always less than 15%, so we general let ε be about 0.95. If we have prior knowledge on the ratio, we may select ε more accurate.

4. Experimental results

The 10% subset of KDDCUP99[6] is used to evaluate our algorithm. We divide the subset into two subset P1, P2. P1 contains 40459 records (96% normal). P2 contains some unknown attacks type in the P1. We set up model on training set P1, and test model on testing set P2. By computing, EX=0.063, DX=0.043, let ε =0.95, the table 1 show detection result with distinct r. The table 2 shows contrast of results on dataset KDDCUP99 among methods.

Table 1 Detection result with distinct r

	r=0.031	r=0.042	r=0.052	r=0.063	r=0.073	r=0.084
Total detection rate	98.79%	98.53%	98.47%	93.33%	93.18%	27.69%
False alarm rate	1.24%	0.12%	0.40%	1.37%	1.36%	0.43%
Detection rate for unknown attack	37.40%	33.60%	33.56%	58.92%	57.81%	21.24%

Table 2 The contrast of results with different methods on dataset KDDCUP99

Ref.	Detection rate	False alarm rate	Detection rate for unknown attack
[1]	55%-82%	0.8%-4.9%	/
[2]	43.1%-75.2%	/	/
[3]	35.7%-88%	1.44%-8.14%	/
[4]	28%-93%	0.5%-10%	/
[5]	91.8%	0.5%	/
Our method	27.69%-98.79%	0.4%-1.37%	21.24%-58.92%

5. Conclusion

In practice, unsupervised detection methods are important, because these methods can be applied to raw collected system data and do not need to be manually labeled which can be an expensive process. In this paper, we presented a new unsupervised intrusion detection method,the method needn't any prior classification about training data and the knowledge about new attacks. The experimental results show that our method outperforms the existing methods on accuracy.

Acknowledgments

This work is supported by NSFC of P.R.China(No.60273075).

Reference

1. Yamanishi,K.,Takeuchi. J. and Williams, G. On-line unsupervised outlier detection using finite mixtures with discounting learning algorithms. In: Proceedings of the Sixth ACM SIGKDD00, Boston, MA, USA, pp 320-324
2. Yamanishi, K.,Takeuchi, J. Discovering outlier filtering rules from unlabeled data: combining a supervised learner with an unsupervised learner.In:Proceedings of the seventh ACM SIGKDD international conference on Knowledge discovery and data mining , 2001
3. Portnoy, L.,Eskin,E. and Stolfo,S. J.Intrusion Detection with Unlabeled Data using Clustering.In: Proceedings of ACM CSS Workshop on Data Mining Applied to Security (DMSA-2001). Philadelphia, PA: November 5-8, 2001
4. Eskin,E.,Arnold,A.,Prerau,M.,Portnoy, L. and Stolfo, S. A geometric framework for unsupervised anomaly detection: Detecting intrusions in unlabeled data. In Data Mining for Security Applications, 2002
5. Charles Elkan .Results of the KDD'99 Classifier Learning Contest. URL:http://www.cs.ucsd.edu/users/elkan/clresults.html
6. Merz, C. J.,Merphy,P. UCI repository of machine learning databases. URL: http://www.ics.uci.edu/ mlearn/ MLRRepository.html