DoS Attacks Intrusion Detection Algorithm Based on Support Vector Machine

Lingren Wang[1], Jingbing Li[1,2](✉), Jieren Cheng[1],
Uzair Aslam Bhatti[1], and Qianning Dai[1]

[1] College of Information Science and Technology, Hainan University, Haikou 570228, China
Jingbingli2008@hotmail.com

[2] State Key Laboratory of Marine Resource Utilization in the South China Sea, Hainan University, Haikou 570228, China

Abstract. An intrusion detection method which is suitable for the characteristics of WSN (wireless sensor networks) is proposed intrusion detection based on single-class support vector machine. SVM (Support vector machines) can directly train and model the collected data sets, automatically generate detection models, and improve the efficiency of intrusion detection systems. A three-layer intrusion detection model is defined based on this algorithm. The model is more effectively for classifying the data collected by cluster member nodes into intrusion data and normal data. Finally, On the QualNet simulation platform, we implement SVM for the detection of DoS (denial of service) attacks intrusion detection algorithm. The result show that it is feasible to apply SVM to the design of intrusion detection system, with higher system detection rate and lower false alarm rate.

Keywords: WSN · Security system · Intrusion detection · SVM

1 Introduction

With the rapid development of information age, information has taken an increasingly important position in the production and life of human society. Sensors serve as a window for human perception and access to information [1]. It is closely related to human production activities, scientific experiments and daily life. From perspective of network security technology systems and applications. WSN have become an important part of the network security system. Therefore, network security issues should also keep up with the pace of research. In recent years, the continuous advancement of science and technology has made the information acquisition technology with information monotonous in the past has gradually become integrated, dynamic, miniaturized and networked. From the perspective of network security technology system and application, the WSN becomes an important link in network security system [2]. At present, the most effective method is to make WSN security. The WSN have been widely used in daily life, a wide range of areas of environmental protection, military security, smart home, health care, anti-terrorism disaster, science experiments, and other military battlefield. According to the purpose of use it can be divided into non-commercial areas and commercial areas. The non-commercial field is mainly the detection of the environment

X. Sun et al. (Eds.): ICCCS 2018, LNCS 11067, pp. 286–297, 2018.
https://doi.org/10.1007/978-3-030-00018-9_26

such as forest fire prevention, water quality detection, climate monitoring, and environmental monitoring within the building. In these areas, the sensing function of the WSN is the most important, and the security problem will not cause much impact; but in business areas such as the application of military battlefields and monitoring of important business areas, security issues such as the concealment of sensor nodes the accuracy of collected data, and the confidentiality and integrity of the transmission process in WSN are extremely important. Especially in the field of military security, WSN with features that do not require the installation of network facilities, can be quickly deployed, have strong resistance to damage, good concealment, and large coverage areas are very suitable for use in harsh and complex battlefield environments. WSN can help to monitor the area troops, equipment, supplies, environmental change in the conflict zone, reconnaissance of enemy terrain and deployment of nuclear, biological, chemical attack detection and other functions. When monitoring the conflict zone, wireless sensor-based intrusion detection can use its sensor nodes covered in the monitoring area to sense the external environment, obtain intruder intrusion information, detect enemy intrusion attempts, or detect intrusions that have already occurred [4].

In the age of information, access to information has become a decisive factor in military warfare [5]. In order to win in the war, it is required that one side of the battle be able to understand the battlefield information in real time, accurately, and comprehensively. Only by grasping timely and accurate information can we gain the initiative in the war. Traditional network security technologies include firewalls, intrusion detection systems, and intrusion prevention systems, all of which use information to identify and detect network traffic to determine intrusions. Intrusion detection is a proactive security protection technology which is used to detect any network behavior that destroys or damage the security of the system. Compared with firewalls, intrusion detection systems are more functional. It detects malicious intrusions by monitoring the running state of the protection system, the key information of the system or the traffic volume, and makes different responses to the intrusion behavior [6]. Intrusion detection technology is the study, how in vast amounts of network behavior in the data correctly and timely detect the abnormal behavior, in the WSN is another important reference factors in the consumption of energy. The various security problems encountered in WSN have many similarities with traditional Internet security issues, regardless of the attack method or the types of attacks suffered by each layer. The traditional Internet and wireless Ad-Hoc networks have been relatively mature in detection [7]. Using the relevant research theories and achievements of traditional intrusion detection can make research on the intrusion detection of wireless sensor networks have a very good research basis and theoretical basis.

2 Fundamental Theory

2.1 Wireless Sensor Networks (WSN)

Wireless sensor network (WSN) is a sensor to point-to-point (Ad Hoc) form of wireless network [8]. Its purpose is collaboration to perceive the environmental data of network coverage area, then the data acquisition and processing, and then sent to the observer (see Fig. 1). Wireless sensor nodes are deployed in harsh environments to achieve low power consumption, short distance and low speed data transmission. The sensor nodes are connected and forwarded wireless through wireless transmission to form a wide range of coverage. The data collected by the node can be routed and forwarded by other nodes. Finally, the node can reach the destination node or reach the user's controllable location or traditional network.

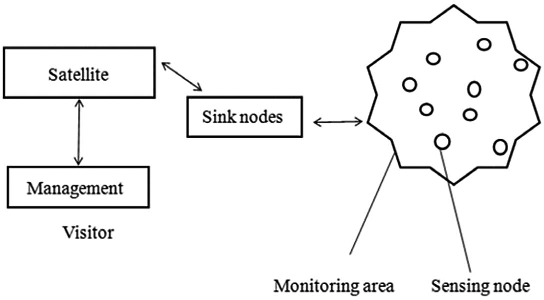

Fig. 1. System structure of WSN.

The three main elements of WSN are sensed objects, sensors and visitors. The essence of the WSN is the communication method of information exchange between the three. The sensed object is the data that the visitor wants to monitor, which has the value of analysis and research. Visitors obtain these data to make simple queries, and also to obtain other more valuable information through analyzing data, or to formulate some strategies. The sensor is the tool for the visitor to collect the data, and the main components of the sensor have the module of sensor, communication, energy supply.

2.2 DoS Attacks

DoS attacks differ from most other attacks because they are not intended to gain access to information on the network or network. The attack is mainly to make the service unable to serve for normal use [9]. The purpose is to make the target computer or network unable to provide normal service or resource access, so that the target system service system stops responding or even crashes.

3 Intrusion Detection Algorithm Model

3.1 Support Vector Machines (SVM)

SVM is a machine learning method based on statistical learning theory [10]. SVM is a classifier developed on the basis of small sample learning, which is specially used for small sample data. It is insensitive to the dimension of data. The main idea of SVM can be summarized as follows: given the training sample, establishes a hyper plane as the decision surface. The purpose of SVM is to find a hyper plane to divide the training samples in the sample space into two parts. In this case, the support vector machine hyper plane is minimum.

Assume we have a training sample set denoted as:

$$S = \{(x_i, y_i)\ |i = 1, 2, 3, \ldots\ldots n\} \quad x_i \subset R^m, \quad y \subset \{+1\ \ -1\} \tag{1}$$

And the hyper plane is denoted as:

$$H\colon \quad Wx + b = 0 \tag{2}$$

SVM Classifier separates data correctly when the distance between the vector closest to the classification surface and the classification surface is the largest and the classification interval (Margin) is the largest. The classification surface is called the optimal classification surface [11] (Fig. 2).

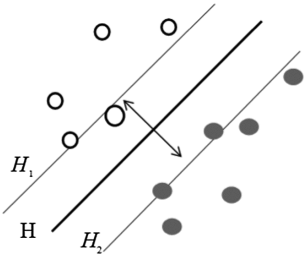

Fig. 2. C-SVM geometry.

M:class interval, H_1: $W^Tx + b = 1$, H_2: $W^Tx + b = -1$, H: $Wx + b = 0$ Make sure no sample exists between H_1 and H_2, we have the following the constraint condition:

$$y_i\{(Wx_i + b) \geq 1, \quad i = 1, 2, \cdots n\} \tag{3}$$

The optimization problem can be expressed as:

$$\min 1/2\|W\|^2 = \frac{1}{2}(w \cdot w) \tag{4}$$

Satisfy (3) conditions make the smallest classification surface is the optimal hyper plane.

*T*he margin(max) $= 2\|W\|^2$. in N dimensional space.

$$\mathrm{f} = (\mathrm{x,w,b})\mathrm{sgn}\ (W^Tx + b) \tag{5}$$

The VC dimension of (4) satisfies the following boundary.

$$h \leq \min([R^2d^2], N) + 1 \tag{6}$$

Introduce the inverse function of Lagrangian.

$$f(w,b,a) = \sum_{i=1}^{N} a_i[y_i(Wx_i + b) - 1] \tag{7}$$

a_i is the Lagrangian multiplier, for W, b for the minimum of the function, which can be converted to the problem of the derivative of the Lagrange function W and b.

$$\partial f(w,b,a)/\partial b = 0,\ \sum_{i=1}^{N} a_i y_i = 0 \tag{8}$$

$$\partial f(w,b,a)/\partial w = 0,\ \sum_{i=1}^{N} a_i x_i y_i \tag{9}$$

Convert (3) to a dual function problem under KKT conditions, that is a_i, the maximum value for solving the following functions.

$$\max\{\sum_{i=1}^{N} a_i - 1/2 \sum_{j=1}^{N} a_i a_j y_i y_j k(x_i \cdot x_j) + b\} \tag{10}$$

This is a quadratic function with constraint conditions. We can solve for a, b, and w are optimal solutions as a^*, b^*, w^*. b:classify thresholds.

The optimal hyper plane function is:

$$f(x) = \operatorname{sgn}\{(w^* \cdot x) + b\} = \operatorname{sgn}\{\sum_{i=1}^{N} a_i y_i k(x_i \cdot x) + b\} \tag{11}$$

3.2 Algorithm Model

Intrusion detection is a very important part of network security [12]. It can be divided into misuse detection intrusion method and anomaly detection intrusion method. When monitored data, misuse detection can detect the signature of an attack by pattern matching to determine whether an attack occurred [13]. Anomaly detection attempts to establish a normal behavior pattern, which can be used to determine whether the system is in an abnormal mode based on some statistical information of the user. In essence, SVM is a behavior that separates normal data from abnormal data. However, the data in the WSN is more complex and has high dimensional, small sample and indivisible features. In existing intrusion detection system structure, according to the relationship between detection node, sensor network intrusion detection can be divided into three types, respectively is a distributed intrusion detection system, peer - collaborative intrusion detection system, hierarchical intrusion detection system. Intrusion detection system mainly includes three basic modules: data acquisition and preprocessing, data analysis and detection and incident response [14] (Table 1).

Table 1. Kernel function table.

Kernel function	Formula
Linear kernel function	$K(x_i, x_j) = x_i \cdot x_j$
Polynomial kernel function	$K(x_i, x_j) = [(x_i \cdot x_j) + \theta]^d, d = 1, 2, \ldots$
Gaussian kernel function	$K(x_i, x_j) = \exp(-\|x_i - y_i\|^2 / \delta^2)$

The data acquisition and preprocessing module is mainly responsible for collecting data from the network or system environment and doing simple preprocessing to make it easy for the detection module to analyze and then directly send it to the detection module. The quality of intrusion detection systems largely depends on the reliability and correctness of information collection. The data analysis and monitoring module is mainly responsible for data analysis of the collected data and detecting the presence of illegal behavior data. The main methods are misuse detection and anomaly detection. The incident response module is mainly responsible for implementing response measures against the analysis results and taking necessary and reasonable actions to prevent the intruder from continuing to destroy the system or recover the damaged system.

The intrusion detection data can be regarded as the different data characteristics of each dimension. Therefore, it can be assumed that the model of the intrusion detection is to collect data points on the n-dimensional space. In general, we can use the kernel function to map the feature vector space from the low dimension to the high dimension, thus achieving the transition from the linear classifier to the nonlinear classifier and reducing the computational complexity. Here we define a three-tier intrusion detection model, which is a cluster member node, cluster head node, Sink node (see Fig. 3). The lowest level is the cluster member node, the middle layer is the cluster head node, and the highest is the Sink node. Also assume that the three types of nodes are heterogeneous nodes. Heterogeneity is reflected in the different communication capabilities, storage capacity, computing power, and energy of the nodes [15]. Among them, the strongest node is the Sink node, and the weakest is the cluster member node. An intrusion detection model based on SVM for wireless sensor networks. The model is based on the network structure of the cluster and divides the network into three layers. Simulation process (see Fig. 4):

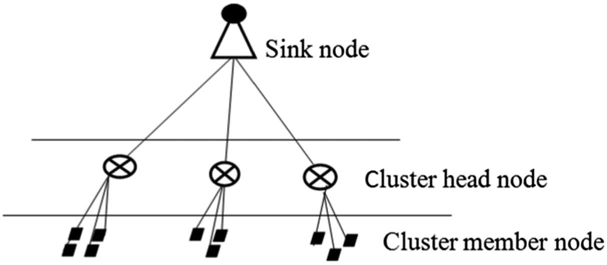

Fig. 3. Intrusion structure model.

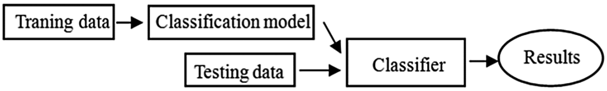

Fig. 4. Simulation process.

For the test effect, the following aspects are considered:

(1) Detection rate = sample number of detected abnormal data/total number of abnormal samples
(2) False positive = number of normal samples misreported as abnormal/normal

The process for the intrusion deployment phase is as follows:

a. In the stage of model establishment, the cluster member nodes are responsible for collecting the original data running in the network and transmitting them to the cluster head nodes. The cluster head nodes aggregate and process the data of the cluster member nodes, process them, and transfer the data aggregation to the Sink nodes after the fusion.
b. The Sink node forms a training data set (12) after receiving n aggregation reports.

$$g(f(x)) = \{f(1),f(2)\ldots f(n)\} \tag{12}$$

c. Normalization of collected sample data sets. Normalization means that in a data set, the range of values between features is often different. If the range of values between features is too different, features with a small range of values are likely to be overwhelmed by features with a large range of values. This can be explained by the fact that features with a small range of values do not have as much effect on the classification results as those with a large range of values. In order to allow each feature to participate in the classification equally, it is necessary to redefine the range of values for each feature.

$$g(f(x)) = Nev = \frac{2Oev - \max(ev) - \min(ev)}{\max(ev) - \min(ev)} \tag{13}$$

Nev is the normalized eigenvalue, max(ev) is the maximum eigenvalue min(ev) is the minimum eigenvalue, Oev is the original data, and the range of eigenvalues is in the [−1, 1].

d. The data completed by the Sink node in the previous step refer to the LibSVM developed by Professor Zhiren Lin, with the specific parameter of SVM type C-SVM. The selection type of kernel function is radial kernel function (the error cost is set to 0.5; tolerance deviation of termination criterion is set to 0.1; weighting coefficient of punishment for all kinds of samples is set to 1) [16].
e. After the training is completed, the Sink node distributes the classification mechanism obtained by the training result to the cluster head node and the cluster member node. Complete the intrusion deployment and start the intrusion test.

After the entire network has completed the deployment of the intrusion detection system, the process of hierarchical processing is still used during the actual testing phase of intrusion detection. The specific steps are:

Step1. When the cluster member node receives the characteristic data (see Table 2), according to its detection system, a preliminary judgment is made first, and then the judgment result and the data are sent to the cluster head node.

Table 2. Packet representation.

Packet name	Method of tagged	Attack type
Number of packets received	NDPR	DoS
Number of received routing request packets	NRRR	Sink Hole
Number of routing request packets sent	NRRS	Sink Hole
Number of lost routing request packets	NRRD	Sink Hole

Step2. After the cluster head node summarizes and processes the data sent by the cluster member nodes, it judges again and checks whether the judgment result of each cluster member node in the cluster is correct and responds accordingly.
Step3. The cluster head node further sends the relevant data to the Sink node to make the most accurate intrusion judgment. The sink node at this time has the most detailed data information of the entire system.

4 Simulation Analysis and Results

4.1 Experimental Platform

In the simulation experiment, we choose QualNet as the test platform (see Table 3), the sensor nodes can perceive the data as a reference index as the simulation object, the statistical properties of the algorithm, intrusion detection accuracy, detection rate, evaluation and analysis of the proposed algorithm. The detection error rate test, assuming that all nodes in wireless sensor network is random deployed in an area, the specific experimental parameters (see Table 4).

Table 3. QualNet's simulation platform.

Assembly	Model/version number	Note
CPU	Intel Core i5-2450 M	3.5 GHz
Memory	DDR3 1600 MHz	8 GB
The operating system	Windows7	SP1
Foundation platform	Matlab	R2012a

Table 4. Parameter values in netwok.

Simulation parameters	Parameter values
Network area (m * m)	100 * 100
Number of nodes	50
Flow size (byte)	512 (B)
Attack time	[250,400] s
Routing protocol	AODV
MAC protocol	IEEE802.11
Flow type	CRB
Maximum moving speed	10 (m/s)
Pause time	5 s

Uniform deployment of 50 nodes to a 100 m × 100 m area, forming 10 clusters through a clustering algorithm. Cluster member nodes and cluster head nodes have only one hop communication distance, and the communication area of cluster head nodes can basically cover the entire deployment area. The communication distance of the Sink node covers the entire area, and its processing capability is strong, and the storage space is large. In the process of node communication, the network intrusion will be simulated. The total run time for each simulation was set to 500 s. The node movement model is a random punctuation model where the pause time is 5 s and the maximum movement speed is 10 m/s. Simulation scenario diagram (see Figs. 5 and 6).

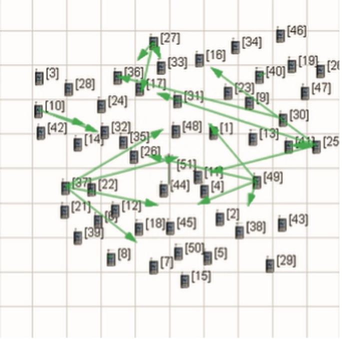

Fig. 5. Simulation scenario.

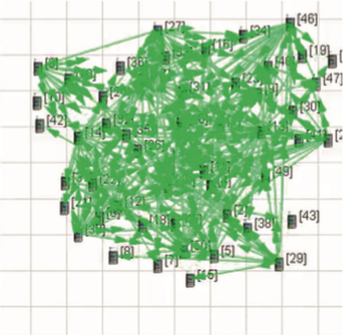

Fig. 6. Simulation scenario.

4.2 Simulation Results

The time interval Δt is taken as a parameter, and the detection rate and false alarm rate received by the intrusion detection algorithm of the SVM classifier during the same time interval Δt are analyzed as experimental results. Four experimental scenarios were set up and the average detection rate and the average false alarm rate were obtained. Set the relationship between different time intervals Δt and the system's average detection rate and detection error. The number of received packets, the number of received route request packets, the number of sent route request packets, and the number of lost route request packets are used as feature vectors for evaluation. When $\Delta t = 10$s the higher the average detection rate, the stronger the detection capability of the system (Table 5).

$$\text{Detection Rate: } DR = \frac{TP}{TP + FN}$$

$$\text{Precision: } P = \frac{TN}{TN + FP}$$

$$\text{False Positive Rate: } FPR = \frac{FP}{TN + FP}$$

Table 5. The meaning of TN, TP, FN, FP.

Symbol	Meaning
TN	Normal samples are identified as normal quantity
TP	Abnormal samples are identified as normal quantity
FN	Normal samples are identified as abnormal quantity
FP	Abnormal samples are identified as abnormal quantity

We can derive line charts (see Figs. 7 and 8) from the experimental test data table and the experimental result table (see Tables 6 and 7).

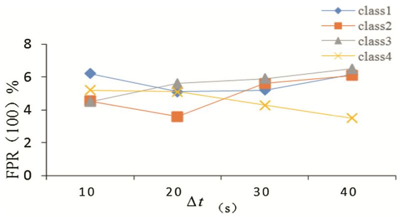

Fig. 7. Relationship between False Positive Rate and time interval Δt.

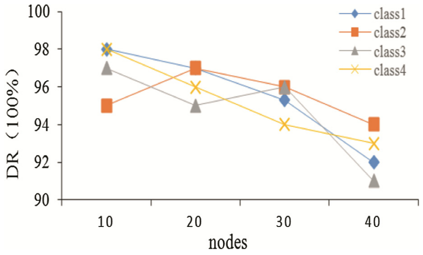

Fig. 8. Relationship between Detection Rate and sensor nodes.

Table 6. Test experimental data sheet.

Δt (%)	Class1		Class2		Class3		Class4	
	DR	FPR	DR	FPR	DR	FPR	DR	FPR
10 s	98	6.2	95	4.54	97	4.5	98	5.2
20 s	97	5.1	97	3.6	95	5.6	96	5.1
30 s	95.3	5.21	96	5.61	96	5.9	94	4.3
40 s	92	6.15	94	6.1	91	6.5	93	3.5

Table 7. Test results table.

Δt	Average detection rate (%)	Average false alarm rate (%)
10 s	97	5.11
20 s	96.25	4.85
30 s	95.33	5.26
40 s	92.5	5.56

From the result comparison chart (see Figs. 7 and 8) it can be obtained that the detection effect is better when Δt 10 s in four scenes is. When Δt = 10 s the DR = 97%, and the FPR = 5.11%. The higher the detection rate, the stronger the system detection attack capability; the lower the false alarm rate, the higher the system's intrusion detection capability. Simulation results show that it is feasible to apply SVM to the design of intrusion detection system. The algorithm has higher detection rate and lower false alarm rate. Therefore, the support vector machine algorithm can achieve intrusion detection of wireless sensor networks.

5 Conclusion

Based on the research of various existing intrusion detection algorithms, a support vector machine algorithm is proposed, and the performance of the algorithm is analyzed theoretically and experimentally.

(1) Successfully solved the problem of classification error in training due to the difference between sample class sizes and the problem of discriminating errors caused by neglecting the importance of samples. The solution of these problems is of practical significance for the application of small balance of some sample classes.
(2) SVM is based on the principle of structural risk minimization and the theory of VC dimension, which can maximize the generalization ability of the learning machine, effectively solve the learning problem, and have a good classification accuracy.
(3) A cluster-based distributed network structure is proposed. The entire network is divided into three layers. Each layer adaptively detects the intrusion, so that the detection accuracy is high and the accuracy of the experimental results is high.
(4) QualNet simulation software mainly optimizes the WSN, which greatly improves the simulation speed, and also guarantees the high simulation accuracy of each node independently running.

As a new important branch of machine learning, SVM has attracted the attention of many scholars, and there are still many problems worth studying.

Acknowledgement. This work is supported by the Key Research Project of Hainan Province [ZDYF2018129], and by the National Natural Science Foundation of China [61762033] and The National Natural Science Foundation of Hainan [617048, 2018CXTD333].

References

1. White, B., Huson, L.: A peer-based hardware protocol for intrusion detection systems. In: Military Communications (2005)
2. Shi, E., Perrig, A.: Designing secure sensor networks. IEEE Wirel. Commun. **11**, 38–43 (2006)
3. Heady, R: The Architecture of a Network-Level Intrusion Detection System, 1st edn., p. 18. Department of Computer Science, Mexico (1990)
4. Patal, S.C., Sanyal, P.: Securing SCADA systems. Inf. Manag. Comput. Secur. **16**(4), 398–414 (2008)
5. Vapnk, V.N.: The Nature of Statistical Learning Theory. Springer, New York (1995). https://doi.org/10.1007/978-1-4757-2440-0
6. Park, Y.: A Statistical Process Control Approach for Network Instrusion Detection. Georgia Instrusion of Technology, Atlanta (2005)
7. Qing, W.: Jiulun FAN: Smooth support vector machine based on piecewise function. J. China Univ. Posts Telecommun. **05**, 124–130 (2013)
8. Abdullah, M.Y.: Security and Energy Performance Optimization in Wireless Sensor Networks (2010)
9. Kooijman, M.: Building Wireless Sensor Networks Using Arduino. Packt Publishing, Birmingham (2015)
10. Chmielewska, I.: Dos personas. Oceano Travesia (2009)
11. Tian, Y.J., Ju, X.C., Qi, Z.Q.: Improved twin support vector machine. Sci. China Math. **57**(02), 201–216 (2014)
12. Nakamori, Y.: Forecasting Nikkei 225 index with support vector machine. J. Syst. Sci. Complex. **16**(04), 3–11 (2003)
13. Shi, L., Duan, Q., Ma, X., Weng, M.: The research of support vector machine in agricultural data classification. In: Li, D., Chen, Y. (eds.) CCTA 2011, Part III. IAICT, vol. 370, pp. 265–269. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-27275-2_29
14. Namnabat, M., Homayounpour, M.M.: Refining segmental boundaries using support vector machine. In: 2006 8th International Conference on Signal Processing. Institute of Electrical and Electronics Engineers, Inc. (2006)
15. Dybala, J.: Comparative analysis of support vector machine and nearest boundary vector classifier. In: The 8th International Conference on Reliability, Maintainability and Safety (ICRMS 2009) (2009)
16. Xue, X.H., Yang, X.G., Chen, X.: Application of a support vector machine for prediction of slope stability. Sci. China Technol. Sci. **57**(12), 89–96 (2014)