Academic Journal of Computing & Information Science
ISSN 2616-5775 Vol. 2, Issue 3: 22-33, DOI: 10.25236/AJCIS.020304

Research on Prediction Method of Network Security Trend Based on Big Data

LIN Yuanjian*, YANG Fei

Nanchang Institute of Science and Technology, Nanchang 330108, Jiangxi
**corresponding author e-mail: linyuanzhou@126.com*

ABSTRACT. *The routing conflict of deep wireless communication network is easy to lead to channel imbalance. In order to improve the security trend of deep wireless communication network, a security trend prediction algorithm of deep wireless communication network based on Kalman fusion filter detection is proposed. The link communication signal reflecting the security trend of deep wireless communication network is extracted, and the channel model of deep wireless communication network is reorganized by using grid packet switching structure. The characteristic quantity of security trend attribute of communication signal in deep wireless communication network is extracted, and the security trend data of deep wireless communication network is detected by autocorrelation matching filter detection method, and the transmission channel equilibrium processing of deep wireless communication network is realized. Combined with association rule mining and matching filtering technology, the security trend of deep wireless communication network is predicted accurately. The simulation results show that the accuracy of this method for predicting the security trend of deep wireless communication network is high, and the balance of transmission channel in deep wireless communication network is improved.*

KEYWORDS: *big data; network security; trend prediction; wireless communication; channel*

1. Introduction

With the development of deep wireless communication network communication technology, the use of deep wireless communication network for network communication and data transmission has become the first choice of network communication in the future[1]. Deep wireless communication network has the advantages of wide and high spectrum resolution, so as to ensure the fidelity of network communication transmission. The transmission network of deep wireless communication network is self-organized, and the routing nodes are prone to channel imbalance and link conflict in the process of packet forwarding, which leads to the poor security of the network. It is necessary to predict the security trend of the

ISSN 2616-5775 Vol. 2, Issue 3: 22-33, DOI: 10.25236/AJCIS.020304

deep wireless communication network[2]. Combined with the channel equilibrium design method, the communication security of the deep wireless communication network is improved, and the level prediction method of the security of the deep wireless communication network is studied. In the field of communication security and network security, great attention has been paid to it, which is of great significance in improving the transmission information security of deep wireless communication network.

The security trend prediction research on the deep wireless communication network is based on the detection of the communication signals and the channel equalization design, and analyzes the security attribute characteristics of the transmission signals by filtering and detecting the network transmission signals, And the safety trend prediction of the deep wireless communication network is carried out in combination with the channel equalization design method[3]. In the traditional method, the method for predicting the safety trend of the deep wireless communication network mainly comprises a safety trend prediction method based on the self-correlation filtering monitoring amount, the invention relates to a method for predicting a network security trend of a deep wireless communication based on a maximum likelihood estimation and a safety trend prediction method based on the spectrum analysis, and the like, the transmission communication signal detection and the self-adaptive frequency spectrum characteristic modulation of the deep wireless communication network are carried out through the matching filtering and the self-correlation characteristic detection method, and the security level prediction is carried out in combination with the characteristic decomposition method, and a certain research result is obtained, a deep wireless communication network security trend prediction and collision detection algorithm based on Hilbert-Huang transform time-frequency analysis is proposed in the reference [5], and the time-frequency decomposition and adaptive modulation filtering are carried out on the communication signals of the deep wireless communication network by using the Hilbert-Huang transform, the transmission performance prediction and the safety trend detection are realized, but the anti-interference capability of the prediction method is not strong, and the prediction and detection performance under the large electromagnetic interference is not good. In reference [6], a method for prediction and security of the intrusion level of a deep wireless communication network based on a route conflict is propose, The method realizes the decomposition and detection of the deep wireless communication network communication signals by adopting a spectrum detection method, improves the prediction accuracy of the security trend, but the calculation complexity of the algorithm is high, and the security protection performance of the deep wireless communication network is not good.

In order to solve the above problems, this paper proposes a security trend prediction algorithm for deep wireless communication network based on Kalman fusion filter detection. Firstly, the link communication signal reflecting the security trend of deep wireless communication network is extracted, and the network transmission signal is decomposed by empirical mode decomposition, and then the transmission signal is converted from time domain to frequency domain by time-frequency analysis method, and the security trend attribute characteristic

ISSN 2616-5775 Vol. 2, Issue 3: 22-33, DOI: 10.25236/AJCIS.020304

quantity of deep wireless communication network communication signal is extracted. The transmission channel equilibrium processing of deep wireless communication network is realized. Finally, the security trend of deep wireless communication network is predicted accurately by combining association rule mining and matching filtering technology, and the simulation experiment is carried out to show the superior performance of this method in improving the accuracy of security trend prediction of deep wireless communication network.

2. Network security transmission channel model and signal analysis of deep wireless communication

2.1 Secure transmission link channel model for deep wireless communication network

In order to predict the security of deep wireless communication network, the secure transmission channel model of deep wireless communication network is constructed, the transmission link structure model of deep wireless communication network is designed by using AD Hoc network structure[7], the channel model of deep wireless communication network is reorganized by using grid packet switching structure, and the transmission link structure model of deep wireless communication network is designed and represented as $L_i\{i=1,2,...,C_L\}$. A directed graph $G=\{V,E\}$ is used to describe the security trend attribute set of deep wireless communication network. The security output task attribute set of deep wireless communication network communication is represented as $neighbor(L_i)=\{L_{i1},\ L_{i2}\}$. Assuming that the communication channel of deep wireless communication network is an extended channel, the link forwarding node includes Sink node and Source node S, assumes that the geometric feature space S of signal transmission in deep wireless communication network under routing conflict. The inter-grid distance between link h_1 and h_2 is represented by the following vector quantification function:

$$x(t)=\frac{1}{\sqrt{T}}rect(\frac{t}{T})\exp\{-j[2\pi K\ln(1-\frac{t}{t_0})]\} \tag{1}$$

Wherein, $rect(t)=1,\ \ |t|\leq 1/2$. Adaptive link equalization method is used to modulate the output signal bit sequence of deep wireless communication network. The initial modulation frequency is as follows:

$$f_i(t)=\frac{K}{t_0-t}\qquad |t|\leq\frac{T}{2} \tag{2}$$

ISSN 2616-5775 Vol. 2, Issue 3: 22-33, DOI: 10.25236/AJCIS.020304

Wherein, $K = Tf_{\max} f_{\min} / B$, $t_0 = f_0 T / B$ is the arithmetic center frequency and $f_{\min}$, $f_{\max}$ is the lowest and highest frequencies of the transmission channel in the deep wireless communication network, respectively. On this basis, the distributed cache technology is used to reorganize the link transmission data, the forwarding routing protocol of the output link layer of deep wireless communication network is constructed, the network security trend is evaluated by cyclic segmentation technology[9], the decision function of network security trend prediction is constructed, the signal model of deep wireless communication network is rebuilt and all routing nodes are traversed by adaptive link balancing method. For security detection and security trend prediction, this implementation process is shown in figure 1.

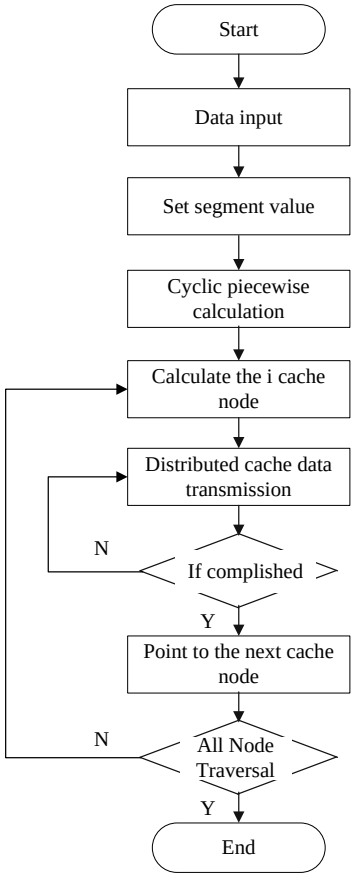

Fig. 1 Implementation process of the trend of the network security trend of the deep wireless communication

According to the analysis of figure 1, it is found that the security trend prediction of deep wireless communication network is based on communication signal

ISSN 2616-5775 Vol. 2, Issue 3: 22-33, DOI: 10.25236/AJCIS.020304

detection and channel balancing design to improve the secure transmission performance of deep wireless communication network communication[10].

2.2 Extraction and preprocessing of communication signals in deep wireless communication networks

On the basis of constructing a deep wireless communication network communication channel model, extracting a link communication signal reflecting the network security trend of the deep wireless communication[11], performing empirical mode decomposition on the network transmission signal, carrying out noise reduction filtering on the signal, The comprehensive load of the depth wireless communication network security trend is as follows:

$$R = w_1 C_i + w_2 D_i + w_3 M_i + w_4 N_i \tag{3}$$

The initial amplitude of the transmission signal of the deep wireless communication network under the routing conflict is X_s, and the link balance configuration is carried out by adopting a time-span sliding time window, so that the impulse response function of the network channel is expressed as follows:

$$h(\tau_i, t) = \sum_{i=1}^{N_m} a_i(t) e^{j\theta_i(t)} \delta(t - \tau_i(t)) \tag{4}$$

The method comprises the following steps of: carrying out empirical mode decomposition on a network transmission signal, then converting a transmission signal from a time domain to a frequency domain by using a time-frequency analysis method[12], obtaining the phase deflection of the depth wireless communication network routing node on the m-th scale as:

$$\phi(i) = \arg\min_{j \in B} \left\| x_i^a - x_j^b, y_i^a - y_j^b \right\| \tag{5}$$

The size of the limited data set m of the deep wireless communication network node link field determines the degree of network security trend, the security attribute factor between A, B is self-adaptive estimation, and the measure function of network security should be recorded as:

$$h(A, B) = \frac{1}{N_A} \sum_{i \in A} \left\| x_i^a - x_{\phi(i)}^b, y_i^a - y_{\phi(i)}^b \right\| \tag{6}$$

Wherein, the link channel equalization configuration function between the weighted vector average, the N_A and the A, B are recorded as:

$$H(A, B) = \begin{cases} h(A, B), if, h(A, B) \le h(B, A) \\ h(B, A), if, h(A, B) \ge h(B, A) \end{cases} \tag{7}$$

The minimum value of the above formula is found, and the directional gain control is carried out according to the matched filter function of the hidden link layer

ISSN 2616-5775 Vol. 2, Issue 3: 22-33, DOI: 10.25236/AJCIS.020304

of the deep wireless communication network. It is assumed that the intensity level TLX, TLY, of the transmitted signal of the deep wireless communication network can obtain the equilibrium position of the communication signal of the deep wireless communication network on the two-dimensional plane (m,n):

$$TL_X(x,y)=\begin{cases} Text & ,if\,(GD_X(x,y)>T_X) \\ NonText & ,Otherwise \end{cases} \tag{8}$$

According to the principle of similarity transitivity, the parameter estimation is carried out in two discrete sampling intervals. The amplitude-frequency parameter estimation value is that a_{mn}, adaptively adjusts the security trend control coefficient of deep wireless communication network by using Gabor basis function:

$$d_{j^*}=\min_{0\le j\le N-1}\{d_j\} \tag{9}$$

And a specific window function is selected to extract the characteristic quantity of the security trend attribute of the deep wireless communication network communication signal, and the safety trend prediction is carried out[13].

3. Improvement of network security trend prediction algorithm for deep wireless communication

3.1. Autocorrelation matched filter detection

On the basis of extracting the link communication signal reflecting the trend of the network security trend of the deep wireless communication, the network transmission signal is subjected to empirical mode decomposition, and the design of the depth wireless communication network security trend prediction algorithm is carried out[14], in this paper, a deep wireless communication network security trend prediction algorithm based on Kalman filter detection is proposed, and a Kalman filter for deep wireless communication network signal filtering is constructed to obtain the filter transfer function:

$$H(t)=\hat{h}(t)*p(t)*p(-t)=(\sum_{i=1}^{M}h_i'(t)*h_i(-t))*p(t)*p(-t) \tag{10}$$

Wherein the channel impulse response estimates $\hat{h}(t)$ and $p(t)*p(-t)$ of the deep wireless communication network approximate the Kalman filter coefficients of the $\delta(t)$ in the spread spectrum channel. By using the complex-envelope feature decomposition method, the high-order cumulant estimation value of the transmission channel of the deep wireless communication network is obtained as follows:

ISSN 2616-5775 Vol. 2, Issue 3: 22-33, DOI: 10.25236/AJCIS.020304

$$\hat{x}(k/k)=\sum_{j}^{m}\hat{x}^{i}(k/k)u_{j}(k) \tag{11}$$

$$P(k/k)=\sum_{j}^{m}u_{j}(k/k)\{P^{j}(k/k)+[\hat{x}^{j}(k/k)-\hat{x}(k/k)][\hat{x}^{j}(k/k)-\hat{x}(k/k)]^{T}\} \tag{12}$$

Wherein, $\hat{x}$ is the instantaneous frequency estimation value of the network output signal, $u_j(k)$ is the time-frequency distribution attribute set, u_j is the pulse impulse response in the neighborhood, which can effectively reflect the security trend attribute of the deep wireless communication network.

The correlation matching filter detection method is adopted, and the communication signals of the output link layer of the deep wireless communication network are subjected to noise reduction filtering, and the correlation dimension characteristic quantity of the extracted signals is recorded as follows:

$$Posi(B)=-\sum_{i=1}^{m}p_{i}\times\log_{2}p_{i} \tag{13}$$

In the above formula, the p_i represents the weighted arithmetic average amount of the signal receiving end, and the correlation degree evaluation method is adopted to carry out the deep wireless communication network security trend prediction equilibrium game control, and the output gain of the network channel is obtained as follows:

$$Gain_{A}(B)=\sum_{j=1}^{v}\frac{|B_{j}|}{|B|}\times Info(B_{j}) \tag{14}$$

In the above formula, B_j is the noise spectrum level (dB/Hz), and the Doppler shift modulation method is used as follows:

$$a_{k}=(\sum\nolimits_{k}+\varepsilon U)^{-1}(\frac{1}{|w|}\sum_{i\in w_{k}}I_{i}p_{i}-u_{k}\overline{p}_{k}) \tag{15}$$

According to the similarity transmission principle, the safety trend rule-shaped function I_i of the deep wireless communication network is generalized and matched, and the self-correlation matching filter detection method is adopted to carry out the quantitative balance, and the safety trend attribute is improved[15].

3.2. Security trend estimation and prediction implementation of deep wireless communication network

The phase of the multi-path signal of the deep wireless communication network on the strip transmission channel is carried out, the propagation loss of the routing node i of the deep wireless communication network in the $t(n)$ time window is

ISSN 2616-5775 Vol. 2, Issue 3: 22-33, DOI: 10.25236/AJCIS.020304

estimated, and obtaining the parameter estimation value of the transmission safety trend prediction of the deep wireless communication network as follows:

$$a_k = (\sum\nolimits_k + \varepsilon U)^{-1}(\frac{1}{|w|}\sum_{i\in w_k} I_i p_i - u_k \overline{p}_k) \tag{16}$$

$$b_k = \overline{p}_k - a_k^T u_k \tag{17}$$

$$q_i = \frac{1}{|w|}(\sum_{i\in w_k} a_k I_i + b_k) = \overline{a}_i^T I_i + \overline{b}_i \tag{18}$$

In the transmission channel coverage space $L^2(R)$, the network communication multipath transmission channel attenuation is obtained by logical reasoning:

$$CIntra_i(n) = \frac{NIntra_i(n)}{T}, CInter_i(n) = \frac{NInter_i(n)}{T}. \tag{19}$$

The security trend prediction is carried out by using association rule mining and matching filtering technology, and the prediction results are as follows:

$$\lambda^n(d_{\gamma_0}) = \int_{-\infty}^{+\infty} f(t) \otimes d_{\gamma_0}^*(t) dt \tag{20}$$

Considering the heterogeneity of transmission channels from N deep wireless communication network communication nodes, when the security trend of deep wireless communication network as $x_j \in \boldsymbol{R}^m$, $j \in 1, 2, \cdots, N$ is satisfied, the security trend of deep wireless communication network is predicted through the above algorithm design, and the security performance of the network is improved.

4. Simulation experiment and performance analysis

In order to test the application performance of this method in predicting the security trend of deep wireless communication network, the simulation experiment is carried out. The experiment adopts Simulink platform to simulate the communication platform of deep wireless communication network, uses Matlab 7 programming to design the algorithm, and sets the impulse response characteristic coefficient of Kalman filter coefficient $r_1 = r_2 = 1$, $p_1 = 2$, matching filter detection coefficient $m = 12$, deep wireless communication network transmission signal frequency range: 24~36kHz. The Gaussian noise interference intensity in bandwidth $B = 1000$, channel is -24dB. According to the above simulation environment and parameter setting, the security trend prediction simulation of deep wireless communication network is carried out. Taking a set of LMF signals as test signals, the original signal acquisition in deep wireless communication network is obtained as shown in figure 2.

ISSN 2616-5775 Vol. 2, Issue 3: 22-33, DOI: 10.25236/AJCIS.020304

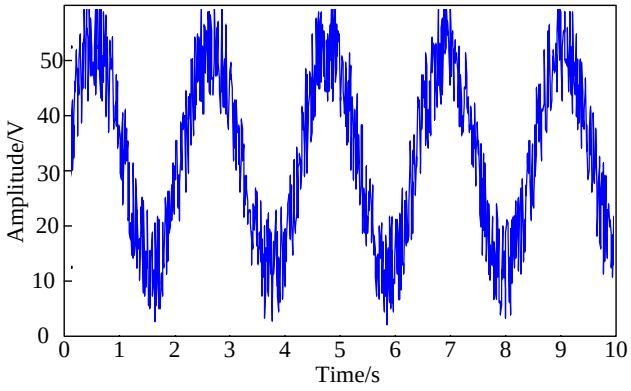

Fig. 2 Original signal of the deep wireless communication network communication

Based on the test set of communication signal in deep wireless communication network shown in Fig. 2, the security trend of communication signal transmission in deep wireless communication network is analyzed. The security trend data detection and channel equilibrium configuration of deep wireless communication network are carried out by using autocorrelation matching filter detection method. The optimized output signal waveform is shown in Fig. 3.

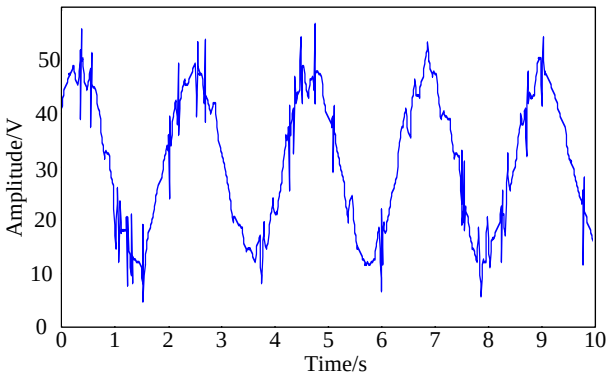

Fig. 3 output signals after channel equalization and filtering in deep wireless communication networks

Figure 3 is valuable, and the channel equilibrium configuration of deep wireless communication network is carried out by using this method, which improves the anti-interference of transmission signal and reduces the interference of noise to network communication channel, thus improving the security of the network. On this basis, the network security trend evaluation is carried out, and the accuracy of security trend prediction is compared with the traditional method, and the comparison of prediction accuracy is obtained as shown in figure 4. Figure 4 shows

ISSN 2616-5775 Vol. 2, Issue 3: 22-33, DOI: 10.25236/AJCIS.020304

that the proposed method has the highest accuracy in predicting the security trend of deep wireless communication networks.

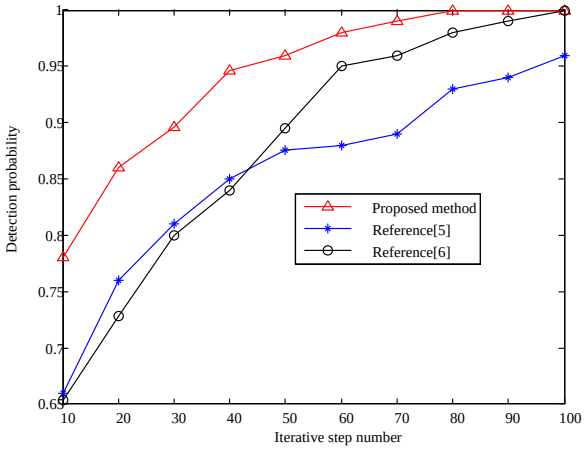

Fig. 4 Comparison of accuracy of security trend prediction in deep wireless communication networks

Further testing the security trend of deep wireless communication network to predict the bit error rate (BER) of the output communication signal, and then evaluate the channel equalization and the security of the transmission data, the comparative results of BER are shown in Table 1. The analysis shows that the output BER of this method is low, which indicates that the security of the communication network is the best and the fidelity rate of the data is the highest.

Table 1 Comparison of the output error rate of the deep wireless communication network

SNR/dB	Proposed method	Lyapunov prediction	Mutual information prediction
-10	0.123	0.325	0.434
-6	0.114	0.216	0.324
-2	0.032	0.165	0.124
2	0.025	0.034	0.121
6	0.010	0.021	0.034
10	0	0.018	0.012

ISSN 2616-5775 Vol. 2, Issue 3: 22-33, DOI: 10.25236/AJCIS.020304

5. Conclusions

The security trend prediction of deep wireless communication network is carried out, and the communication security of deep wireless communication network is improved by combining the channel equilibrium design method. In this paper, a security trend prediction algorithm of deep wireless communication network based on Kalman fusion filter detection is proposed, and the security trend attribute characteristic quantity of communication signal of deep wireless communication network is extracted. The autocorrelation matching filter detection method is used to detect the security trend data of the deep wireless communication network, and the security attribute factors of the deep wireless communication network are estimated adaptively, and the measure function of the network security is obtained. The correlation matching filter detection method is used to reduce the noise of the communication signal in the output link layer of the deep wireless communication network. The accurate prediction of security trend and the channel equilibrium design of deep wireless communication network is realized. The results show that this method has high accuracy and low output bit error rate (BER), which improves the security of network transmission.

Acknowledgements

This work is supported by Department of Nanchang Institute of Science&Technology and Technology research youth project in 2018(Item no.NGKJ1814).

References

[1] Youcef AMIRAT,Arnaud MÜ,NCH. On the Controllability of an Advection-diffusion Equation with Respect to the Diffusion Parameter: Asymptotic Analysis and Numerical Simulations[J]. Acta Mathematicae Applicatae Sinica, English Serie, 2019, 35(1): 54-110.

[2] Wei-ke WANG,Yu-tong WANG. The Well-Posedness of Solution to Semilinear Pseudo-parabolic Equation[J]. Acta Mathematicae Applicatae Sinica, English Serie, 2019, 35(2): 386-400.

[3] Al-Hussein A, Haldar A. Unscented Kalman filter with unknown input and weighted global iteration for health assessment of large structural systems. Structural Control and Health Monitoring, 2015, 23(1),156-175

[4] Liu Yilong, Liu Jie, Liu Jiangnan. Research on composite inversion of dynamic loads and structural parameters based on sub-structure analysis. Journal of Mechanical Strength, 2013, 35(5),553-558.

[5] Noël J P, Kerschen G. Nonlinear system identification in structural dynamics,10 more years of progress. Mechanical Systems and Signal Processing, 2017, 83,2-35.

[6] ALI M S, TABASSUM H, HOSSAIN E. Dynamic user clustering and power

ISSN 2616-5775 Vol. 2, Issue 3: 22-33, DOI: 10.25236/AJCIS.020304

allocation for uplink and downlink Non-Orthogonal Multiple Access (NOMA) systems[J]. IEEE Access, 2016, 4:6325-6343.

[7] KIM B, CHUNG W, LIM S, et al. Uplink NOMA with multi-antenna[C]//Proceedings of the 2015 IEEE 81st Vehicular Technology Conference. Piscataway, NJ:IEEE, 2015:1-5.

[8] JIANG Y Z, CHUNG F L, WANG S T, et al. Collaborative fuzzy clustering from multiple weighted views[J]. IEEE Transactions on Cybernetics, 2015, 45(4): 688-701.

[9] TU Binbin, CHUAI Rongyan, XU Hui. Outlier Detection Based on K-mean Distance Outlier Factor for Gait Signal[J]. Information and control, 2019, 48(1): 16-21.

[10] ZHOU S B, XU W X. A novel clustering algorithm based on relative density and decision graph[J]. Control and Decision, 2018, 33(11):1921-1930.

[11] HE H, TAN Y. Automatic pattern recognition of ECG signals using entropy-based adaptive dimensionality reduction and clustering[J]. Applied Soft Computing,2017, 55:238-252

[12] ZHU Yuelong, ZHU Xiaoxiao, WANG Jimin. Time series motif discovery algorithm based on subsequence full join and maximum clique. Journal of Computer Applications, 2019, 39(2): 414-420.

[13] HUANG S C, LIU Y. Classification algorithm for noisy and dynamic data stream[J]. Journal of Jiangsu University of Science and Technology (Natural Science Edition), 2016, 30(3):281-285.

[14] SUN B, WANG J D, CHEN H Y, et al. Diversity measures inensemble learning[J]. Control and Decision, 2014, 29(3):385-395.

[15] ZHOU Yuhao, ZHANG Hongling, LI Fangfei, QI Peng. Local focus support vector machine algorithm[J]. Journal of Computer Applications, 2018, 38(4): 945-948.