Research on the Network Intrusion Detection System based on Modified Particle Swarm Optimization Algorithm

Xuesong Wang
FoShan Polytechnic,
FoShan,Guangdong,528137

Guangzhan Feng
Foshan Huijia science and technology CO.,Ltd

Abstract—**In this paper, we conduct research on the network intrusion detection system based on the modified particle swarm optimization algorithm. Computer interconnection ability put forward the higher requirements for the system reliability design, the need to ensure that the system can support various communication protocols to guarantee the reliability and security of the network. At the same time also require network system, the server or products have strong ability of fault tolerance and redundancy, better meet the needs of users, to ensure the safety of the information data and the good operation of the network system. For this target, we propose the novel paradigm for the enhancement of the modern computer network that is innovative.**

***Keywords*- Intrusion Detection, Network, Particle Swarm Optimization, Modification, Algorithm.**

Introduction

At present, the generally recognized by the international computer security means, mainly includes two aspects: one is the physical aspect, it mainly involved the related to support the normal operation of the computer system hardware and has certain anti-interference ability of the physical environment of security maintenance, the other is a logic level, it refers to the network information availability, integrity and confidentiality protection, we usually call this information security. Computer network security is an extension of the information security, it is not invariable, the standards and requirements of primary dynamic varies as the general user requirements [1-3].

Computer network security architecture and security model, and understanding of the concept of the security, security system design, implementation and verification are very necessary. According to the literature review, the developmental trend of the network could be summarized as follows. (1) The development of general computer network is a very strong regularity, integration, openness, the high performance, the intelligent standard. The inheritance of the computer network performance in highly centralized computer network resources, all kinds of service and the high integration of the media application, at the same time allow peer-to-peer, opposite the point, in the face of a variety of basic transmission, there is no special service can provide the best quality of the information transmission, there is a requirement for a certain time delay and error can also provide real-time interaction in order to ensure the quality of service. (2) The development of the computer network technology presents a spiral pattern, namely for computer network technology development is an iterative process, the need to constantly research and application validation work to confirm and push. (3) With the development of the expansion of the Internet to promote more routing algorithm, in the Internet on the core routers of the routing table is becoming bigger, this leads to a router needs to accelerating are complicated.

The current intrusion detection system is the main problem is: the trend of diversification of the intrusion method is more and more obvious, as the traditional intrusion detection knowledge update have been unable to meet, causing the attack characteristic library or system normal behavior is not timely update description, eventually led to the high rate of false positives and high non-response rates, that need to establish a new behavior description to cope with the new environment. Traditional intrusion detection system is based on the cognitive model of intrusion detection, in this model, the audit records, network packets, and other observable activities as abnormal operation according to the detection system, and using the method of tracking and comparing with known attacks to be tested. For the further modification of the traditional approaches, in this paper, we conduct research on the network intrusion detection system based on modified particle swarm optimization algorithm. The particle swarm optimization algorithm for monotone function, strictly convex function or unimodal function that can quickly find optimal solution but the algorithm dependence on initial value is bigger, and in the late algorithm converges slowly, especially for more extreme, the complex function that is reflected from the figure one, we will optimize it that will be discussed in the later sections.

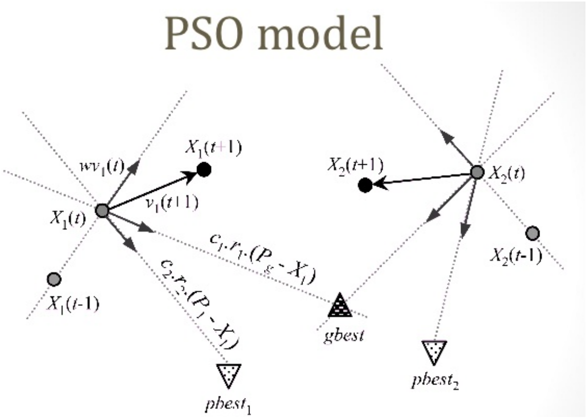

Figure 1. The Illustartion of the PSO Model

The Proposed Algorithm

The Characteristics of the Computer Network. With the rapid development of computer network technology and the Internet spreading throughout the world, all kinds of information system for the dependence of the basic computer network is more and more high, the network security factors have become an increasingly important research subject. Network topology information is the important foundation of computer network, while it is the basis of the network management, data modeling and information collection as is also the precondition of network security assessment and implementation of network attacks [4-5].

With the wide application of computer network, people realize that it is necessary to spread to far around several nodes are connected, resulting network security problem is more and more important, the openness and sharing of the network, the complexity of the system, the boundary uncertainty and uncertain path led to the network security problems. Security policy is aimed at the sensitive or the classified information release, protection and management of a series of laws and regulations and the guidelines for implementation as can be seen from the concept of computer network security and its security strategy should be from the physical configuration of the computer itself and the information access and encryption transmission and so on to develop. A computer network security should have the following characteristics as the basic feature.

- Only authorized users can access specific information and the unauthorized users can only get some meaningless data to provide users with safe and reliable communication security is the most important content of computer network security.
- Network system can under prescribed conditions and within the stipulated time to complete the prescribed function. Such as hardware reliability, software reliability, reliability, reliability of the environment as the human reliability is the most important in the whole network system reliability, for most of the causes of system failure is caused by human error.
- Only authorized users can modify the system resource and the unauthorized users to do any changes will be found

immediately. Destroy the integrity of the information is the common use of the impact of information security.

Looked from the current development status, both in abroad and domestic in the field of network topology discovery in the immature stage, foreign research on this field started earlier, although some network topology algorithms have been proposed and in practice, but also on the basis of graph theory and probability and statistics on the number of network topology display model was established, but there are still many limitations as the results of the study is only to certain extent, reflect the topology structure while the practicality is not strong. Network routing according to the routing algorithm can be divided into source routing algorithms, distributed routing algorithm and the hierarchical routing algorithm. The source routing algorithms assume that each node knows about the entire global state of the network while the global state with link-state protocols through radio, or with the distance vector protocols, a swap adjacent node periodically distance vector [6].

The Modified Particle Swarm Optimization Algorithm. Parameters of particle swarm algorithm mainly includes the inertia weight and accelerating factor, convergence factor, such as population, a large number of general experimental analysis shows that these parameters had a great influence on optimization performance of particle swarm algorithm. The different types of basic optimization, the parameters of particle swarm optimization have different settings, the same optimization problem, the different model of the particle swarm optimization and the parameters in the model set there may be differences. The figure two illustrates the principles.

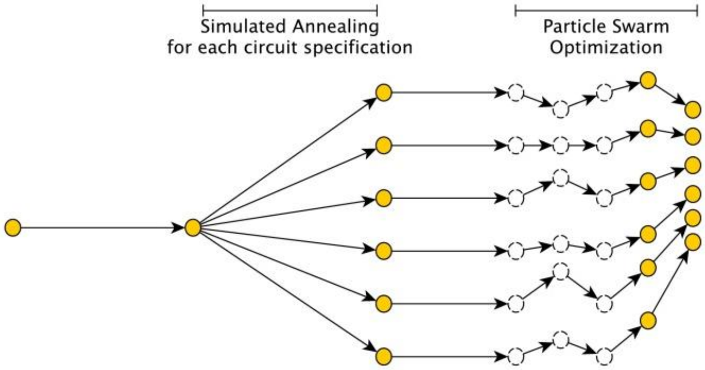

Figure 2. The Visualized Demonstration of the Particle Swarm Optimization

PSO algorithm is an optimization method based on iteration the system is initialized to a group of random solutions, through the iterative search for the optimal value, the particles in the solution space to follow the search for the optimal particle. In the each iterations the particles by tracking the two extreme values to update, one is the particles themselves now to find the optimal solution, namely the individual extreme value and the other one is the entire population is to find the optimal solution, that known as the global extremum. Its mathematical description and iterative formula is as follows.

$$\min f\left(X\right), X=\left[x_1,\cdots,x_n\right] \quad s.t. \quad x_i \in \left[a_i, b_i\right]$$

(1)

All the particles in the particle swarm update its velocity and position according to the following expression 2~3.

$$x_{ij} = x_{ij} + v_{ij}$$

(2)

$$v_{ij} = wv_{ij} + c_1 r_1 \left(p_{ij} - x_{ij} \right) + c_2 r_2 \left(g_j - x_{ij} \right)$$

(3)

Write the application of particle swarm optimization for the same different component of velocity vector, the velocity updating formula, the corresponding random parameters can be set to the same value or the different values. Niche strategy for its effective solving multimodal function optimization problems and the evolutionary algorithm is widely used. In genetic algorithm, the niche technology is mainly to exclude and sharing method. The two methods all need more individuals to participate in the competition to a shared resource that cause the waste of time. For these drawbacks, we introduce the parameters as formula 4 to optimize the traditional PSO algorithm.

$$\lambda_{generated} = 1 - \left(\left(g - 1 \right) / g \right)^m$$

(4)

The Network Intrusion Detection System. Intrusion detection to a large extent depends on the reliability and validity, to gather information, therefore, it is necessary to use only know the real and accurate software to report this information. Therefore, we should focus on the following issues. (1) System and network log file. Hackers often leave their traces in the system log files, therefore, make full use of the system and network log file information is the necessary condition to detect intrusion. (2) File system contains a lot of software in a network environment and data files, and private data file contains important information is often the target of basic hackers modified damage. (3) Don't expect behavior of program execution. In the network system program including operating systems, network services, users start the program and the application of a specific purpose, such as the database server. A process execution behavior by its runtime execution operation, operation way is different its use of system resources is different also operation including computing, file transfer, equipment and other processes, as well as the communication between the network and other processes [7].

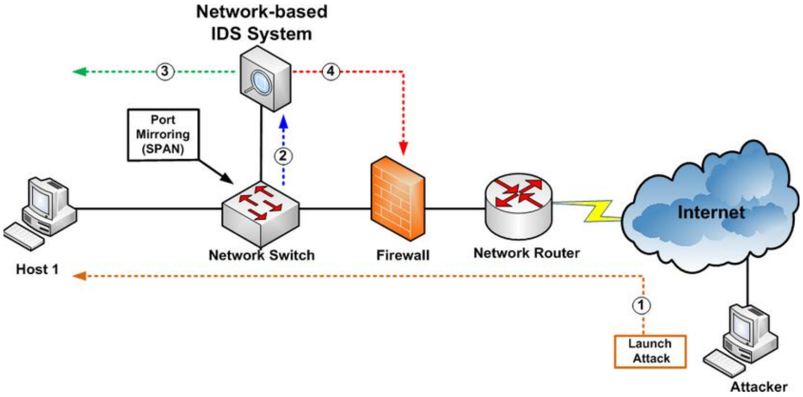

Figure 3. The Illustartion of the Network Intrusion Detection System

Host mainly analyze and audit the network data of a single host, looking for the possible intrusion behavior a bit similar to firewalls and network detection, usually on a single machine, analysis of the network traffic data. For this, we propose the new architecture steps for detection.

- Decision support. In the model based on historical data analysis and expert knowledge in the field of network security establishment decision-making parts, these parts making a decision are based on the rules of interpretation system. Action decision to trigger a decision or action to consider these rules.
- Layered detection. Through the realization of different mechanism of the multilayer structure security protection, in the model using layered monitoring,

network activity can be divided into user layer, system layer, process layer and network layer, monitor, respectively.

- Test match. To realize the network anomaly detection, mature detection agents and network self-description, it is concluded that the degree of similarity between the two. When similarity exceeds a predetermined threshold, then inform the communication agent.

The Network Optimization. In the process of the above analysis, realize that there are some influenced the stability of the computer network reliability, therefore need to take effective strategies to improve the computer network reliability effectively, and ensure the basic safety of the computer network information. To optimize the design of the computer network fault tolerance, need to select effective network mode, the general selection of redundant parallel network mode, the terminal can keep connection and the computer network center, the computer network security defense ability to effectively improve, and then make some effective control of network failure happened. If there are unexpected, the network center will also be able to coordinate that make failure caused by the loss is reduced greatly. To effectively improve in order to guarantee the reliability of the server is running, can choose the high quality of network equipment, application of modern network technology at the same time, faced with many problems, fault defense capabilities of the computer effectively [8].

Based on primary computer network structure, involving the network nodes are keep connection relationship, at the same time the network link as the channels to make information data transmission effectively. Based on computer network design process, to ensure the normal and safe operation of the computer, both should be considered a single network, also need to consider the double network, and redundant design reinforced on computer network, so can make the effectively guarantee the normal operation of the network, to effectively ensure the reliability of the computer network.

Conclusion

In this paper, we conduct research on the network intrusion detection system based on the modified particle swarm optimization algorithm. Along with the computer network and the computer system application in various fields in the national life continue to expand, the load types and volume of the business is also increasing. How to reasonably in complex application environment of the system resource allocation and task scheduling, in order to improve the efficiency of computer system and computer network, reduce running cost is a problem to be solved. Under this background, we combine the particle swarm optimization methodology to propose the enhancement countermeasures for the contemporary networks that is meaningful.

Reference

[1] Ye, Zhifan, and Yuanlong Yu. "Network Intrusion Detection." Proceedings of ELM-2014 Volume 2. Springer International Publishing, 2015. 71-80.

[2] Hu, Weiming, et al. "Online adaboost-based parameterized methods for dynamic distributed network intrusion detection." Cybernetics, IEEE Transactions on 44.1 (2014): 66-82.

[3] Mukherjee, Saurabh, and Neelam Sharma. "Intrusion detection using naive Bayes classifier with feature reduction." Procedia Technology 4 (2012): 119-128.

[4] Mantur, Bhimshankar, Abhijeet Desai, and K. S. Nagegowda. "Centralized Control Signature-Based Firewall and Statistical-Based Network Intrusion Detection System (NIDS) in Software Defined Networks (SDN)." Emerging Research in Computing, Information,

Communication and Applications. Springer India, 2015. 497-506.

[5] Hoque, Mohammad Sazzadul, et al. "An implementation of intrusion detection system using genetic algorithm." arXiv preprint arXiv:1204.1336 (2012).

[6] Bao, Fenye, et al. "Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection." Network and Service Management, IEEE Transactions on 9.2 (2012): 169-183.

[7] Shanklin, Steven D., and Gerald S. Lathem. "Parallel intrusion detection sensors with load balancing for high speed networks." U.S. Patent No. 8,239,942. 7 Aug. 2012.

[8] Chauhan, Amanpreet, Gaurav Mishra, and Gulshan Kumar. Survey on data mining techniques in intrusion detection. Lap Lambert Academic Publ, 2012.