The Development Of Intrusion Detection System Based On Wavelet Network

Guang-xian Ji

Abstract

IDS (Intrusion Detection) is through a computer network or computer system from a number of key points in the collection of information and analyze, from a network or system is found in violation of security policy behavior and signs of an attack, while making response. As a mathematical tool, wavelet analysis has been widely used in signal analysis, image processing, numerical analysis, etc. This paper presents the development of intrusion detection system based on wavelet network and proposes the wavelet network algorithm based intrusion detection system. Finally, the paper designs a wavelet-based network intrusion detection system. And verified through simulation experiments of this intrusion detection system is feasible.

Keywords: Wavelet Network, Intrusion Detection System, Network Security

1. Introduction

IDS (Intrusion Detection) is through a computer network or computer system from a number of key points in the collection of information and analyze, from a network or system is found in violation of security policy behavior and signs of an attack, while making response. With the continuous development of network security technology, network security concepts continue to be deepened and constantly with new features and meaning [1]. Network security issues is actually composed of two aspects: First, the network's system security, it mainly refers to the network resources, physical and safety of the carrier, whose main task is to ensure that all network resources, stable and reliable operation, and controlled legitimate use; the second is the network information security, it refers to information storage, transmission and application security, and its main task is to ensure information confidentiality, integrity, and availability of anti-repudiation.

Expanding the scope of the network, network technology advances, network attacks are increasing, and the degree of harm is also growing. Intrusion detection requires a lot of data acquisition and processing, the use of traditional intrusion detection methods have been unable to meet. The traditional pattern matching detection is based on known attacks or system vulnerabilities identified a significant invasion of this method can not detect unknown attacks. The traditional anomaly detection using conventional statistical methods to establish the state library, to determine the behavior does not meet the general conditions for the exception. Disadvantage of this approach is the false negative rate and false alarm rate.

Intrusion detection system (Intrusion Detection Systems, IDS) is based on certain security policy for the system to establish the safety support systems. If the system is under attack, intrusion detection system can detect as much as possible, even in real time to detect and take appropriate measures. Intrusion detection system as a safety trigger, by detecting intrusion events, you can in a timely manner to prevent the occurrence of the event and on a larger scale.

IDS we need to find a way to improve the effectiveness, applicability and scalability of the method, thus, this wavelet network technology to intrusion detection systems. Another wavelet neural network nonlinear mapping ability to ensure its successful implementation of the classification of simple or complex, it will store the information in distributed connection weights in the network has a higher fault tolerance and robustness.

In this paper, the field of network security as a vital branch - intrusion detection technology to do analysis and research related to. This paper presents the development of intrusion detection system based on wavelet network. For the intrusion detection research, audit trail from the early data analysis, to real-time intrusion detection system, to the current applied to a large network of distributed detection system, essentially developed into a theory of a certain size and the corresponding field of study.
2. The research of Intrusion Detection Systems

The rapid development of computer network has penetrated into our work and life, followed by the illegal invasion and malicious destruction has become more rampant. How to protect system resources and data, enabling them to controlled access, network security is an important issue, more attention has been paid [2]. The original static, passive security and defense technology has been unable to meet the higher requirements for network security. A dynamic security and defense technology - intrusion detection technology came into being on this.

IDS (Intrusion Detection) is through a computer network or computer system from a number of key points in the collection of information and analyze, from a network or system is found in violation of security policy behavior and signs of an attack, while making response.

Intrusion detection process is generally in two steps: First, information gathering, also known as information gathering. Collected include system, network, data and user activity in the state and behavior. Need in the computer network system in a number of different key points (different segments and different hosts) to collect information, which in addition to the expanded detection range of factors, there is an important factor on the information from a data source might look no doubt, but a few inconsistencies in the data source information is suspicious behavior or invasion the best logo. The use of intrusion detection system and network information from the general log, the file directory and file do not expect change, program execution is not expected behavior and physical information, and other forms of invasion; Second, the data analysis. Data analysis is the core of intrusion detection, in this phase, Intrusion detection using a variety of detection techniques first step in processing the information gathered and the analysis results to determine whether the conduct of an object is detected intrusion, as shown by figure 1.

\[
\text{dist} = \sqrt{\sum_{m=1}^{n} [F(h_m) - F(T_m)]^2}
\]  

Figure 1. The intrusion detection process diagram

Intrusion detection system (Intrusion Detection Systems, IDS) is based on certain security policy for the system to establish the safety support systems. If the system is under attack, intrusion detection system can detect as much as possible, even in real time to detect and take appropriate measures [3]. Intrusion detection system as a safety trigger, by detecting intrusion events, you can in a timely manner to prevent the occurrence of the event and on a larger scale.

Intrusion detection to help system administrators deal with cyber attacks, expanded the system administrator's security management capabilities (including security auditing, monitoring, attack recognition and response), improve the integrity of the information security infrastructure. Firewall, intrusion detection is considered to be safe after the second gate, does not affect network performance in the case of the network can be detected, thus providing internal attacks and external attacks and misuse in real-time protection.

(1) User and system behavior detection and analysis;
(2) Important system files and data integrity assessment;
(3) The system configuration and vulnerability of the audit examination;
(4) Statistical analysis of abnormal behavior patterns;
(5) Known attack pattern recognition;
(6) The operating system audit trail violations of security policy management and the identification of user behavior.

In general, an intrusion detection system consists of the following components.
(1) Data source
Data source is the IDS monitors and found unauthorized or unusual behavior of the original network packets. Usually the data sources include the original network packets, operating system audit records, audit records and the application system calibration data, etc.

(2) Sensor
Sensor unit is in order to collect data from the data source. Different IDS, the sensor unit is different frequency of data collection.

(3) Unit of analysis
Analysis of the sensor element analysis and processing the collected data (if authorized or abnormal behavior, and other useful events, etc.) and generate alarms. Existing IDS systems, sensor unit and the unit of analysis is often part of a unified component.

(4) Management unit
General, the management unit include analysis of cell configuration examples. Informed management, data integration and reporting, etc.

\[
\frac{R}{S}(n) = \frac{1}{S(n)} \left[ \max \left( Y(t) - \frac{1}{n} Y(n) \right) \right] - \left[ \min \left( Y(t) - \frac{1}{n} Y(n) \right) \right]
\]

(5) Response Unit
Response unit is the functional unit to respond to alarms, such a strong reaction, or just a simple alarm. In some systems, the management unit and response unit are functions by the same module implementation. The response unit can also be called a snap, as this model and inform an inquiry model.

(6) Behavior
Behavior is an instance of the data source, such as a network connection, a user performs an action and an application of such an event is triggered. Behavior can be both dangerous malicious attacks, users can also be a harmless occasional abnormal operation.

(7) Alarm
Alarm message is generated and sent by the unit of analysis corresponding to the response unit. Warning messages usually include the type of event, event time, and event handling information such as the priority.

(8) Reaction
Reaction may be triggered automatically by the system. Can also be launched by the security manager. Among them, notify the administrator is a common reaction. Other reactions include behavioral records, characteristics of the raw data records, cut off the network connections, terminate processes, change attributes such as network or system access.

Figure 2. The intrusion detection system consists of the reaction components

This model is host-based and integrated application of both network-based technology, the network from external attacks and internal abuse at the same time for testing. Model includes four modules: network data capture module, the host detection module, network detection module and RS modules. Capture network data capture module into the PC’s network data, there are data link packet header information, TCP / IP header information and network session state information. Host detection module is relevant documents by scanning the local host or network usage statistics, plus analysis of audit records to detect whether there had been invaded on a PC activities. The main function of network detection module analyzes network data packets through the relevant information to determine whether there is intrusion to occur. RS module detection module is based on test results to take appropriate measures, such as alarm messages, disconnect the network connection, etc.
Most scholars will detect IDS analysis engine research as a key factor; the key analytical techniques are misuse detection (misuse detection) and anomaly detection (anomaly detection) into two categories. Misuse detection searches audit event data to see if the existence of pre-defined pattern of misuse; anomaly detection is to extract the normal mode, the mathematical characteristics of audit data, check the event data is inconsistent with the existence of abnormal patterns. Misuse detection can be more accurately detect attacks, but the false negative rate is high; anomaly detection may detect unknown attacks, but a high false alarm rate. Here we introduce these two aspects to the analysis of intrusion detection technology.

Misuse detection is based on the inspection system events such a problem: the system acts on behalf of a specific attack mode? First identify a specific behavior patterns encoded invasion, the establishment of misuse pattern library, and then get the actual testing process to filter the audit event data to check whether it contains the identity of intrusion. Perform misuse detection, need to have the following conditions: about misuse behavior components; complete testing rule base; credible record of user behavior; feasible behavior log analysis techniques. Defect: can only detect known attack patterns, when there is a means for new exploits for old vulnerabilities or new attacks, the need for the manual or other machine learning systems reveals a new mode of attack of the features added to the misuse model library in order to make the system detect the ability of the new means of attack, as many anti-virus software on the market, like the need to constantly, timely detection capability upgrade in order to ensure the completeness of the system, as shown by equation 3.

\[
(\sum x_i (2^\alpha \mathbf{P}_i + \phi(N_i)) + \beta(U_i - W_i))(\sum x_i W_i \leq E)
\]

Intrusion detection technology can be seen in the development, invasive techniques are updated. How will a number of underground organizations have to bypass IDS or attack IDS system as a research priority? High-speed networks, especially through the exchange of technology and data communication channel encryption makes the listener through a shared network segment becomes insufficient data collection method. The significant amount of traffic is the data analysis as well as new requirements. With the information system of a country's social production and the impact of the national economy has been gradually increasing importance of information warfare seriously by all countries. The importance of information warfare attack "weapon" is one of the network intrusion technology, information warfare defense work to include the "protection", "test" and "response", intrusion detection is one of "testing" and "response" is not part of integral part of the.

3. The algorithm analysis of wavelet network induction

For a long time, both the signal processing community, or the mathematical community, people trying to find the signal representation, trigonometric series with integrated Harr the advantages of both systems function to break down some arbitrary function[4]. We know that these two functions in the sense lines occupy two extreme positions. Department of trigonometric functions in the frequency domain that is variable in the Fourier domain is completely localized, but in space or time domain without any locality. On the contrary, Harr lines in the time domain function is completely localized, but it is localized in the Fourier domain variable is poor because it lacks the regularity and the oscillation caused by it.

Wavelet analysis of major research functions that will function into the "basic function" of and, while the "basic function" is a wavelet function obtained by scaling and translation, this wavelet function with good locality and smoothness, characterization makes it through the decomposition coefficient function, the function can be analyzed and the overall nature of the local nature.

The emergence and development of wavelet analysis, from many different scientific fields signal processing requirements. As a mathematical tool, wavelet analysis has been widely used in signal analysis, image processing, numerical analysis, etc., and the issues arising from these applications further stimulated interest in the people of wavelet analysis. As a result, it is brought rapid development of wavelet analysis [5].

Grossman and Morlet wavelet was first proposed (Wavelet) concept, is given by a translation system to determine the function of the stretch to start the function to signal that new methods and new ideas. Subsequently, Meyer proved the existence of one-dimensional wavelet and constructed with a certain decay properties of smooth wavelet function. For a given sample classification desired information required is given by equation 4.
\[ \hat{q}_b(Y_0) = C_1 \sum_{i=1}^{n} \|Y_0 - X_i \|^2_h \|X(X_i) - b_i\|, \quad \text{if } 1 \leq j \leq m \]  

(4)

The paper is in order to function as a quadratic spline wavelet, using Mallat algorithm for seismic signal decomposition and reconstruction; good use of wavelet transform time-frequency localization properties to more accurately detect the signal and appear singular position. Introduced the FM and Gaussian wavelet for ECG signal processing and research are shown that it is able to correctly identify normal and abnormal electrocardiogram, as shown by figure 3.

![Figure 3. Schematic diagram of wavelet time-frequency analysis](image)

Applied Daubechis wavelet transform are using the binary wavelet Mallat algorithm to extract partial discharge signals [6]. The paper is using wavelet transform method will be broken down into five sunspot number scale factor and a residual factor, and then use dynamic feedback neural network, respectively, fitting them with the forecast, the final cumulative, results show that this approach is effective. Set, the Fourier transform. When allowed to meet the conditions (Admissible Condition).

\[ C_\psi = \int_{\mathbb{R}} \left| \tilde{\psi}(\omega) \right|^2 \frac{d\omega}{\omega} < \infty \]  

(5)

We called a basic wavelet or mother wavelet called (Mother Wavalet). The generating function by scaling and translation, you can get a wavelet sequence. For the continuous case, the sequence of wavelet is shown by equation 6.

\[ \psi_{a,b}(t) = \frac{1}{\sqrt{|a|}} \psi \left( \frac{t-b}{a} \right) \]  

(6)

Wavelet analysis is a window size (ie, window size) fixed and can change its shape, the time window and frequency window can change the time-frequency localization analysis. That low-frequency part of the high frequency resolution and low time resolution, the high frequency part of the higher time resolution and lower frequency resolution, so the known mathematical microscope. It is this feature, so that the signal wavelet transform with adaptive, as is shown by equation 7.

\[ P\{S|E \in R\} = \sum_{i=0}^{h-1} \sum_{j=0}^{h-1} P\{S|E \in C(i, j)\} * P\{E \in C(i, j)\} \]  

(7)

![Figure 4. Displacement and stretching of wavelet algorithm diagram](image)
Which the expansion factor or scale factor, to do the basic wavelet expansion; of translation factor, the basic wavelet do shift. For the continuous wavelet time-limited, it is \( \psi(t) \) and \( \psi_{a,b}(t) \) the relationship is shown by figure 4.

\[
W_{\psi} f(m, n) = a_0^{-rac{m}{2}} \int_{-\infty}^{\infty} f(t) \overline{\psi(a_0^{-m} t - nb_0)} dt
\]  

(8)

Different frequency components, in the time domain sampling step is, is adjustable, high-frequency were (corresponding to small values) sampling step is small, low persons (corresponding to large values) grew up in the sampling step. In other words, the wavelet transforms to achieve a fixed window size, shape, and variable time-frequency localization.

Algorithm: Wavelet is a shock features that quickly decay to zero of a class of function algorithm
Input: Known by the former to meet the permit conditions referred to as the base wavelet function, the scaling and translation functions constitute a cluster system.
Output: Scale factor or frequency factor.

Step 1: calculated by the Kalman filter moving target position of the first frame of the forecast for the Mean-Shift algorithm provides the location search initialization.

Step 2: \( \{ \hat{y}_b(y_b) \} \quad b = 1, 2, \cdots, n \)

\[
W_f(a, b) = \left| a \right|^{rac{1}{2}} \int_{-\infty}^{\infty} f(t) \overline{\psi(t-b)} dt
\]

Step 3: if

Step 4: ENDIF

Step 5: IF \( \mathcal{C}((x^*) \epsilon \text{Intent(inf(L))) THEN} \)

\[
C = \int_{-\infty}^{\infty} |\psi(\omega)|^2 d\omega < +\infty
\]

Step 6: IF

\[
f(t) = C_i \int_{-\infty}^{\infty} W_{\psi} f(a, b) \psi_{a,b}(t) \frac{dadb}{a^2} \quad \text{THEN}
\]

Step 7: While

\[
\rho_\omega([\hat{p}(\hat{y}_1), \hat{q}] < \rho_\omega([\hat{p}(\hat{y}_0), \hat{q}) \quad \hat{y}_1 = \frac{1}{2} (\hat{y}_0 + \hat{y}_1)
\]

\[
\rho_\omega([\hat{p}(\hat{y}_1), \hat{q}]
\]

Step 8: if \( \|\hat{y}_1 - \hat{y}_0\| < \epsilon \) ELSE \( \hat{y}_0 = \hat{y}_1 \)

\[
W_{\psi} f(a, b) = \left| a \right|^{rac{1}{2}} \Delta t \sum_{k=1}^{N} f(k \Delta t) \overline{\psi \left( \frac{k \Delta t - b}{a} \right)}
\]

Step 9:

Step 10: IF \( \delta_\omega([\hat{p}(\hat{y}_1), \hat{q}] \quad \text{THEN exit algorithm;}

Step 11: ENDIF

Step 12: ENDIF

4. The development of intrusion detection system based on wavelet network

Wavelet network based intrusion detection system only in the detection rate is higher than traditional methods is not enough, they need to learn other aspects of speed and false alarm rate in an acceptable range, is available. Therefore, the purpose of this study is to design an intrusion detection system to study the detection efficiency and accuracy to achieve more satisfactory results. So this paper, the wavelet network and SNORT intrusion detection system combined [7].

Wavelet transform is a very effective mathematical transformation, which overcomes the traditional Fourier transform does not reflect the signal characteristics of local information, and access to local information of the object model pattern recognition is very important. Wavelet transform, through its unique translation factor and scale factor to ensure that model changes in the proportion of samples and the relative translational invariance, the results obtained to distinguish a variety of scales, which have good function approximation capabilities. So the wavelet transforms and networks combined will be able to essentially improve the neural network learning. Based on this idea, we construct a wavelet network.
Wavelet analysis and neural networks combined with the following two ways: 1) a loose combination, the wavelet analysis as a means of pre-processing neural networks, neural networks for the input feature vector; 2) The combination of compact type, that is, wavelet analysis and direct integration of neural networks to form a wavelet function of neurons. Using a compact-type wavelet neural network structure, that is a radial basis function (Radial Basis Function, RBF neural networks, each hidden layer activation function system constituted by a wavelet function [8], as is shown by equation 9.

\[
f_{m} = f(u_{m}) = f\left[ \sum_{k=1}^{K} w_{k} \sum_{m=1}^{M} x_{m} \phi\left( \frac{x_{m} - b_{k}}{a_{k}} \right) \right]
\]

(9)

The error function is less than a predetermined value, then stop learning, or return to the input sample vector learning steps. Continuing the above steps, the network showed strong and flexible line of high approximation capability.

Intrusion detection system based on wavelet network algorithm described as follows:

Algorithm: Intrusion detection system based on wavelet network

Input: Input vector from the input layer through the middle layer of the network signal activation function.

Output: After transformation of the group and then multiplied with the conversion coefficient calculations, the final sum output from the output layer.

(1) Number of pixels for the center as a candidate for the target area image integrated histogram, cross-section through the window width for the smooth function of the model after;

(2) IF \( x < N \) Then Calculate the instantaneous gradient;

(3) Let \( x = \{x_{i}, i = 1, 2, \ldots\} \), in which \( x_{1}, x_{2}, \ldots, x_{t} \) are independent \( N(0,1) \) with distribution, \( x_{t+1}, x_{t+2}, \ldots \) are independent \( N(\delta, 1) \) with the distribution;

(4) IF Each function has B, C, D words as input and produces as output a word THEN

(5) While \( x=10 \), \( x' = (x_{i} - b_{k}) / a_{k} (i = 1, 2, \ldots, M) \);

(6) Based on the sensor nodes receive the encoded data in the time interval, Sink node decoder reconstruct the estimated value of the event source;

\[
\Delta w_{k}^{\text{new}} = -\eta \frac{\partial E}{\partial w_{k}^{\text{old}}} + \alpha \Delta w_{k}^{\text{old}}
\]

(8) Back propagation, the network training process,

(9) Denoted by \( B[i] = |C: | | \text{Intent}(C) | = i \};

(10) Sampling time is an effective model based system model set is \( M = \{m_{1}, m_{2}, \ldots, m_{i}\} \), the model conversion process in line with Markov processes;

(11) \( a_{k}, b_{k}, w_{k}, a_{k}^{\text{new}} = a_{k}^{\text{old}} + \Delta a_{k}^{\text{new}}, b_{k}^{\text{new}} = b_{k}^{\text{old}} + \Delta b_{k}^{\text{new}}, w_{k}^{\text{new}} = w_{k}^{\text{old}} + \Delta w_{k}^{\text{new}} \)

(10) Stop.

Wavelet neural network training to 4005 times the data has been convergence time, and BP neural network to reach 7317 times the data when it is convergent. This shows that the wavelet neural network has better training speed, can be used for intrusion detection to better improve the efficiency of the system to save time is shown by figure 5.

**Figure 5.** Wavelet neural network training data convergence map
Using wavelet network has good localization characteristics of wavelet functions as basis functions, these functions can be entered only in the local area to ensure a response, thereby avoiding the problem of slow convergence. Wavelet network is the promotion of radial basis function network, the wavelet basis functions are orthogonal, the correlation between network nodes, the weight redundancy is very small, and of a weight training will not affect the other weights, which has a faster canonical signed speed. When the input signal is non-uniform distribution of the sample space, the wavelet neurons of good local features and multi-resolution learning to achieve a good match with the signal, making the wavelet neural network has a greater adaptive capacity and higher precision of early warning.

5. Conclusions

IDS (Intrusion Detection) is through a computer network or computer system from a number of key points in the collection of information and analyze, from a network or system is found in violation of security policy behavior and signs of an attack, while making response. Wavelet analysis of major research functions of the network that will function broken down into "basic function" of and, while the "basic function" is a wavelet function obtained by scaling and translation, this wavelet function with good locality and smoothness, making it through the decomposition coefficients characterize the function, you can analyze the nature and function of the overall nature of the local. This paper presents the development of intrusion detection system based on wavelet network and propose algorithm of the Wavelet network based intrusion detection system.

Finally, the paper designs a wavelet-based network intrusion detection system. And verified through simulation experiments of this intrusion detection system is feasible.

6. References