# Small area purification and recognition of network intrusion signals based on the second-order matching filter detection

Lianguang Mo

School of Management,
Hunan City University,
Yi yang 413000, China
Email: molianguang12@sina.com

Yucai Zhou*

School of Energy and Power,
Changsha University of Science and Technology,
Changsha 410076, China
Email: zhouyucaii@sina.com
*Corresponding author

**Abstract:** In order to improve the ability of intrusion detection and recognition. This paper proposes a method of small area purification and recognition of network intrusion signal based on second-order matched filter detection. In this method, the time-frequency analysis of network intrusion signal is carried out, and Hilbert Huang transform is used to decompose the time-delay scale of small-scale network intrusion signal, and then the spectrum feature is input into the second-order lattice matched filter to improve the signal resolution, and adaptive weighting method is used to adjust the filter tap coefficient to improve the detection and recognition ability. The simulation results show that the method can accurately recover two groups of component information of network intrusion signal: sinusoidal signal and sinusoidal frequency modulation signal. The recognition accuracy of network intrusion signal can reach 100%, which shows that the method has good signal purification performance.

**Keywords:** network intrusion signal; detection; filter; recognition; spectral characteristic quantity extraction; time-frequency analysis.

**Reference** to this paper should be made as follows: Mo, L. and Zhou, Y. (2022) 'Small area purification and recognition of network intrusion signals based on the second-order matching filter detection', *Int. J. Internet Protocol Technology*, Vol. 15, No. 1, pp.1–7.

**Biographical notes:** Lianguang Mo received his PhD degree from School of Finance and Taxation of Central University of Economics and Law in 2008. Now he is a Professor in the School of Management of Hunan City University. His research interests include intelligent control and project management, information management of Internet of Things.

Yucai Zhou received her PhD degree in Mechanical and Electrical Engineering from Central South University in 2012. He is a vice professor in the Energy and Power Institute of Changsha University of Science and Technology, and his research interests are in signal processing, intelligent control and intelligent system, embed system.

## 1 Introduction

With the development of network information technology, a large amount of data information is transmitted and stored through the network. The network brings convenience of information utilisation. But at the same time, due to the openness and uncertainty of the cyberspace, it also produces a large amount of network security problems. The network attackers carry out information theft and tampering by implanting intrusion signals to steal information concerning user's account and business information, which will result in network users' privacy leakage and property losses. Therefore, it is required to study an effective network security defence method to protect against network intrusion attacks, and improve network security performance. Now, network security detection has become a research hotspot. Network security detection is divided into active detection and passive prevention, in which active detection has more initial lead

Copyright © 2022 Inderscience Enterprises Ltd.

than passive firewall detection. Active detection can discover the intrusion information characteristic quantity in time to realise early prevention and recognition of network intrusion (Zhang and Chen, 2014). The active detection of network attacks is based on the detection and recognition of network intrusion signals. The network intrusion signals are strictly-sense stationary, resulting in a lot of colour noise in the signal, so it is required to carry out purification processing to the signal. Therefore, it is of great significance to study the small area purification and recognition algorithms of network intrusion signals in the improvement of network security performance. In the design of small area purification and recognition algorithms for network intrusion signals, the typical algorithms include time-frequency detection method, Gaussian filtering method, wavelet detection method and spectral analysis detection method and so on (Chen et al., 2017; Mi et al., 2016; Mernik et al., 2015). In those methods, the spectrum characteristic quantity of network intrusion signals is extracted and the filter detector is adopted to realise the small area purification and recognition of network intrusion signals, and improve the detection performance. Some research achievements have been obtained about it. In Hsieh (2014), a multi-component network intrusion signal recognition method based on adaptive cascade filtering is proposed, which adopts a autocorrelation matching filter for signal interference filtering, and the wavelet feature decomposition method to extract time-frequency component, so as to realise signal filter detection. But this method is not accurate in detecting large scale intrusion signals and poor in anti-interference ability. In Moradi and Keyvanpour (2015), a network intrusion detection method based on empirical mode decomposition and Gauss recombination is proposed, which adopts the empirical mode decomposition method (EMD method for short) to decompose the spectrum of intrusion signals and decompose the intrusion signals into multiple intrinsic modal components, adopts the statistical analysis method to purify signals, so as to improve small area purification ability of intrusion signals. But the computational overhead in the process of implementation of the method is too large and the real-time detection is not good. In Zhou and Peng (2015), a network intrusion signal detection algorithm is proposed. In this algorithm, a network intrusion signal model under low SNR is constructed, and the local feature compression sampling detection of network intrusion signals is realised. The simulation results show that the algorithm has good detection performance, and it provides better detection probability than traditional algorithms. But the overall detection overhead of it is too large and the recognition performance of network intrusion signals with high SNR is not considered. In Gu (2017), a network intrusion signal extraction and detection model based on large data driving and rough set-decision tree is proposed. With a rough set, properties of different data sets are valued dispersedly and the attribute core of network intrusion extraction is obtained. With the decision tree, the extracted intrusion data with different properties are classified, and the HMM model parameters are initialised. The detected network intrusion signal eigenvectors are input into the model, and the final network signal intrusion detection model based on rough set-decision tree and large data driving is constructed. The experiment results show that the proposed model has high detection accuracy. However, only the detection accuracy is considered in it, and algorithm is complex without considering the time cost and the influence of different random factor on the test result.

In view of the above problems, a method of small area purification and recognition of network intrusion signals based on the second order matching filter detection is proposed. In this method, the time-frequency analysis of network intrusion signals is performed; the Hilbert-Huang transform method is adopted for time delay scale decomposition of network intrusion signals in a small area, and the fractional Fourier transform method is adopted to extract spectrum characteristic quantity of the network intrusion signals; and then the spectrum characteristic quantity is input into the second order lattice matching filter to purify the signal in a small area to filter the coherent colour noise and improve the distinguishable ability of the signals, and the adaptive weighting method is adopted to adjust the filter tap coefficient. The spectrum and bandwidth of the inputted network intrusion signals can be independently adapted and the detection and recognition ability can be improved. Finally, a simulation experiment is carried out for intrusion detection simulation, which demonstrates the application performance of this method in improving the small area recognition of intrusion signal.

## 2 Model and time frequency analysis of network intrusion signals

### *2.1 Analysis of network intrusion signals*

In order to realise the small area purification and recognition of network intrusion signals, a network intrusion signal model is constructed firstly, and the grid partition node overlay structure model is constructed, which is represented by $\mathbf{EH}(s,t)=(\mathbf{V},\mathbf{E})(s\geq 1,t\geq 1)$. In the connected region, the data transmission bit rate of $\frac{N}{WL}$ nodes is obtained. Set the transmission powers as $p_i$, $p_k$ and $p_{k+1}$, and the corresponding network forwarding control protocols of them are described as $r_i$, $r_k$ and $r_{k+1}$. Under the optimal transmitting power control, the transmission link impulse response model of the network is constructed (Dong et al., 2013). If $p^2G_T+\alpha T-pC>0$, under the optimal hop number $hop\_count_{opt}$, the transmission model of network intrusion signals in the channel is obtained, which satisfies

$$\begin{aligned} H(P_e^E)+P_e^E\log\left|S^N\right| &\geq H(S^N\mid\hat{S}_E^N) \\ &\geq NR-N\varepsilon \end{aligned} \tag{1}$$

where $P_e^E$ is instantaneous bandwidth of network intrusion signals; $\left|S^N\right|$ is bit sequence length of network intrusion data with length $N$. With the non-stationary signal analysis

method (Khalili and Sami, 2015), the modulation variable $R^N$ of the intrusion signal is obtained, which satisfies

$$\begin{aligned} &\left|R^N\right| = \left|X^N\right|, \\ &angle\left(R^N\right) = \left(angle\left(X^N\right) + \varphi_g\right) \bmod (2\pi) \end{aligned} \tag{2}$$

where the phase angle is $\varphi_g = angle(g)$. The phase deflection of intrusion signal is obtained with intra-wave frequency modulation as follows:

$$angle\left(gX^N\right) = \left(angle\left(X^N\right) + \varphi_g\right) \bmod (2\pi) \tag{3}$$

According to the positive correlation between wave frequency and interwave frequency, the multipath attenuation of network intrusion signals is obtained:

$$gX^N = |g| R^N \tag{4}$$

By combining the above formula, it is obtained that

$$Z^N = |g| R^N + W^N \tag{5}$$

Based on the above analysis, the transmission model of network intrusion signals is constructed as shown in Figure 1.

The analysis of Figure 1 shows that network intrusion signals are processed with phase deflection modulation and adaptive filtering via channel 1 and channel 2, for example, real network intrusion signals are scanned for stampede points, and then relevant information is collected, and the signals are converted from time domain to frequency domain based on time-frequency analysis. And the data transmission gap $\varphi_g$ between network user Alice and Bob is expressed as a constant. According to the phase deflection characteristic of the signals (Keshavamurthy et al., 2013), the autocorrelation between the channel independence phase $R^N$ and $X^N$ is obtained, which is described as:

$$p\left(R^N = r_i\right) = p\begin{pmatrix} X^N = x_i \left| |x_i| = |r_i|, angle(x_i) \right. \\ = \left(angle(r_i) - \varphi_g\right) \bmod (2\pi) \end{pmatrix} \tag{6}$$

By introducing the concept of intrinsic modal function and instantaneous frequency, the transfer function model of network intrusion signals is:

$$\begin{aligned} H\left(R^N\right) &= -\sum_{i=1}^{M} p\left(r_i\right) \log^{(p(r_i))} \\ &= -\sum_{i=1}^{M} p\left(x_i\right) \log^{(p(x_i))} \\ &= H\left(X^N\right) \end{aligned} \tag{7}$$

where $M$ is the number of elements in the symbol set.

## *2.2 Time delay scale decomposition of network intrusion signals*

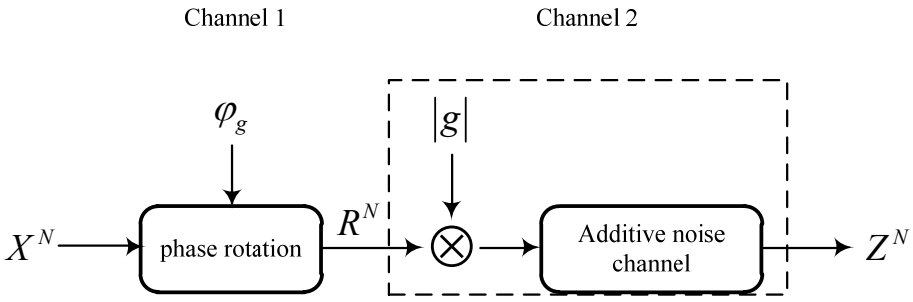
The Hilbert-Huang transform method is adopted for time delay scale decomposition of network intrusion signals in a small area (Xu and Cheng, 2013), to achieve the time-frequency analysis of network intrusion signals. Hilbert-Huang transform is:

$$\begin{aligned} C_S &= \max_{X^N}\left[I\left(X^N; Z_B^N\right) - I\left(X^N; Z_E^N\right)\right] \\ &= \max_{X^N}\left[H\left(R_E^N \mid Z_E^N\right) - H\left(R_B^N \mid Z_B^N\right)\right. \\ &\quad \left. + H\left(\varphi_E \mid Z_E^N\right) - H\left(\varphi_B \mid Z_B^N\right)\right] \\ &= \max_{X^N}\left[H\left(W_E^N \mid Z_E^N\right) - H\left(W_B^N \mid Z_B^N\right)\right. \\ &\quad \left. + H\left(\varphi_E \mid Z_E^N\right) - H\left(\varphi_B \mid Z_B^N\right)\right] \end{aligned} \tag{8}$$

where $\varphi_B$ and $\varphi_E$ $R_B^N$ and $R_E^N$, $W_B^N$ and $W_E^N$ are extensions and displacements of network intrusion signals in time domain and frequency domain respectively. In the case of fixed window shape and single time frequency resolution (Guan et al., 2016), the minimum mean square error estimation and small area detection are carried out on parameters $\varphi_g$, $R^N$ and, $W^N$. Then $C_{B,2}$ and $C_{E,2}$ are adopted to represent decision threshold and threshold value, and then the decision function of signal detection is obtained:

$$\begin{aligned} H\left(X^N \mid Z^N\right) &= H\left(R^N, \varphi_g \mid Z^N\right) \\ &= H\left(R^N \mid Z^N\right) + H\left(\varphi_g \mid Z^N\right) - I\left(R^N; \varphi_g \mid Z^N\right) \end{aligned} \tag{9}$$

**Figure 1** Transmission model of network intrusion signals



When the phase distribution $angle\left(X^N\right)$ of the intrusion signal is uniformly distributed on $[0,2\pi)$, $R^N$ and $\varphi_g$ are independent, and the frequency resolution at high frequency band can be decomposed by the time delay scale (Dou et al., 2016). The time delay scale decomposition is:

$$\begin{aligned} &H\left(g_1,g_2,\cdots,g_N\right)\\ &\quad=H\left(g_1\right)+H\left(g_2,\cdots,g_N\left|g_1\right.\right)\\ &\quad\vdots\\ &\quad=H\left(g_1\right)+H\left(g_2\left|g_1\right.\right)+\cdots+H\left(g_N\left|g_1,g_2,\cdots,g_{N-1}\right.\right)\end{aligned} \tag{10}$$

At this moment, based on the phase information of the intrusion signal $I\left(R^N;\varphi_g\mid Z^N\right)=0$, the frequency domain transform characteristic component of intrusion signals is obtained:

$$H\left(X^N\cdot Z^N\right)=H\left(R^N\cdot Z^N\right)+H\left(\varphi_g\cdot Z^N\right) \tag{11}$$

Mutual information is:

$$\begin{aligned} I\left(X^N;Z^N\right)&=H\left(X^N\right)-H\left(X^N\mid Z^N\right)\\ &=H\left(X^N\right)-H\left(R^N\mid Z^N\right)-H\left(\varphi_g\mid Z^N\right)\end{aligned} \tag{12}$$

According to the result of the time delay scale decomposition of network intrusion signals in a small area, the signal filter is detected, and a filter is designed to filter the interference to improve the purification ability of intrusion signals.

## 3 Realisation of intrusion signal purification and recognition

After time delay scale decomposition of network intrusion signals, the frequency domain transform characteristic component of intrusion signals is obtained. According to the characteristic component, the spectrum characteristic quantity of the intrusion signals is extracted. According to the spectrum characteristic quantity, the intrusion signal is done with matching filter purification to realise the recognition of the intrusion signals.

### *3.1 Spectrum characteristic quantity extraction of intrusion signals*

In the time-frequency analysis of network intrusion signals, the Hilbert-Huang transform method is adopted for time delay scale decomposition of network intrusion signals in a small area, and the fractional Fourier transform is carried out for intrusion signals in a small area (Pattewar and Sonawane, 2016). The resolution of the intrusion signals on time-frequency plane is $\nu(t,\theta)$, which satisfies:

$$\nu(t,\theta)=\sum_{m=1}^{M}\omega_i^*(\theta)x_i(t)=\sum_{m=1}^{M}x_i^*(t)\omega_i(\theta) \tag{13}$$

where "*"represents complex conjugate operator. The fractional Fourier transform is adopted for spectral feature extraction of intrusion signal, which satisfies:

$$\nu(t,\theta)=\omega^H(\theta)x(t)=x^H(t)\omega(\theta) \tag{14}$$

where "$H$" represents complex conjugate transpose, $x(t)$ and $\omega(\theta)$ represent empirical mode decomposition of time-frequency surface $w(t)$, which satisfies:

$$x(t)=\left[x_1(t)\ x_2(t)\cdots x_M(t)\right]^T \tag{15}$$

$$\omega(\theta)=\left[\omega_1(\theta)\ \omega_2(\theta)\cdots\omega_M(\theta)\right]^T \tag{16}$$

The displacement of the wavelet function in the transformation is calculated in the spectral component of the intrusion signals, and the output delay of the signals is $\tau_0(\theta)=\frac{\Delta}{c}\sin\theta$. According to the changing characteristic of signal decomposition, the extraction result of spectrum characteristic quantity of intrusion signal is expressed as:

$$\begin{bmatrix}x_1(t)\\x_2(t)\\\vdots\\x_M(t)\end{bmatrix}=\begin{bmatrix}\sum_{i=1}^{d}g_1(\theta_i)s_i(t)\\\sum_{i=1}^{d}g_2(\theta_i)s_i(t-\frac{\Delta}{c}\sin\theta_i)\\\vdots\\\sum_{i=1}^{d}g_M(\theta_i)s_i(t-(M-1)\frac{\Delta}{c}\sin\theta_i)\end{bmatrix}+\begin{bmatrix}n_1(t)\\n_2(t)\\\vdots\\n_M(t)\end{bmatrix} \tag{17}$$

The signal empirical orthogonal function is decomposed on plane $t-\omega$, and output is:

$$\tau_m(\theta_i)=(m-1)\tau_0(\theta_i)=(m-1)\frac{\Delta}{c}\sin\theta_i\quad(m=1,2,\cdots,M) \tag{18}$$

where $\tau_0(\theta_i)=\frac{\Delta}{c}\sin\theta_i$ is energy distribution characteristic function decomposed by empirical orthogonal function. And $c$ is a test statistic.

### *3.2 The second order matching filter of intrusion signals*

In order to realise purification and recognition of network intrusion signals in a small area, matching filter is carried out to the spectrum characteristic quantity of the intrusion signals obtained above, to improve the anti-interference ability of the algorithm, so as to increase the precision of purification and recognition of network intrusion signals.

Input spectrum characteristic quantity into the second order lattice matching filter to purify signals in a small area. The system transfer function of the second order matching filter is:

$$H_B(z)=\frac{(1+\sin\theta_2)}{\cos\theta_2}\frac{\cos\theta_1(k)\cos\theta_2z^{-1}}{1+\sin\theta_1(k)(1+\sin\theta_2)z^{-1}+\sin\theta_2z^{-2}}G(z) \tag{19}$$

where

$$G(z)=\frac{1-\sin\theta_2}{2}\frac{1-z^{-2}}{1+\sin\theta_1(k)(1+\sin\theta_2)z^{-1}+\sin\theta_2 z^{-2}} \quad (20)$$

The iterative formula of the filter tap coefficient is :

$$\theta_1(k+1)=\theta_1(k)-\mu\,\mathrm{Re}[y(k)\varphi^*(k)] \quad (21)$$

where $\mu$ is the modulated frequency of windowed Fourier spectrum, known as step size (Jyothi et al., 2015); $\varphi(k)$ is the amplitude-frequency response of the output purified signal $y(k)$ to the tap coefficient$\theta_1(k)$. The filtering output of the intrusion signals is:

$$x'=\sum_{v=1}^{V}b_v\bullet IFFT\{X_v\}=\sum_{v=1}^{V}b_v x_v \quad (22)$$

The expected output impulse response function of the signals is:

$$X'=\sum_{v=1}^{V}b_v X_v \quad (23)$$

Input spectrum characteristic quantity into the second order lattice matching filter to purify the signals in a small area (Tang et al., 2016; Hamid, 2016; Ponomarev and Atkison, 2017), to filter the coherent colour noise and improve the distinguishable ability of the signals. Input spectrum characteristic quantity $x(k-1),\ldots,x(k-M)$ (Han et al., 2016) of intrusion signals into $M$ tap nodes of the filter, and calculate the time-frequency distribution cross-term of intrusion signals:

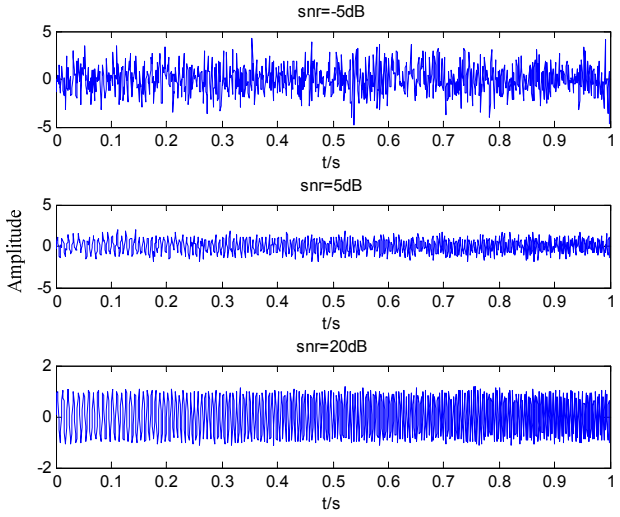
$$x_k=\sum_{n=0}^{N-1}C_n\cdot e^{j2\pi kn/N}\qquad k=0,1,\cdots,N-1 \quad (24)$$

According to the calculated time-frequency distribution cross-term, the adaptive weighting method is adopted to adjust the filter tap coefficient, which can independently adapt to the spectrum and bandwidth of the inputted network intrusion signals, and realise purification and recognition of network intrusion signals in a small area and improve the self-adaptability of the purification and recognition of network intrusion signals. During it, the spectrum characteristic quantity is input into the second order lattice matching filter for purification of signals in small area, which can effectively improve the distinguished ability of signals, improve the accuracy of purification and identification of network intrusion signals when strengthening the anti-interference ability of the signals.

## 4 Simulation experiment and analysis

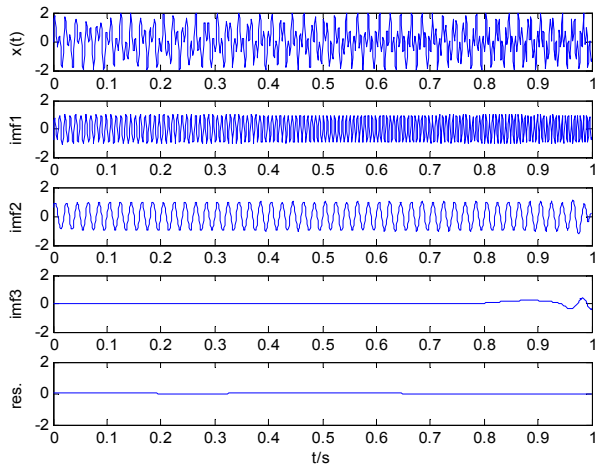
In order to test the application performance of this method in the small area network intrusion signal purification and recognition, select an actual gateway data in Data.gov (https://www.data.gov/), and input the experimental data into simulation system for display. The experiment is designed with Matlab and Visual C ++ simulation tools. In the experiment, the network intrusion signals are simulated by superimposing a sine signal and a sine frequency modulation signal; the fundamental frequency of the network intrusion signals is 150 Hz; the frequency of the frequency modulation is changed between [30 Hz, 80 Hz]; the fading spectral bandwidth of illusive component is 20 dB; the interference signal to noise ratio is –10~10 dB; the filter order is 2; the phase offset is 0.23 and the interference noise is the colour noise with a variance of 0.5. Based on the above simulation parameter settings, simulation and analysis are carried out to the small area purification and recognition of network intrusion signals. Firstly, crude sampling is carried out to network transmission data. The sampling frequency is 21 KHz; the sampling duration is 1200 s; the number of data samples is 1024. When the signal to noise ratio are –5 dB, 5 dB and 20 dB respectively, the result of crude sampling is obtained as shown in Figure 2.

**Figure 2** Input of primary signals




The network intrusion signals shown in Figure 2 are taken as a sample, and the method proposed in this paper is adopted for signal purification. First, the time-scale decomposition is performed, and then the decomposition result is obtained as shown in Figure 3.

**Figure 3** Result of time-scale decomposition of network intrusion signals



On this basis, the decomposed signal is input into the filter to achieve intrusion signal purification and recognition. The recognition result is shown in Figure 4.

**Figure 4** Output of intrusion signal purification and recognition

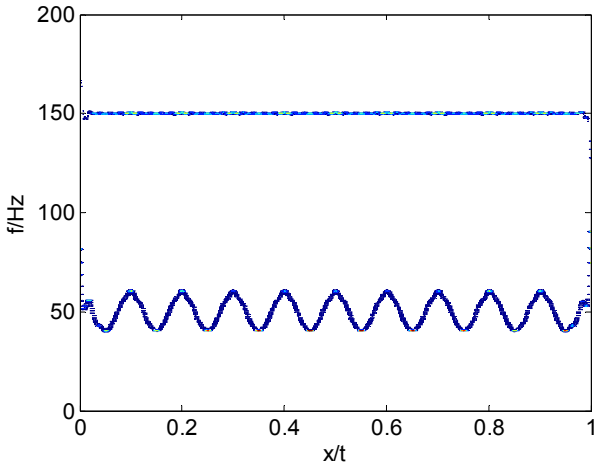
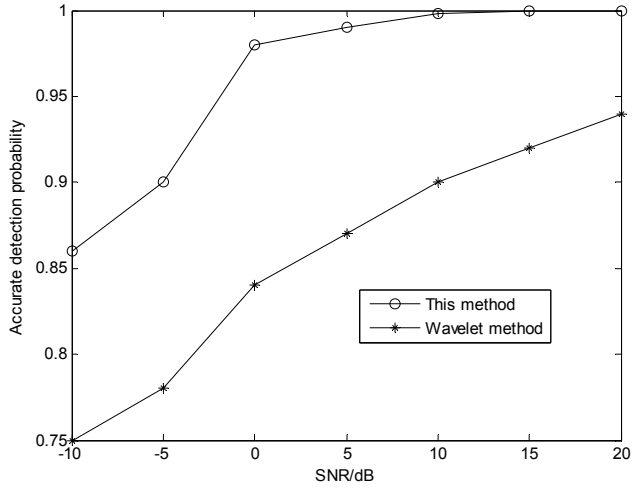



**Figure 5** Comparison in intrusion signal detection accuracy probability




The analysis of Figure 4 shows that the method proposed in this paper can accurately recover two groups of component information of network intrusion signal: sinusoidal signal and sinusoidal frequency modulation signal. The signal fluctuation amplitude is relatively stable, which shows that the method can provide good signal purification performance and strong resolution.

In order to compare the detection performance of the algorithm, the method proposed in this paper is compared with the wavelet detection method, and the detection performance curve of the network intrusion signal is obtained, as shown in Figure 5. The analysis in Figure 5 shows that with the increase of signal-to-noise ratio, the detection accuracy of network intrusion signals provided by the proposed method and wavelet detection method has been improved. However, the maximum accuracy of wavelet detection method is 94%, and the minimum value is 75%. When the signal-to-noise ratio is 10 dB or greater, the minimum accuracy of the method proposed in this paper is 86%, and its accuracy can reach 100%. The results show that the method proposed in this paper can provide higher detection accuracy and better performance in network intrusion signal recognition.

## 5 Conclusion

1 The active detection of network attacks is based on the detection and recognition of network intrusion signals. In order to improve network security and detect and recognise network intrusion signals, a method of small area purification and recognition of network intrusion signals based on the second order matching filter detection is proposed in this paper.

2 Signals are converted from time domain to frequency domain based on time-frequency analysis. The Hilbert-Huang transform method is adopted for time delay scale decomposition of network intrusion signals in a small area, and the second order lattice matching filter is constructed to purify signals in a small area, to filter the coherent color noise and improve the distinguishable ability of the signals.

3 The research shows that in small area purification and recognition to network intrusion signals, the method proposed in this paper can accurately recover two sets of component information of network intrusion signals, the sinusoidal signals and sine frequency modulation signals and give rise to a stable signal fluctuation range, which indicates that with this method, the signal purification performance is good, the distinguishable ability is strong, and the detection ability to intrusion signals can be improved. When the signal-to-noise ratio reaches 10 db or above, with the method proposed in this paper, the accuracy of recognising network intrusion signals can reach 100%, so the proposed method has a good application value in network security.

## References

Chen, Z.W., Huang, X.W., Chen, Z.X., Zhao, Z.Z. and Huang, L.F. (2017) 'Non-dominated sorting cloud model algorithm for interval multi-objective optimization', *CEA*, Vol. 53, No. 22, pp.143–149.

Dong, G.L., Ryu, K.S., Bashir, M. et al. (2013) 'Discovering medical knowledge using association rule mining in young adults with acute myocardial infarction', *Journal of Medical Systems*, Vol. 37, No. 2, pp.1–10.

Dou, H.J., Wang, Q.L. and Zhang, X. (2016) 'A joint estimation algorithm of TDOA and FDOA based on wavelet threshold de-noising and conjugate fuzzy function', *JEIT*, Vol. 38, No. 5, pp.1123–1128.

Gu, Y.L. (2017) 'Simulation of network intrusion detection and extraction based on large data driven', *Computer Simulation*, Vol. 34, No. 9, pp.370–373.

Guan, Y.Q., Zhao, X.S., Wang, P.F. and Li, D.P. (2016) 'Parallel algorithm for massive point cloud simplification based on slicing principle', *Journal of Computer Applications*, Vol. 36, No. 7, pp.1793–1796.

Hamid, Y. (2016) 'A fusion of feature extraction and feature selection technique for network intrusion detection', *International Journal of Security & Its Applications*, Vol. 10, No. 8, pp.151–158.

Han, X., Xu, L., Ren, M. et al. (2016) 'A Naive Bayesian network intrusion detection algorithm based on principal component analysis', *International Conference on Information Technology in Medicine and Education. IEEE*, Vol. 35, No. 17, pp.325–328.

Hsieh, T.J. (2014) 'A bacterial gene recombination algorithm for solving constrained optimization problems', *Applied Mathematics and Computation*, Vol. 231, No. 15, pp.187–204.

Jyothi, V., Addepalli, S.K. and Karri, R. (2015) 'Deep packet field extraction engine (DPFEE): a pre-processor for network intrusion detection and denial-of-service detection systems', *IEEE International Conference on Computer Design. IEEE*, Vol. 3, No. 11, pp.266–272.

Keshavamurthy, B.N., Khan, A.M. and Toshniwal, D. (2013) 'Privacy preserving association rule mining over distributed databases using genetic algorithm', *Neural Computing & Applications*, Vol. 22, No. 1, pp.351–364.

Khalili, A. and Sami, A. (2015) 'SysDetect:a systematic approach to critical state determination for industrial intrusion detection systems using Apriori algorithm', *Journal of Process Control*, Vol. 15, No. 2776, pp.154–160.

Mernik, M., Liu, S.H., Karaboga, M.D. et al. (2015) 'On clarifying misconceptions when comparing variants of the Artificial Bee Colony Algorithm by offering a new implementation', *Information Sciences*, Vol. 291, No. 10, pp.115–127.

Mi, J., Zhang, P. and Yu, H.P. (2016) 'Large data clustering algorithm based on particle swarm differential perturbation optimization', *Journal of Henan University of Engineering (Natural Science Edition)*, Vol. 28, No. 1, pp.63–68.

Moradi, M. and Keyvanpour, M.R. (2015) 'An analytical review of XML association rules mining', *Artificial Intelligence Review*, Vol. 43, No. 2, pp.277–300.

Pattewar, T.M. and Sonawane, H.A. (2016) 'Neural network based intrusion detection using Bayesian with PCA and KPCA feature extraction', *IEEE International Conference on Computer Graphics, Vision and Information Security. IEEE*, Vol. 12, No. 9, pp.83–88.

Ponomarev, S. and Atkison, T. (2017) 'Session duration based feature extraction for network intrusion detection in control system networks', *International Conference on Computational Science and Computational Intelligence. IEEE*, Vol. 32, No. 14, pp.892–896.

Tang, J., Zhuo, L., Jia, M. et al. (2016) 'Supervised nonlinear latent feature extraction and regularized random weights neural network modeling for intrusion detection system', *International Conference on Cloud Computing and Security*, Vol. 16, No. 12, pp.343–354.

Xu, G. and Cheng, X.J. (2013) 'Adaptive reduction algorithm of scattered point clouds based on wavelet technology', *Journal of Tongji University (Natural Science)*, Vol. 41, No. 11, pp.1738–1743.

Zhang, W.M. and Chen, Q.Z. (2014) 'Network intrusion detection algorithm based on HHT with shift hierarchical control', *Computer Science*, Vol. 41, No. 12, pp.107–111.

Zhou, X. and Peng, Q.H. (2015) 'Network intrusion detection based on local features of signal compression sampling', *Bulletin of Science and Technology*, Vol. 32, No. 6, pp.220–222.