Study on Effective Detection Method of Large Random Network Intrusion Signal

Dai Jiapeng

(Department of Science and Technology Guizhou Radio & TV University Guiyang,Guiyang,550004, China)

Keywords: network intrusion; signal detection; wavelet transform

Abstract: In the detection process of large random network intrusion signal, the signal detection method is key to guarantee the network security, the traditional detection method is simple, time-consuming, and the error is big, the detection precision is low. In view of this situation, a ORB wave intrusion signal detection method is proposed based on three B spline wavelet transform, discrete orthogonal wavelet filtering algorithm is used for decomposition filtering, according to the relationship between wavelet transform and signal singularity, the signal processing method is used for intrusion signal detection, time-frequency analysis is taken for intrusion signal, by extracting the characteristics of the signal, distinguish the jamming signal characteristics of intrinsic signal characterization, the R wave peak is recognized in 2^3 scale, the starting point and end point of QRS wave are detected in the 2^1scale, for each intrusion signal, IMF spectrum analysis with Hilbert transform is taken for mode decomposition, and the network intrusion database is used in simulation. Simulation results show that this algorithm can improve the detection accuracy, and effectively improve the work efficiency in network security defense.

1. Introduction

With the development of computer technology, the rapid development of information technology, network data security issue is increasingly prominent, with the escalation of network invasion and anti invasion against for network intrusion, network intrusion shows diversified forms and frequent development trend, and network intrusion signals are implanted trojan virus, through persistent attacks on the network and computer terminal, tampering and theft of user information are obtained, cause the system to collapse, so the situation network security is serious, network security is related to all aspects of people's life and production, it needs for an efficient intrusion detection and filtering separation method, the intrusion signal interception should be realized, and a more effective network intrusion detection algorithm should be researched, and it is necessary to improve the detection performance, so as to improve network security, ensure the stability of the system. The network intrusion detection and attacking signal detection plays an important role in network security area[1].

In recent years, the detection of large random network intrusion signal gradually comes into people's research fields, especially with the increasingly rampant Internet attacks, modern signal processing technology is introduced, and the research of network intrusion detection has become the focus of research in the field of network security[2], traditionally, traditional methods mainly use the intrusion signal detection based on time-frequency analysis algorithm and signal detection algorithm based on nonlinear time series analysis, where, in reference [3], the interference attack localization method was proposed to optimize the intrusion tolerant system state transfer characteristics, the quantitative analysis of path of the virus intrusion was obtained, and the hierarchical structure of the characteristics of the potential intrusion signal decomposition was used to improve the detection performance, however, the algorithm could not effectively avoid the interplay between network defensive measures, resulting in intrusion signal detection effect was not good in low SNR, the security of the system was limited. In reference [4], it proposed an algorithm of intrusion detection data stream classification and fractal dimension analysis based on DoS classification, improved classification attribute of virus and clutter signal, improve the clustering

ability, realize virus immunity against aggression. The algorithm had two stages in training and testing in the implementation process, each stage required the communication flow characteristics of information read virus, so it had high computational complexity, and poor real-time, it was difficult to implement in fact. According to the problems as above, the detection algorithm is improved in this paper[5,6], and a ORB wave intrusion signal detection method is proposed based on three B spline wavelet transform, discrete orthogonal wavelet filtering algorithm is used for decomposition filtering, according to the relationship between wavelet transform and signal singularity, the signal processing method is used for intrusion signal detection, time-frequency analysis is taken for intrusion signal, by extracting the characteristics of the signal, distinguish the jamming signal characteristics of intrinsic signal characterization, the R wave peak is recognized in 2^3 scale, the starting point and end point of QRS wave are detected in the 2^1 scale, for each intrusion signal, IMF spectrum analysis with Hilbert transform is taken for mode decomposition, and the network intrusion database is used in simulation. Simulation results show that this algorithm can improve the detection accuracy, and effectively improve the work efficiency in network security defense. It will have good application value in practice.

2. Intrusion signal detection method of large randomized network

2.1 Intrusion signal model and problem description

In the research of intrusion signal detection method of large randomized network, the first step is to construct the signal model, the signal processing method is taken for intrusion signal detection, assumed there are M full direction of intrusion signals, and there are a mathematical expectation signal A_c and P interference signals, the interference signals are input to the network intrusion detection system with angles $\theta_0, \theta_1, ..., \theta_P$. The construction of near field source network intrusion signal array is shown in Figure 1.

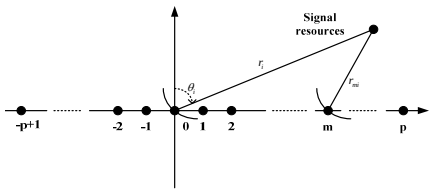

Figure 1. Network intrusion signal model

In the figure 1, construct the matrix vector columns in Z matrix, independent group is composed of matrix Z^m with rank $n+t$, then the network intrusion model state transition equation is expressed as:

$$x(n) = s(n) + v(n) = \omega_{k-1}^{(i)} \frac{p\left(y_k \mid X_k^{(i)}, Y_{k-1}\right) p\left(x_k^{(i)} \mid X_{k-1}^{(i)}, Y_{k-1}\right)}{q(x_k^{(i)} \mid .)} \tag{1}$$

In the formula, $s(n)$ is the intrusion signal, $v(n)$ is the color noise component, φ_i shows the non steady instantaneous frequency estimation value of signal. The intrusion signal is processed with time-frequency analysis, by extracting the characteristics of the volume, and can distinguish the interference signal characteristics of the internal nature of the signal, with the Fourier transform, signal is transited from time domain to the frequency domain, and with the Fourier inversion transform, the signal is transited from frequency domain to time domain, and its expression is

$$s(t) = \frac{1}{2\pi} \int_{-\infty}^{\infty} S(f) e^{j2\pi ft} df \tag{2}$$

Given a binary network intrusion feature vector set, it is expressed as:

$$F = \{ f_1, f_2, \cdots, f_n \} \tag{3}$$

Calculate the adaptive power spectral density feature of the signal intrusion, get the information capacity of the network virus mutates, the estimation result is:

$$x(t) = \sum_{i=0}^{p} a(\theta_i) s_i(t) + n(t) \tag{4}$$

In the formula, $a(\theta_i)$ is the value of large randomized network link layer, $s_i(t)$ said signal component characteristics, and $n(t)$ is noise signal.

Large random network intrusion signal detection process is an iterative process, because the virus is hidden in the nonlinear characteristics environment, assuming that capture data desired signal and P interference signal is input o the firewall detection system with angle t$\theta_0, \theta_1, \ldots, \theta_P$, realize the stability control of the network, analytical model of intrusion signal is obtained as:

$$z(t) = x(t) + iy(t) = a(t)e^{i\theta(t)} \tag{7}$$

In the formula, $z(t)$ is the capture data, $x(t)$ is the real feature of intrusion signal, and $\theta(t)$ is the high frequency component. In frequency domain, the signal $s(t)$ is continuous signal, definition of time frequency distribution can be described as:

$$P(t, f) = \int_{-\infty}^{\infty} s(u + \frac{\tau}{2}) s^*(u - \frac{\tau}{2}) \alpha(\tau, v) e^{-j2\pi(vt + f\tau - vu)} du dv d\tau \tag{8}$$

Through the above analysis, the network intrusion signal model is obtained, it can provide the basic signal model for network intrusion detection.

2.2 Intrusion signal detection principle of large randomized network

In a large random network intrusion signal detection process, according to the intrusion signal, the wavelet transform correlation filter is used to filter the signal, scale series increased with 2 growth in the number of data points$\left(a_0 = 2, a = 2^j\right)$, the level is constructed respectively for a data extraction, so as to realize wavelet transform. Using the time-frequency analysis method to construct the network intrusion signal constraints and characteristics, instantaneous frequency oscillation data is estimated as:

$$\hat{f}_i(n) = \frac{1}{2\pi} \sum_{i=0}^{p} i a_i n^{i-1} \tag{9}$$

WVD time-frequency distribution is combined with Hough transform, time-frequency analysis is carried out, and the feature extraction and signal filtering analysis of signal are taken in time-frequency domain, the objective function is generated by the contract matrix, which expressed as:

$$x_i = f_i(M, n, w, c, r) = \min\{f(M, n, w, c, r)\}, M - \sum_{j=1}^{\lfloor n/2 \rfloor} w_j - \sum_{j=\lfloor n/2 \rfloor + 1}^{i} w_j - \sum_{j=i+1}^{k} w_j > 0 \tag{10}$$

Wherein, $\theta_1(k)$ is the initial state vector, $\theta_1(k+1)$ is network state vector of two iterations, and then get the beam directivity for domain constraints:

$$\varphi_{mi} = \frac{2\pi r_i}{\lambda_i} \left(\sqrt{1 + \frac{m^2 d^2}{r_i^2} - \frac{2md \sin\theta_i}{r_i}} - 1 \right) \approx \gamma_i m + \phi_i m^2 \tag{11}$$

Where, $\gamma_i = -2\pi \frac{d}{\lambda_i} \sin\theta_i$, $\phi_i = \pi \frac{d^2}{\lambda_i r_i} \cos^2\theta_i$, d and λ_i meet $d \le \lambda_i / 4$, large random network intrusion signal $f(n)$ is taken with two discrete wavelet transform, Mallat algorithm is applied for computing, the digital filter is expressed as:

$$s_2^j f(n) = \sum_{k \in z} h_k s_2^{j-1} f\left(n - 2^{j-1} k\right) \quad , \quad w_2^j f(n) = \sum_{k \in z} g_k s_2^{j-1} f\left(n - 2^{j-1} k\right) \tag{12}$$

In the formulas, $s_2^0 f(n)$ is the singular signal in large random network, $w_2^j f(n)$ is the wavelet coefficient, and it is the wavelet transform of $f(n)$, it can get the following results:

$$s_2^j f(n) = f(n).\phi_2^j(n) \tag{13}$$

Where, $s_2^j f(n)$ is the scale coefficient, ϕ is called scaling function, h_k and g_k are the orthogonal digital low-pass filter and high pass filter $H(\varpi)$ coefficients, which is composed of basic wavelet and scale function to decide. The intrusion signal is detected as:

$$R_s^{(0)} = \sum_{n=0}^{k} \left\langle R_s^{(n)}, d_{\gamma n} \right\rangle d_{\gamma n} + R_s^{(k+1)} \tag{14}$$

According to the detection model and detection algorithm principle, the signal feature extraction and intrusion detection are obtained, and large random network intrusion signal detection system structure diagram is shown in Figure 2.

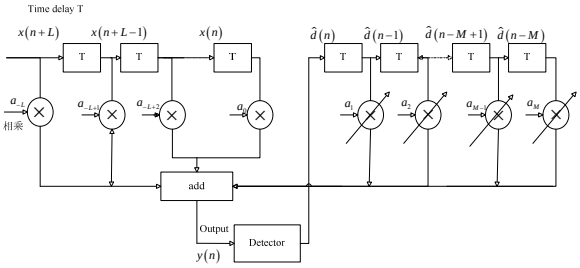

Figure 2. Intrusion signal detection system structure diagram

3. Key technology to realize the detection algorithm

In the large random network, the intrusion signal detection uses the signal singularity location and classification for location and amplitude information of the signal with wavelet transform, its essence is the use of signal and noise in different frequency band energy distribution for the location of singular points, different distribution uses energy in the frequency band to distinguish singular point types. The research shows that the starting point and end point of QRS wave corresponding to the maximum value, the transform of opposite sign mode has small deviation, the error $j \prec 4$. The key technology of large random network intrusion signal detection with application of wavelet transform is wavelet function structure and characteristic scale selection, and the design of anti-interference. In large random network intrusion signal detection process, *Mexicanhat* and spline wavelet base on R wave have good detection perspective with high accuracy, line wavelet is better than $H(\varpi)Mexi-canhat$ wavelet base, but *Mexicanhat* is not orthogonal wavelet, we can only use discrete wavelet transform algorithm for detection, real-time performance is bad, and programming has complexity, the effect is not very ideal, and the spline wavelet basis is orthogonal, we can use two wavelet algorithm to construct wavelet coefficients, regardless of the speed of calculation simplicity or programming point of view, the correspond constraints are shown as follows:

$$\left|\widehat{w}_f\right| \| \geq \lambda \qquad \left|\widehat{w}_f\right| \| \leq \lambda, \widehat{w}_f = \left\{\operatorname{sgn}(\widehat{w}_f)\left(\left|\widehat{w}_f\right| - \lambda\right), \left|\widehat{w}_f\right| \| \leq \lambda \right. \tag{15}$$

Where, $\widehat{w}_f$ is the wavelet coefficient threshold after denoising, wf is the wavelet coefficient, and λ is threshold value.

According to the empirical mode decomposition theory, $c_i(t)$ can be taken as a single component signal, when meet the inherent conditions of modal functions of the components, using the concept of instantaneous frequency of the signal $x(t)$ is expressed as:

$$x(t) = \operatorname{Re}\left[\sum_{i=1}^{n} a_i(t) e^{j\omega_i(t)}\right] = \operatorname{Re}\left[\sum_{i=1}^{n} a_i(t) e^{j\int \omega_i(t)dt}\right] \tag{16}$$

It reflects the relationship between the amplitude, time and frequency of the signal, the amplitude of network intrusion signal can be expressed as a function $H(\omega,t)$ of time t and frequency ω, the HHT spectrum with joint time frequency can be obtained as:

$$H(\omega,t) = \operatorname{Re}\sum_{i=1}^{n} a_i(t) e^{j\int \omega_i(t)dt} \tag{17}$$

Then, the R wave peak is recognized in 2^3 scale, the starting point and end point of QRS wave are detected in the 2^1 scale, for each intrusion signal, IMF spectrum analysis with Hilbert transform is taken for mode decomposition, the detection algorithm is improved.

4. Simulation results and analysis

In order to prove the superiority of this algorithm, we need for an experiment. The DAPRPA intrusion data from the MIT Lincoln Laboratory are taken in simulation experiment as sample data, two kinds of intrusion behaviors respectively are called as ipsweep and Smurf, testing the algorithm on detection ability in low SNR, experimental parameters of the sample are selected, legal network information number is 1024, the access number is 10256 times, e intrusion signal sample number is 238, the center frequency $f_0 = 1000$ Hz, and the discrete sampling rate $f_s = 10 * f_0 \text{Hz} = 10\text{KHz}$, bandwidth $B = 1000$ Hz, sampling points $N = 201$, the network intrusion signal waveform in time domain is shown in Figure 3.

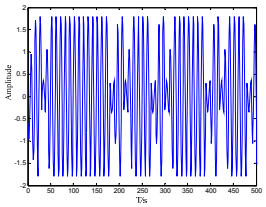

Figure 3. Network intrusion signal waveform in time domain

The signal waveform is taken as object detection for intrusion detection, in the process of the experiment, using the traditional signal intrusion detection method and 3 B spline wavelet transform algorithm for intrusion detection experiments, spectrum signal detection is shown in Figure 4. It can be seen from the diagram, using this method, can effectively realize the network intrusion detection, peak search is significantly, and it as higher detection performance.

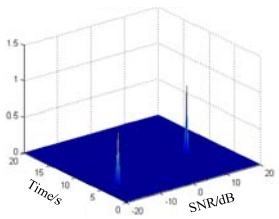

Figure 4. Analysis of detection spectrum of intrusion signal comparison

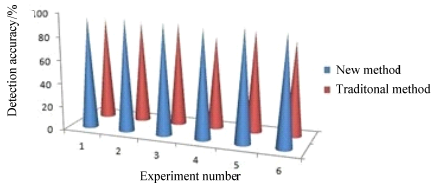

Figure 5. Detection accuracy

In order to test the accuracy of the method in this paper, 2000 Monte-Carlo experiments are taken, and the detection performance analysis results are shown in Figure 5 and Table 1.

Table 1.Detection accuracy comparison

Number of experiments (time)	Accuracy of new algorithm/%	Accuracy of traditional algorithm/%
1	95	88
2	96	87
3	95	88
4	93	79
5	96	87
6	94	80

From the simulation results, it shows that the new algorithm has better detection performance, the detection accuracy is better than traditional method, so it has good performance in large randomized network intrusion detection.

5. Conclusions

In the detection process of large random network intrusion signal, the signal detection method is key to guarantee the network security, the traditional detection method is simple, time-consuming, and the error is big, the detection precision is low. In view of this situation, a ORB wave intrusion

signal detection method is proposed based on three B spline wavelet transform, discrete orthogonal wavelet filtering algorithm is used for decomposition filtering, according to the relationship between wavelet transform and signal singularity, the signal processing method is used for intrusion signal detection, time-frequency analysis is taken for intrusion signal. Simulation results show that this algorithm can improve the detection accuracy, and it has good application value in practice.

References

[1] Rao Yutai,Yang fan.Network Intrusion Stir the Network Instability Control Methods of the Research[J].Bulletin of Science and Technology,2014,30(1):185-188.

[2] Ye Qing,Huang Yanlei.Non-uniform Distribution Intrusion Detection Research and Simulation of the Model[J].Bulletin of Science and Technology.2013; 29(8): 169-171.

[3] ZHANG Ren-shang. Network Intrusion Detection System Based on Expert System and Neural Network[J].Computer Simulation.2012, 29(9): 162-165.

[4] PU Baoxing, ZHAO Chenglin. Tradeoff between multicast rate and number of coding nodes based on network coding. Journal of Computer Applications, 2015, 35(4): 929-933.

[5] WU Chun-qiong.Network Intrusion Detection Model Based on Feature Selection[J].Computer Simulation.2012; 29(6): 136-139.

[6] ZHANG Wumei, CHEN Qingzhang. Network Intrusion Detection Algorithm Based on HHT with Shift Hierarchical Control[J]. Computer science, 2014,41(12):107-111.