Cubic Polynomial Smooth Support Vector Machine Used in Intrusion Detection

Zhixin Cai [1, a]

[1] Faculty of Computer, Guangdong University of Technology

[a]email: janson_1015@163.com

Keywords: Intrusion Detection; Polynomial support vector machine; accuracy; Data mining

Abstract. In the research of intrusion detection, we mainly focus on how to improve the accuracy of detection. Based on the introduction of support vector machine, this paper proposes a cubic polynomial smooth support vector machine model and uses it into intrusion detection. Subsequently we analyze each part of the model. Finally we conducted experiments to show that the proposed algorithm has higher accuracy than similar algorithms in Intrusion Detection.

Introduction

With the increasing popularity of computer and network technology, more and more people pay attention to computer network security. As an important part of network security, intrusion detection has attracted more and more attention of scholars. Intrusion detection can be considered as a classification problem, so all kinds of algorithms are used to detect the network system, e.g. Neural Network algorithm [1], Bayesian algorithm[2] and other Machine learning algorithms[3].However, All of the above methods need a lot of or complete audit data set to achieve the desired performance, and the training time is long. How to extract the characteristics of audit data in the case of small samples, and realize the intrusion detection?

Support vector machine[4] can also have a good effect in the case of insufficient training samples. So it was widely used and intrusion detection. In order to improve the performance of support vector machine, one way is to use cubic polynomial to make the objective function smooth[5].

The paper is organized as follows: In section 2, we introduce the cubic polynomial smooth support vector machine algorithm. In section 3, we propose a new model and use the model for intrusion detection .In Section 4 we put forward two experiments. At last, we give our conclusions in section 5.

Cubic Polynomial Smooth Support Vector Machine

Support vector machine use kernel to map the linear non categorical data to the high dimension, so that algorithm can achieve linear classification. The target function of the support vector machine is shown as follows:

$$\begin{aligned} &\text{Min} && \nu e'y + \frac{1}{2}\omega'\omega \\ &\text{s.t.} && D(A\omega - e\gamma) + y \geq e \\ & && y \geq 0 \end{aligned} \tag{1}$$

In the target function (1) y is a slack variable. However y is a 1-norm variable. O.L.Mangasarian and Musicant.D.R[5] proved that it has little effect on the algorithm when y is a 2-norm variable. The improved algorithm is shown as follows. We assume that:

$$y = F_+\left[e - D(A\omega - e\gamma)\right] \qquad F_+(x) = \begin{cases} -\ x \ , x < 0 \\ \ \ x \ , x \geq 0 \end{cases} \tag{2}$$

Then the target function of the algorithm is:

$$\text{Min} \qquad \frac{\nu}{2}\left\| F_{+}\left[e - D\left(A\omega - e\gamma\right)\right]\right\|_2^2 + \frac{1}{2}\left(\omega'\omega + \gamma^2\right) \tag{3}$$

However the function (3) is not the second order differential equation. YUH-JYE LEE and O.L. MANGASARIAN[6] proposed smooth support vector machine and proved that it has better perform compared to SOR algorithm and SMO algorithm. They use function (4) instead of plus function (2):

$$p_0\left(x, k\right) = x + \frac{1}{k}\log\left(1 + \varepsilon^{-kx}\right), k > 0 \tag{4}$$

The target function of the smooth support vector machine is shown as follows:

$$\text{Min} \qquad \frac{\nu}{2}\left\| F_{+}\left[e - D\left(A\omega - e\gamma\right)\right]\right\|_2^2 + \frac{1}{2}\left(\omega'\omega + \gamma^2\right) \tag{5}$$

Yuan Yubo, Yan Jie and Xu Chengxian [7] proposed p1 and p2 smooth support vector machine and Yuan Huaqiang, Tu Wengen, Xiong Jinzhi, Liu Tingting [6] proposed p3 smooth support vector machine. As shown in Fig 1, p3 is the most fitting with p0. So we use the cubic polynomial smooth support vector machine for intrusion detection and it has good effect. And the target function of cubic polynomial smooth support vector machine is shown as follows:

$$\text{Min} \qquad \frac{\nu}{2}\left\| p_3\left[e - D\left(A\omega - e\gamma\right)\right]\right\|_2^2 + \frac{1}{2}\left(\omega'\omega + \gamma^2\right) \tag{6}$$

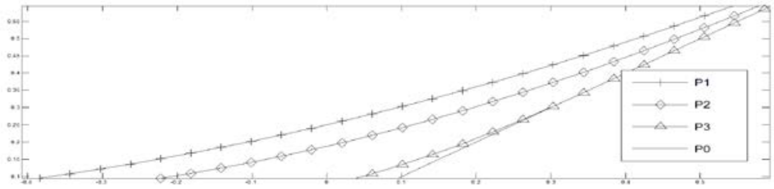

Fig 1. The comparison of four functions.

Cubic Polynomial Smooth Support Vector Machine Used In Intrusion Detection

This paper proposed a model, which is based on cubic polynomial smooth support vector machine. The frame of model consists of three parts, data preprocessor, cubic polynomial smooth support vector machine classifier and decision system. The whole framework of the model is illustrated in Fig 2.

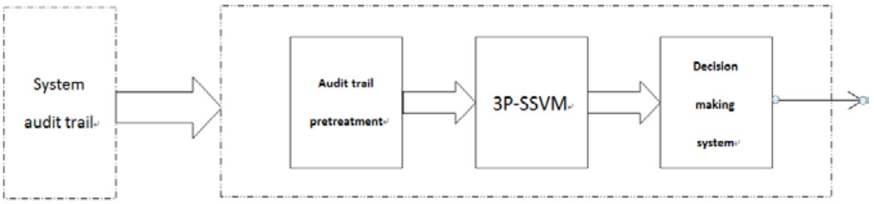

Fig 2. The framework of model.

The data preprocessor is used to process or transform a large number of system audit records. Because the classifier can only classify the data with the same dimension and the data in the network is not only of the same length, but also is likely to be not a digital type. Therefore, we must standardize the original data. The data classification module is the main part of the model .It uses cubic polynomial smooth support vector machine to classify the data. The decision module makes the corresponding decision based on the data obtained from the classifier. The design of this module needs to be very careful. If the model is too sensitive, the model will treat the normal behavior as the invasion. If the detection ability of the model is weak, it will produce a lot of false negatives. So the design of this module needs to be very careful.

The working process of the whole system is divided into two stages: training and testing. In training stage the model is trained according to the known normal data and abnormal data in accordance with the formula (6). In the detection stage, firstly the preprocessing of the unknown state data is processed into the form of digital vector. Secondly use the classifier to classify the data. Thirdly the result will be submitted to the decision making system and system will make the final judgment.

Experiment

We conducted experiments in MATLAB environment. Experiments using KddCup99 data set which contains 40 properties. All data are divided into 5 categories(e.g. normal,DOS,Probing,R2L and U2L). In order to facilitate the record, we use 3-PSSVM to represent cubic polynomial smooth support vector machine. Firstly we use the principal component analysis algorithm to reduce the dimension and redundancy of the data. Secondly we use Newton-Armijo algorithm to train target function (9). Thirdly, we use the trained algorithm to test the KddCup99 data.

We use cubic polynomial smooth support vector machine to test the data, and the result is shown in table 1. As we can see that as the accuracy of all algorithms is very low. However cubic polynomial smooth support vector machine still perform better than others. With the increase of data size, the accuracy of all algorithms is also increased. When the data size is 1000 our algorithm has 94 ccuracy rate which is the highest accuracy in this algorithms. When the data is more and more big, the back of the three algorithms are almost the same. As the amount of data becomes larger and larger, the effect of the machine learning algorithm is very close.

Then, on the premise of the data scale is 1000, 100 sets of noise data are introduced to the above algorithm. The results of the experiment are shown in Table 2. It can be seen from the experimental results that the accuracy of the algorithm is decreased after the introduction of the noise data. But 3-pssvm compared to the other 3 algorithms, still can have a better effect in intrusion detection.

Table 1 The comparation of 4 algorithms

Data size	svm	1pssvm	2pssvm	3pssvm
100,100	49.75%	49.82%	49.93%	50.2%
1000,1000	89.7%	93.2%	93.8%	94%
10000,10000	93.7%	93.9%	94.1%	95.6%

Table.2 After introducing the noise data,The comparation of 4 algorithms

Data size	svm	1pssvm	2pssvm	3pssvm
10000,10000	84.01%	93.20%	95.26%	95.72%

Conclusion

Based on the analysis of the mechanical theory as the foundation, designed the soccer robot pick the ball institutions optimal design process, found aim function, select design variables and the corresponding optimization algorithm to optimize a complete set of institutions. At last through the test to get the final performance parameters of the institution. Experiments show that the system has higher accuracy and stability, the new optimize pick the ball have design basic requirements, and achieved good ideal control effect.

Acknowledgement

This work is supported by the science and technology project of Guangdong Province (No. 9151008990).

References

[1] Wei Wu, Guorui Feng, Zhengxue Li, Yuesheng Xu. Deterministic Convergence of an OnlineGradient Method for BP Neural Networks[J]，2005,16(3):1-9.

[2] H.Altwaijry， S.Algarny. Bayesian based intrusion detection system[J], Computer and Information Sciences, 2012, 24(1): 1-6.

[3] Ahmed H.Fares ,Mohamed I. Sharawy. Intrusion Detection:Supervised Machine Learning[J].Computing Science and Engineering,2011(5)4:305-313

[4] Srinivas Mukkamala,Guadalupe Janoski,Andrew Sung, “Intrusion Detection Using Neural Nerworks and Support Vector Machines,” Neural Networks, vol. 2, pp. 1702 – 1707, May 2002. 10.1109/IJCNN.2002.1007774.

[5] O.L. Mangasarian, Musicant D R. Successive overrlaxation for support vector machines[J]. IEEE Transactions on Neural Networks,1999, 10(5): 1045-9227.

[6] Yuan Yubo, Yan Jie, Xu Chengxian. Polynomial Smooth Support Vector Machine[J]. Chinese Journal Of Computer, 2005, 28(1): 9-17.

[7] YUH-JYE LEE, O.L.MANGASARIAN. SSVM: A Smooth Support Vector Machine for Classification[J]. IEEE Transactions on Neural Networks, 1999, 10(5): 1045-9227.

[8] Yuan Huaqiang, Tu Wengen, Xiong Jinzhi, Liu Tingting. New Polynomial Smooth Support Vector Machine[J]. Computer Science,2011, 38(3): 243-247.

[9] Yuan Huaqiang, Tu Wengen, Xiong Jinzhi, Liu Tingting. New Polynomial Smooth Support Vector Machine[J]. Computer Science,2011, 38(3): 243-24