Attack Detection Algorithm Based on Rossle Chaotic Average Mutual Information Feature Mining

Liu Zai-ying [1], Zhou Ming-sheng [2]

[1] College of Information Science and Technology, Sanda University, Shanghai 201209, China;

[2] *School of Information Management and Engineering*, Shanghai University of Finance and Economics, Shanghai 200433, China.

Abstract **- chaotic systems combined with Gauss mixture model to achieve synchronic control detection is often used in traditional network attack detection methods, and the effect of detection is good when the attack signal to be detected has Gauss linear features. As the cyber-attack signals develop toward nonlinear random sequence, traditional detection models cannot achieve effective attack detection. A potential mining algorithm of average mutual information feature based on Rossle chaotic model is proposed, and according to the nonlinearity feature solution of the mutual information, the realization of effective detection of cyber-attack signals with stochastic nonlinear characteristics is obtained. On the basis of the foundation model of Rossle chaotic system, design an adaptive cascade notch filter which can remove multiple known interference frequency with the minimum mean square error criterion, realize the filtering pretreatment of the attack signals, extracting of Rossle nonlinear mutual information feature of the network data flow to be detected, and accomplish feature mining and detection of cyber-attack signals. Simulation results show that the detection performance is improved obviously, and the probability of detection reaches 98.7%, which appears superior performance of detection and value of network security defense.**

Keywords - chaotic; mutual information feature; detection; data mining

I. INTRODUCTIONS

With the growing popularity and development of computer network technology, Internet has become the main tool of human communication and production life. A variety of data and information has been constantly transmitting and sharing in the network, with which problems of computer network are brought about at the same time[1]. Currently, signals of network attacks tend to concealment and nonlinear randomization, and using conventional algorithm of network attack detection to achieve effective attack detection has been increasingly difficult. Of traditional methods, attack detection can be divided into expert knowledge abusing detection and abnormal behavior detection, and the foundation of research on attack detection systems is the applications of digital signals in the area of security, as well as promotion of signal and information processing disciplines and development of modern network security disciplines. From the aspects of data analysis and means of signal processing, the abusing detection technology sets up a database of attack mode first, when the signals and information of the system or users' mode of behavior are detected a matching correlation with records in the database, then the behavior or these data information can be considered to be attack. On the contrary, it is considered to be legitimate. The advantages of this method are easy to implement and high accuracy [2]. The disadvantage is weak openness, and new attack information outside the database category cannot be detected, and its effectiveness heavily depends on the update of the expert database, what's more, in reality, this update is often delayed and cannot effectively update and implement the selection and matching of the feature of attack database [3].

Traditional proactive detection method of network attacks uses a combination of chaotic systems and Gaussian mixture model to implement synchronic control detection algorithm, and the effect of detection is good when the attack signal to be detected has Gauss linear features. As the cyber-attack signals develop toward nonlinear random sequence, traditional detection models cannot achieve effective attack detection [4-5].

To solve these problems, this paper has proposed a potential mining algorithm of average mutual information feature based on Rossle chaotic model, and simulation results show that the detection algorithm has superior detection performance in covert network attack detection, and can achieve quick and accurate detection of weak attack signals at very low signal to noise ratio, which ensures security of network.

II. CHAOTIC SYSTEM MODEL FOR ROSSLE CYBER-ATTACKS SIGNAL

A. Building of Chaos Model and Analysis of Chaotic Time Series

In the field of signal detection of network attacks, theories of traditional network attacks signal processing is to assume that the research signal, namely, time series is linear or Gaussian, although this assumption of linearity and Gaussian is beneficial to the development and realization of signal processing, but after all, various types of signals acquired in reality, especially time series of cyber-attacks signals has more or less a certain nonlinear components. Presence of this ingredient may not hinder people from studying the original time series, on the contrary, through analysis of nonlinear time series and chaotic method [6-8], the essential characteristics of truly acquired signal can be effectively discovered. Traditional proactive detection method of network attacks uses a combination of chaotic systems and Gaussian mixture model to implement synchronic control detection algorithm, which cannot effectively meet the trend that cyber-attack signals exhibit the nature of nonlinear and non-Gaussian, so this paper adopts nonlinear time series analysis method for signal detection, firstly building chaotic system model for Rossle cyber-attacks signals. The detection method employs Rossle chaotic system of chaotic synchronization, and Rossle chaotic system is a typical three-dimension continuous autonomous system, whose mathematical model is expressed as:

$$\begin{cases} \dot{x} = -\sigma x + \sigma y \\ \dot{y} = -xz + rx - y \\ \dot{z} = xy - bz \end{cases} \tag{1}$$

In Rossle chaotic system above, taking parameter σ = 10, r = 28, b = 8/3, using the fourth-order Runge-Kutta method to solve equation (16), doing 10,000 times iteration, phase space reconstruction is needed to carry out firstly to study of chaotic sequence, use C-C algorithm to obtain the optimal time-delay and the minimum embedding dimension of phase space reconstruction, achieving the phase space reconstruction of the feature set of network status in the chaotic system, assuming that a given binary feature vector set of network intrusion state is expressed as:

$$F = \{ f_1, f_2, \cdots, f_n \} \tag{2}$$

Embed the feature state vector of network intrusion mentioned above into Rossle chaotic system, building a objective function of network intrusion characteristics, which is expressed as:

$$\theta_1(k+1) = \theta_1(k) - \mu \operatorname{Re}[y(k)\varphi^*(k)] \tag{3}$$

In the formula above, $\theta_1(k)$ represents the vector of initial state, and $\theta_1(k+1)$ indicates the network state vector of second iteration, and μ is the contraction coefficient of the phase space reconstruction of the chaotic sequence. Through the objective function constructed above, the curve of delay parameter variation obtained by C-C algorithm in Rossle chaotic system described above is shown in Figure 1, which indicates that the optimal delay parameter is 20, so as to lay the data foundation of further building the feature space of network status. According to the model constructed above and parameters striking, the analysis principle of detection model of cyber-attack based on Rossle chaotic model is established.

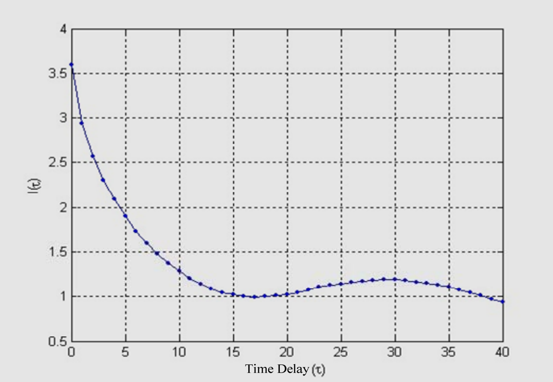

Fig. 1 Curve of delay parameter variation in Rossle chaotic system.

1.2 –B. Filter Preprocessing of Cyber-Attacks Signal

Based on the foundation model according to Rossle chaotic system above, design a cascaded adaptive notch filter ruled by minimum mean square error criterion which can remove a number of known interference frequency components to achieve filtering pretreatment of the attack signals, and the algorithm is described as follows:

In Rossle chaotic system, cyber-attack signals intervenes, the attack model is a nonlinear time series, which is expressed as:

$$F(z) = \frac{\sqrt{1-b^2}}{1-bz^{-1}}, -1 < b < 1 \tag{4}$$

The formula above is the result of first-order regression model analysis of cyber-attack nonlinear signals, and the transfer function of the cascade filter is obtained as:

$$\phi(z) = F(z)F(z^{-1})\sigma_n^2 \tag{5}$$

Using minimum mean square error criterion, the real part $n_r(k)$ and imaginary part $n_i(k)$ of input cyber-attack signal $n(k)$ are independent white noise, and mean of both are zero and variance of both are σ_n^2 . Under the premise of ensuring the convergence probability of mean square error minimum, the average length of parameters iterations of Rossle chaotic system of the attack process of cyber-attack signal obtained is required to meet:

$$\operatorname{Re} \mathrm{E}[n_1(k)n_2^*(k)] = 0 \tag{6}$$

Based on minimum mean square error criterion above, design a cascaded adaptive notch filter ruled by minimum mean square error criterion which can remove a number of known interference frequency components, and the design diagram is shown in Figure 2.

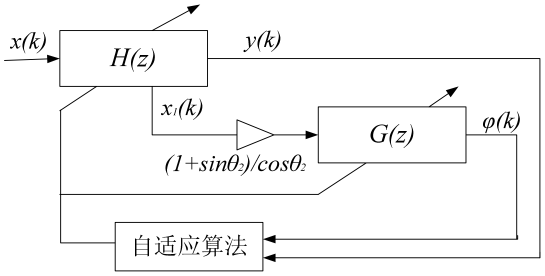

Fig. 2 Design diagram of adaptive cascade notch filter

In Rossle chaotic system model, a simplified gradient algorithm is introduced, and convergence curve of output response function of cyber-attack model is shown in Figure 3, from which we can see an adaptive cascaded notch filter, which can remove a plurality of interference frequency components known based on minimum mean square error criterion, has achieved the preprocessing of the attack signal and provided a source basis for the subsequent extraction of characteristics of the signal attack and finite detection attack signal.

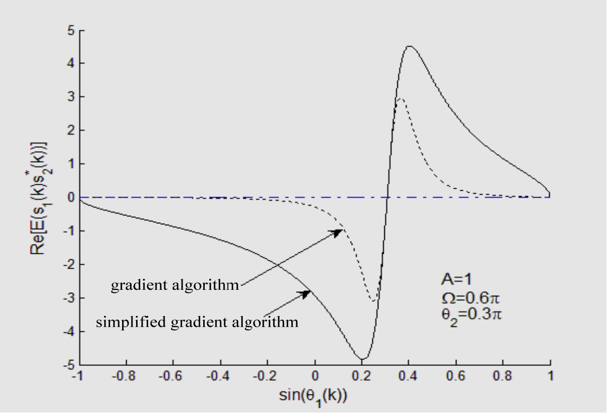

Fig. 3 Output response function of the adaptive cascade notch filter in cyber-attack model.

III. ATTACK DETECTION ALGORITHM

A. Introduction of Average Mutual Information Feature Mining Algorithm

Based on the model built above and signal preprocessing, extract the average mutual information characteristics of the attack signal under Rossle chaotic system model for signal detection, and the algorithm is described as follows:

In case that the monitoring data is incomplete, parameters estimation value is achieved through maximum likelihood estimation. The analysis above shows that the estimation value is very suitable for the detection and modeling of weak Trojan-attack characteristics. In the first place, using Gaussian mixture model for normal and legitimate network data modeling, three estimated parameters are obtained. Estimating the parameters which have been monitored to observe whether the attack was, intercept a while for data analysis. If there is no attack signal, the Rossle chaotic system can accurately calculate the three parameters of Gaussian mixture model. However, if there is disguised attack data, according to the relative difference of statistical characteristics, there will be a big gap between the estimated parameters and the normal parameters estimated. Because the mean feature vector μ can obviously reflect the characteristics of high-disguised attack data, the article chooses μ as the feature value for synchronic control amount introduced into the chaotic synchronization system for attack signature detection.

Assuming that $Z = (U,V)$ is a collection, which is consisted of network information data U and data that is not monitored V, thus, Z is called the complete data, and U is called incomplete data, and the joint probability density function Z is defined as: $p(U,V|\Theta)$, in which, Θ is the set of parameters to be estimated, the maximum value of maximum likelihood function $L(\Theta|U)$ of the incomplete data can be obtained through the maximum likelihood logarithm. As V is a continuous variable, then:

$$\begin{aligned} p(U,V|\Theta)L(\Theta|U) &= \log p(U|\Theta) \\ &= \int_V \log p(U,V|\Theta)dV \end{aligned} \tag{7}$$

By iteration of E steps and M steps, iterate the expectation value of average mutual information function $L_c(\Theta|Z)$ of the largest complete data to achieve the maximization of the log likelihood function $L(\Theta|Z)$ of the missing data, in which:

$$L_c(\Theta|Z) = \log p(U,V|\Theta) \tag{8}$$

In the iterative calculation, the estimated value $\Theta(t)$ of Θ is gained after the tth iteration, in the next iteration of the $t+1$ th time, the desired value of average mutual information function of the complete data is calculated by the iteration of E steps:

$$Q(\Theta|\Theta(t)) = E\left\{L_c(\Theta|Z)|U;\Theta(t)\right\} \tag{9}$$

Using iteration of M steps and multiple cyber-attack model adaptive cascade notch filter to remove interference frequency components known by us, and at last a new $\Theta(t+1)$ is achieved by maximizing the function $Q(\Theta|\Theta(t)) =$.

Suppose V is a behavior of cyber-attack and performs as random variable and discrete, and V satisfies the distribution function $[\delta_1,\delta_2,\cdots,\delta_N]$, in which, $\delta_i = p(V=i)$. Owing to:

$$\delta_k = G(V=k|U_i) \tag{10}$$

The type above represents that U_i is the probability by the kth multidimensional normal distribution, with the progress of the tth iteration, and δ_k becomes $\delta_{ik}(t)$:

$$\delta_{ik}(t) = G(V=k|U_i,\Theta(t)) \tag{11}$$

Here, the t+1 times estimation solves the global average mutual information feature vector of cyber-attack model under Rossle chaotic systems, and the process of iterative solution is:

$$\alpha_k(t+1) = \frac{1}{N}\sum_{i=1}^{N}\delta_{ik}(t) \tag{12}$$

$$\mu_k(t+1) = \frac{\sum_{i=1}^{N}\delta_{ik}(t)U_i}{\sum_{i=1}^{N}\delta_{ik}(t)} \tag{13}$$

$$\sum\nolimits_k(t+1) = \frac{\sum_{i=1}^{N}\delta_{ik}(t)(U_i-\mu_k(t+1)(U_i-\mu_k(t+1))^T}{\sum_{i=1}^{N}\delta_{ik}(t)} \tag{14}$$

In the formula above, U_i is the subset of the network feature, and μ_k is the inertia weight, and $\delta_{ik}(t)$ is the number of space dimension of chaotic phase space, and N is the number of step of iteration. Through the equation iteration above, adopt the proposed method based on Rossle chaotic model to realize the potential mining of the feature of average mutual information.

B. Attack Detection Algorithm Based on the Average Mutual Information Feature Mining Algorithms

Introduced by the algorithm above, on foundation of the achievement of mining of nonlinear cyber characteristics of average mutual information based on Rossle chaotic model, effectively detection of nonlinear cyber-attack signal which has the properties of nonlinear and stochastic is realized, the process is as follows:

Firstly, using a two-order cascaded notch filter which can extract a set of cyber signals in complex network background, based on the foundation model of Rossle chaotic system, design an adaptive cascaded notch filter which can remove a number of interference frequency components known by us ruled by minimum mean square error criterion for pretreatment, output signal is obtained as:

$$u(k) = \sum_{i=1}^{N} A_i \mathrm{e}^{\mathrm{j}(\Omega_i k+\theta_i)} + n(k) \tag{15}$$

Among them, $n(k)$ is the interference of network signal with legitimate background, and A_i is the number of cascade, setting the threshold of the generation system through the threshold set before as α_{FA}, which can be determined specifically based on the actual circumstances of network data and information flow. Finally, the data signal extracts the average mutual information feature of chaos through the method above, and compare the output data signal after chaotic synchronization processing with the threshold α_{FA}. The decision threshold can accurately determine whether the detected network signal is attack or legitimate, the guideline of judge is described as:

In case：

$$\begin{aligned} \dot{e} &= \dot{X} - \dot{Y} \\ &= \frac{Y_N(z)}{U(z)} = \prod_{i=1}^{N} H_i(z) \ge \alpha_{FA} \end{aligned} \tag{16}$$

Then judge the monitoring signal as attack signal; otherwise, the monitoring signal is a legitimate signal. Ultimately attack detection of cyber signal is achieved.

IV. SIMULATION RESULTS AND ANALYSIS

In order to verify the effectiveness of the proposed cyber-attack detection algorithm, this paper conducts the experiment through actual network signal acquisition and simulation tests. The experimental simulation environment is IntelCore3-530 1G memory, and the operating system is Windows XP, and the algorithms uses MATLAB programming implementation, and the network signal is acquired in KDD Cup2012 network virus database, and types of network attacks are DoS attacks, Probe attacks and ipsweep, and each class includes 50 samples, and each sample has four attributes, and the data set of attacks class is divided into three types, and each category includes 59, 71 and 48 samples, respectively, and each sample has 13 properties, setting the start and end of detection, continuously attacking computer systems and acquiring signal characteristics. The distribution of test samples is shown in Table 1.

TABLE 1. EXPERIMENTAL SAMPLE DISTRIBUTION OF CYBER-ATTACK SIGNAL

Type of attack	Normal sample	Sample of attack characteristics
DoS	2536	632
Probe	2365	325
ipsweep	3658	453

Under the circumstances of different characteristic subsets and cyber-attack samples, build the attack feature model through Rossle chaotic model to achieve effective detection of cyber-attack signal with nonlinear stochastic characteristics. Wherein the original data sequence of a set of samples acquired is shown in Figure 4.

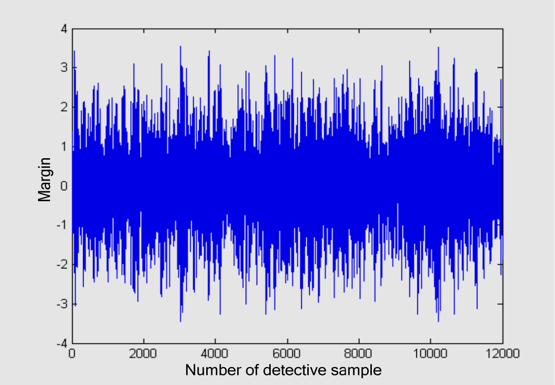

Fig. 4 Original sample of cyber-attack

Design an adaptive cascade notch filter ruled by minimum mean square error criterion for signal preprocessing, and the output of the filter obtained is shown in Figure 5.

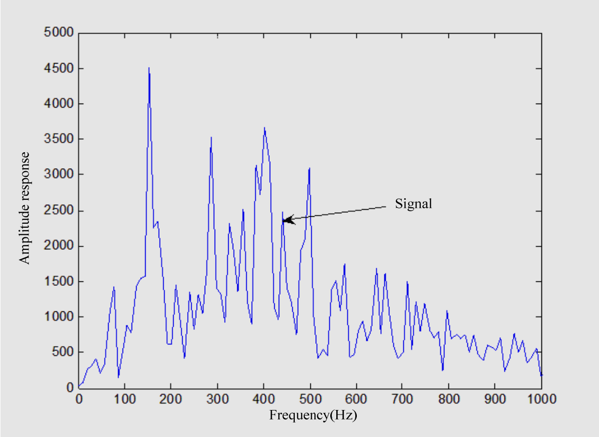

Fig. 5 Output of preprocessing by the adaptive cascade notch filter

Finally, through extracting Rossle chaotic nonlinear characteristics of mutual information of network data stream to be detected to realize the feature digging and testing of cyber-attack signals, the spectrum of attack signals is shown in Figure 6. Monte Carlo experiment is performed to multiple sets of attack samples acquired in experiments, and the probability of detection is 98.7%, showing superior detection performance of the algorithm, which can accurately and effectively position and detect attack signals.

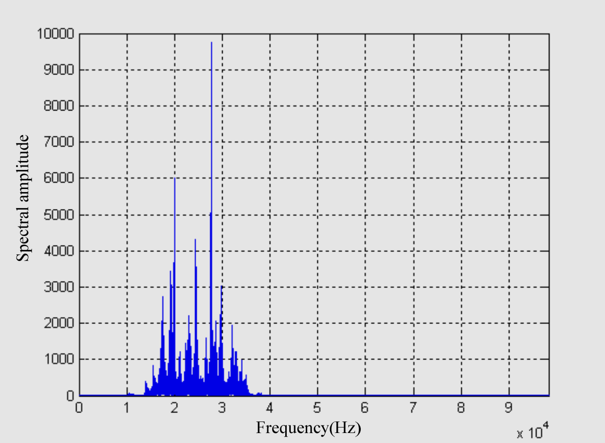

Fig. 6 Spectrum analysis of detection results

In order to further validate the superiority of the proposed method, according to three types of the data sets, randomly select 10 data for attack accuracy detection, the results of accuracy of detection is shown in Figure 7.

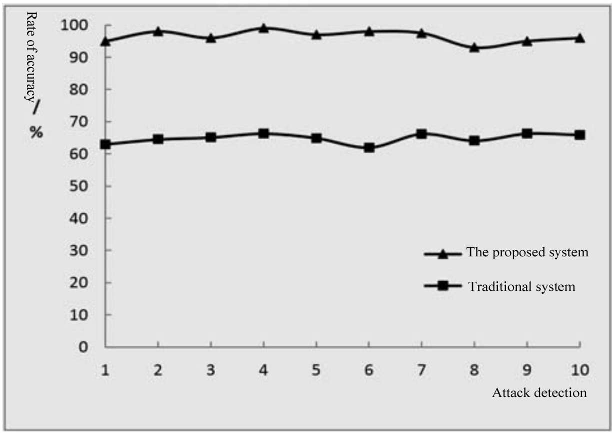

Fig.7 Comparison of detection accuracy of cyber-attack signal

From the experiment above, after selecting the appropriate average mutual information feature and fitness function, the proposed algorithm can accurately detect the cyber-attack signals, and accuracy rate of detection is higher than 95%, improving about 35.6% than the traditional system, which meets the requirements of network security and has broad application value.

V. CONCLUSION

To effectively realize the detection of cyber-attack signals, the paper highlights an average mutual information feature potential mining algorithm based on the Rossle chaotic model, and according to the non-linear characteristic solution of the mining mutual information, valid detection of cyber-attack signals with nonlinear stochastic characteristics is achieved. This paper designs an adaptive cascade notch filter which can remove a number of interference frequency components known ruled by the minimum mean square error criterion to filtering preprocess the attack signals, and at last, extracting Rossle chaotic nonlinear mutual information characteristics of the network data stream to be detected, building decision threshold and sentencing guidelines to achieve the characteristic mining and detection of cyber-attack signals. Simulation results show that the algorithm has significantly improved the performance of detection and the probability of detection has reached to 98.7%, showing superior detection performance of the algorithm, which can effectively be applied to the field of network security.

Acknowledgment

This work is supported by Shanghai Education Commission Scientific Research Innovation Project (14ZZ170). The authors are grateful to all colleagues in the Computer Science and Technology Department of Shanghai Sanda University for their help and encouragement.

REFERENCE

[1] Jiang Yun, Chen Na, Ming Li-te. Bagging-based Probabilistic Neural Network Ensemble Classification Algorithm [J]. Computer Science, Vol.40 No.5, May 2013.

[2] Ye Qing, Huang Yan-lei. Non-uniform Distribution Intrusion Detection Research and Simulation of the Model [J]. Bulletin of Science and Technology, Vol.29 No.8, Aug. 2013.

[3] Luo Li-ming, Zhou Zhen. IPV6 Based Network Security Intrusion Detection Technology Research [J]. Bulletin of Science and Technology, Vol.28 No.4, Apr. 2012

[4] He Ran, Wang Yong-ji, Wang Qing, Zhou Jin-hui, Hu Chen-yong. An Improved Particle Swarm Optimization Based on Self-Adaptive Escape Velocity [J]. Journal of Software, Vol.16, No.12, 2005.

[5] Deng Bing, Tao Ran, Ping Dian-fa. Moving Target Dection Algorithm with Compensation for Doppler Migration Based on FRFT [J]. ACTA ARMAMENTARII, Vol.30 No.10, Oct. 2009.

[6] Ou Shi-feng, Gao Ying, Zhao Xiao-hui. Adaptive Combination Algorithm and Its Modified Scheme for Blind Source Separation [J]. Journal of Electronic&Information Technology, Vol.33 No.5, May 2011.

[7] Cheng Dong-nian, Wang Bin-qiang, Wang Bao-jin. Preliminary Study on the Connotation of Flexibility in Dynamically Reconfigurable Networks [J]. Journals of Communications, Vol.33 No.8, Aug.2012.

[8] Chen Hui-lin, Xia Dao-xun. Applied Research on Data Mining Based on CART Decision Tree Algorithm [J]. Coal Technology, Vol.30 No.10, Oct.2011.

Introduction to the authors

1. Liu Zai-ying was born in the year of 1997, and he comes from Shou-guang, Shan-dong province. He has a master's degree and now he is an associate professor. His major research focuses on processing of images and large data.
2. Zhou Ming-sheng was born in the year of 1981, and he comes from Wei-fang, Shan-dong province. His major research focuses on uncertainty reasoning and decision support.