Research on the Applications of Parallel Genetic Algorithm and Optimization Theory in the Enhancement of Network Security

Liwei Chen[1]

[1]College of Computer Science and Technology,
SouthWest University of Science and Technology,
Mianyang,621010,China

Abstract. In this paper, we conduct research on the applications of parallel genetic algorithm and optimization theory in the enhancement of network security. As the using range of the world's biggest information network, the Internet itself agreement the openness of great convenience to all kinds of computer net and broaden the scope of shared resources and the way. Computer virus refers to the blocks in the computer program insert damage computer data and functionality. Therefore, enhancing the security is urgently needed. Our method solves the issues well which illustrates the feasibility and effectiveness of our designed methodology.

Keywords: Genetic Algorithm; Optimization Theory; Network Security; Literature Review.

INTRODUCTION

In computer network technology brings us convenient at the same time, and associated with network security problem. When people is to seek the countermeasure to solve the problem of network security, will be a lot of technology application on the computer network security, due to the constant development and application of the virtual technology in recent years, as a new technology of network, it is also used in the computer network security problems. As the using range of the world's biggest information network, the Internet itself agreement the openness of great convenience to all kinds of computer net, and broaden the scope of shared resources and the way. However, because in the early network protocol design to ignore security issues, as well as in the use and management of anarchy, gradually exposed to the host on the Internet's own security is increasingly serious security threatened. It is a general definition of network security and network security refers to the hardware, software, network system and its system of data protection, not due to accidental or malicious reasons and destroyed. A continuous and reliable system running normally and at the same time, the network service is not interrupted. The content of the network security includes two parts of the system security and information security. System security mainly refers to the hardware of network equipment, security of operating system and application software [1-2].

The general elements of threating network security could be separated into the following parts. (1) The threat of backdoor. Began in the earliest computer is invaded, developed the "back door" the hacker technology, and make use of this technology, they can enter the system many times. (2) The threat of computer viruses. Computer virus refer to the can in a computer program insert damage computer data and functionality, and affect the normal use of the computer and a set of instructions that can self-replicate or code. Such as common worms, is to use a computer application system and procedures of holes on the active attack. The virus in the high destructive, high transmission and the hidden excellent virus disease at the same time, also have their own special some like only exists in memory, thus cause denial of service to the network, and the characteristics of the combination of will and hackers. (3) Natural threats. For natural threat, probably from natural disasters, electromagnetic radiation, network equipment caused by natural aging and bad space environment, etc. The accidental factors may also be directly or indirectly affect the computer network security. (4) Grant access to illegal. Illegal grant access refers to some people use debugging computer programs and proficient programming skills obtained illegally to the enterprise, the company or individual network file access, invaded the internal network of a kind of illegal and criminal behavior. The invasion is mainly in order to achieve the purpose of using the system of writing power, storage power and access to the other's permission to store content, and as a springboard into other systems or even sabotage the system which will eventually led to the loss of service capacity [3].

To enhance the network security and upgrade the network security system of China, in this paper, we conduct research on the applications of parallel genetic algorithm and optimization theory in the enhancement of network security. In order to more effectively find the interesting rules from dense data sets, genetic algorithms and genetic programming was introduced into applied in association rules mining. Genetic programming with tree structure aims to replace the genetic mechanism of genetic algorithm to improve the application in the interpretability of association rule mining. However, genetic programming to improve the expression ability of association rules at the same time which also has a tree structure expansion problem. In order to solve the problem of the series, association rules mining method was proposed based on genetic network. The association the advantage of data mining based on genetic network programming which can according to user requirements elicitation foot more important rules, and do not need to take all conform to the standard rules. In the next sub-sections, we will introduce our methodology in detail.

The Proposed Approach and Algorithm

The Principles of the Network Intrusion Detection. With the rapid development of network, computer network is facing greater risk, network intrusion detection system to become an integral part of basic protection mechanism. Network intrusion detection can be defined as found threat network integrity, confidentiality, and availability of malicious behavior. In general, intrusion detection can be divided into two categories: misuse detection and anomaly detection [4]. Based on knowledge or misuse detection, also known as signature-based intrusion detection and misuse detection of IDS based on knowledge of known attacks to establish library attack characteristics, by the user or the system behavior and all kinds of attack mode in characteristic database comparison to determine whether the invasion. And anomaly detection, also known as intrusion detection based on behavior, system, network, establishing the normal behavior of a user or process contour model, and the deviation of the behavior of the larger interpreted as intrusion behavior. The method is based on the following assumptions: invasion will cause abnormal behavior of users or system. Anomaly detection method has the ability of detection system of unknown attacks. Association rule mining, it is a kind of form has extensive application in data mining, can be defined as found the relationship between various attributes in a data set or a relationship. Establish the effective IDS can be said to be a huge knowledge engineering work, early system which will rely on intuition and experience to choose statistical indicators for anomaly detection. Because of this system to establish artificial sex and specificity, made early IDS in terms of scalability and adaptability has certain restrictions. Therefore, in the following figure, we illustrate the traditional network intrusion detection system [5].

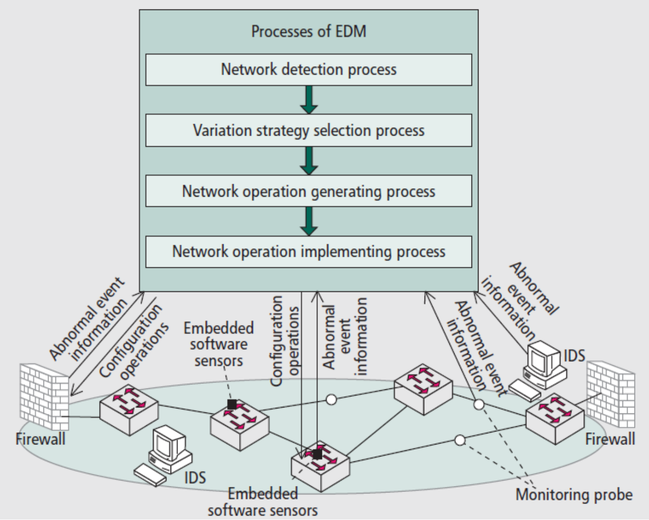
Processes of EDM
Network detection process
Variation strategy selection process
Network operation generating process
Network operation implementing process
Abnormal event information
Configuration operations
Embedded software sensors
Configuration operations
Abnormal event information
Abnormal event information
Abnormal event information
IDS
Firewall
Firewall
IDS
Embedded software sensors
Monitoring probe

Figure1. The General Flowchart of the Intrusion Detection System

Intrusion detection process is also use large amounts of data that is collected information, such as the host system logs, audit records, and network packets and so on, to analyze it to find the invasion or abnormal process. Therefore, we can use data mining technology, extract as much as possible from a large amount of data on the safety information, abstract the model is helpful to compare and judge.

The Parallel Genetic Algorithm. Genetic network programming is a kind of evolutionary optimization algorithm, the algorithm using the directed graph structure to replace the tree structure of genetic programming or genetic algorithm genetic structure. According to each classification of association rule support, confidence, and chi-square value is greater than the minimum threshold, which is a standard GNP will extract important classification association rules and their corresponding rules in the library. The whole process including rule mining based on GNP in the definition of interesting rules in advance, for GNP initialization of an individual connection and function of the node set; Calculate according to the GNP individual connection check database, then the standard values of various rules, through the standard selection rules in the rules of the rolls; Then according to the fitness function to choose the better individual into the next generation, using the genetic operators to GNP evolutionary individuals repeat check rule extraction until end of GNP evolutionary generation database. This method can flexibly according to user requirements definition interesting rules, extracting interesting rules enough to meet user needs, rather than of extracted all the rules, thereby in the certain to extent which reduces the time cost.

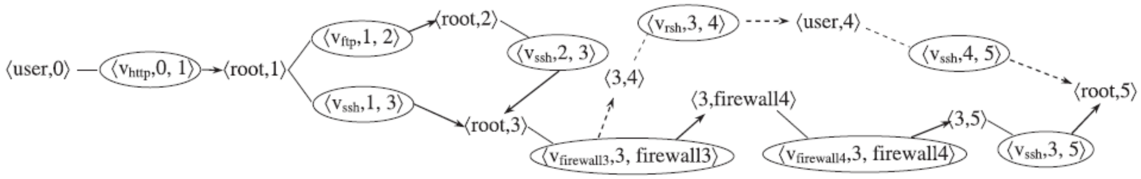

Figure2. The Illustration of the Parallel Genetic Algorithm

Difference to other simple database, network connection database has its obvious characteristics, such as with discrete and continuous attributes, and attribute value contains a lot of important information. GNP judgment nodes are used to check the database records each attribute's value is satisfied, and recycling processing nodes to calculate all kinds of measure of association rules. Attributes and attribute values corresponding to the GNP of judgment node function.

$$sup > 0.25 \qquad conf > 0.6 \qquad c^2 > 6.64$$

(1)

In the formula one, we illustrate the judgement criteria for the parallel genetic algorithm. For the anomaly detection, normal training database contains only connection, GNP in training phase extraction only normal rules in the normal rules of the rolls. In the process, support as the only standard to select rules. Sometimes contain certain attributes and attribute values of fuzzy classification association rules already exist in the rule base, but due to the evolution of the fuzzy member function chi-square value is changed, then we will choose a chi-square value is higher that the rules stored in the repository. So, in a generation, evolution rule base are constantly updated, only the chi-square value is the highest rule and its corresponding more adaptive fuzzy member function are retained in the rule base. Every rule with training database to calculate the fitness value of rules, the individual in the fitness of each classification association is defined in the following formula two.

$$fitness_r = N_{tc} - N_{ni}$$

(2)

Fuzzy classification rule mining algorithm based on GNP is we put forward a new algorithm of network intrusion detection problem, it can handle both discrete and continuous properties of network connecting data database, dig out the useful normal and intrusion rules. According to this algorithm, we also proposed the use of such rules for the new network connection data classification method.

The Optimization Theory with Network Security. The virtual network techniques in combination with the enterprise information and broadband technology, the computer network information security has achieved good effect, enterprise information and resources got maximum guarantee security. With the virtual network technology matures, the security, reliability and stability of the product will be a greater degree of improve. So far, the telecom industry is in a state of weak gradually, the virtual network technology is gradually becoming a new luminescent spot in the computer information network security, and the virtual network technology occupied market share in the market is rising year by year. In all kinds of virtual network technology products, combined with the virtual network firewall software technology and complex network technology products gradually become hot spots in the computer network. Virtual network technology, is a private network technique, namely in the public data network build private data networks. Users can in virtual private network, virtual local area network of proprietary, guarantee in different locations in the local area network do it like a local area network, in order to ensure the security of data transmission. In the following figure, we optimize the current pattern with visual graph.

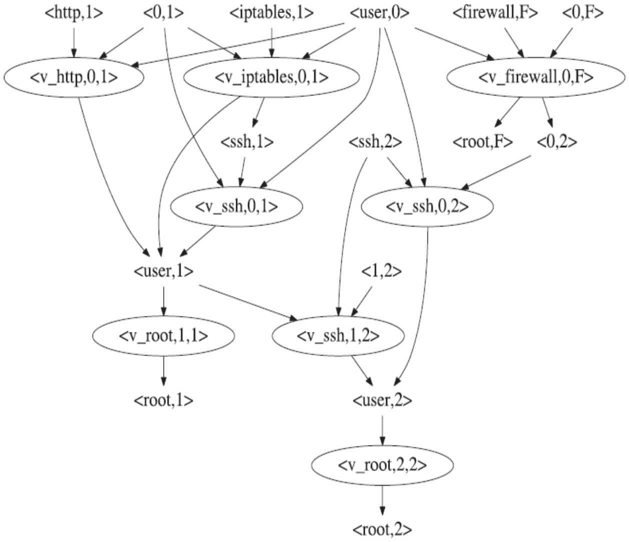

Figure3. The Structure of the Proposed Methodology

CONCLUSIONS

In this paper, we conduct research on the applications of parallel genetic algorithm and optimization theory in the enhancement of network security. With the continuous development of computer technology in the computer system security problem becomes increasingly serious it has evolved from the traditional single form to form based on network. Computer network security evaluation index system for is more than a computer network by holes, such as virus invasion is a complex nonlinear problem. The traditional linear evaluation method cannot accurately describe the indexes influence on the evaluation results and the accuracy of the evaluation results. Our proposed method solves the issues well. In the future, more corresponding research will be conducted.

Acknowledgement

This research is financially supported by the artificial intelligence laboratory in Sichuan province, the key laboratory open fund (NO. 2014RYY03).

References

[1] Xu Q L, University X N. Enhancement Measures of Computer Network Security and Reliability[J]. Information Security & Technology, 2014.

[2] Zhou Z, Feng W, Ye L, et al. Video conference system image evaluation and quality enhancement method is analysed[J]. Network Security Technology & Application, 2014.

[3] Eghbal, M., Abouei, J., Eghbal, M., & Abouei, J. (2014). Security enhancement in free-space optics using acousto-optic deflectors. Optical Communications & Networking IEEE/OSA Journal of, 6(8), 684 - 694.

[4] Howell A. Resilience, war, and austerity: The ethics of military human enhancement and the politics of data[J]. Security Dialogue, 2014, 46(1).

[5] Huang H F, Chang H W, Yu P K. Enhancement of Timestamp-based User Authentication Scheme with Smart Card[J]. International Journal of Network Security, 2014, 16.