Research on the Novel Computer Network Intrusion Detection Model based on Improved Particle Swarm Optimization Algorithm

Juan Fu¹, Hai Hu¹, Leping Wang¹

Abstract

In this paper, we conduct research on the novel computer network intrusion detection model based on improved particle swarm optimization algorithm. TCP flood attack, UDP flood attack, ICMP flood attack, deformity of message attack, the application layer attack is the most typical DDOS attacks, DDOS attacks are also changing to upgrade at the same time, scholars research on DDOS attack defense measures become more and more has the application value and basic practical significance. Network security protection is a comprehensive project, no matter what measures to take that safety is always relative, so as the network security administrator, should change with the network security situation and the security requirements, moderate to adjust security policies, so as to achieve the target. Under this basis, we propose the new perspective on the IDS system that will then enhance the robustness and safetines of the overall network system.

Keywords: Particle Swarm Optimization, Intrusion Detection, Algorithm, Computer Network.

Introduction

With the continuous development of Internet technology that has also created a variety of network applications, there are a huge number of network protocols in network and user data. For common known protocol, these capture tools have been able to identify the corresponding protocol data very well. However, as a private agreement as well as the production of new applications, also exist in the network data capture tools can't identify the unknown protocol, made by traditional based on the analysis of known protocol identification technology can't effectively identify out these unknown protocol, protocol identification technology is facing the challenges, unknown protocol identification technology research will become the research focus of next step.

The root causes of the DDOS attack is not a simple Internet design flaws, by setting the common defense system or modify agreement is irreparable the cause of it lies in the core architecture of the Internet that could be generally summarized as the listed aspects.

- **The incongruity of resources.** The design emphasis of the Internet on the terminal host service guarantee, to ignore the middle network capacity, DDOS attack will have big traffic demand as terminal network only according to the need to apply for the bandwidth, this conflicts with intermediate network capacity is narrow [1-3].

- **The interdependence between the Internet security, access Internet users safety consciousness weak, no in time for the computer to install patches, security holes that make the computer controlled by a hacker, become a puppet host.**

- **Internet design flaws.** The Internet in the early design, there are a number of goals. These targets according to certain significance for sorting. Internet design first target is: even if the network damage of internal or that external damage still can make sure the accessibility and reliability of data transmission.

¹Gongqing College, Nanchang University, Gongqing City, Jiangxi, 332020, China
Although a wireless local area network (LAN) can only consist of a unit, but usually it contains a number of units. This several units through the wireless access point with an AP backbone together, the backbone network that can be a wired network that can also be a wireless network. (1) Outdoor applications. In frequent changes and sudden strong and inconvenient laying network, wireless local area network (LAN) can give full play to its advantages of high rate, flexible and fast networking. (2) Indoor application. Application in the indoor environment, wireless local area network (LAN) as a supplement to the wired LAN, and wired LAN that it is in a large office, workshop, supermarket, intelligent warehouse, such as temporary office, conference room of securities market environment can play a special skill. Particle swarm optimization algorithm is proposed by Kennedy and Eberhart in 1995 bionic algorithm, which is inspired by bird moving regularity of cluster, according to the sociology and psychology and the mathematical models of the swarm intelligence, particle swarm optimization algorithm is a concise form the advantages of flexible, rapid convergence and parameter adjustment mechanism of the evolutionary algorithm, and has been successfully applied to the single objective optimization problem, solve the multi-objective optimization problems is considered to be one of the most promising method. The figure one shows the principles [4].

![Figure 1. The Particle Swarm Optimization Algorithm Architecture.](image)

In this paper, we conduct research on the novel computer network intrusion detection model based on improved particle swarm optimization algorithm. In the later sections, we will discuss in detail.

The Proposed Methodology

**The Clustering Analysis.** Artificial intelligence algorithms such as the neural network and genetic algorithm can obtain high quality of the clustering results, but its computational complexity is often higher, at the same time, the advantages and disadvantages of the clustering results depend on the parameters selection of some experience. For most of the objects in the state and generic there is also the essential list, in order to describe these objects, the proximity between the need to calculate the similarity coefficient of similarity degree between characterization of the objects to be classified, in general need to compute the similarity between objects was classified statistics, establish the fuzzy similar relation on the classified collection of objects as formula one [5].

\[
    r_{ij} = \cos(x_i, x_j) = \frac{\sum_{k=1}^{m} x_{ik} x_{jk}}{\sqrt{\sum_{k=1}^{m} x_{ik}^2 \cdot \sum_{k=1}^{m} x_{jk}^2}} 
\]

Clustering analysis is an important kind of unsupervised learning method and used as a tool of data analysis and its importance in various fields has been widely recognized that can be summarized as:
Based on the hierarchical clustering method. Based on hierarchy clustering algorithm called tree clustering algorithm. The method of using that data connection rule, repeatedly by the hierarchical architecture divided the data or aggregation, to form a hierarchical sequence clustering problem solution. There are two main types of basic algorithm strategy: bottom-up convergent hierarchical clustering and top-down split hierarchical clustering.

Clustering method based on graph theory. Clustering method based on graph theory is used mostly point to the data to indicate the relationship between the data points, compared with other methods, this method is more suitable for the irregular shape of the found data cluster.

The clustering method based on density and grid. Because these two kinds of methods in the processing data are focused on the use of the spatial distribution information of sample points, and are often used together, they can be classified as a class. The method for processing the complicated shape of clusters has obvious advantages [6].

Based on partitioning the clustering method. The advantage of this kind of method can be summed up in convergence speed is fast and easy to expand, the downside is that they often need to specify beforehand clustering number. In addition, the choice of initial cluster centers, the existence of noise data and cluster number set will have great influence to the result.

The purpose of clustering is found between the sample points an objective reflection of the nature of the most essential means. Classification at this point is not the same. Classification need a set of the training samples, by the domain experts to identify sample belongs to the category, which belongs to another kind of sample data, but the classification of the prior knowledge is often is purely subjective and then we define the evaluation criteria as the follows.

\[
distance_{ij}(q) = \left[ \sum_{k=1}^{m} \beta_k \left( F_{ik} - F_{jk} \right) \right]^{1/q}
\]

(2)

The fuzzy transitive closure method can choose according to the classification of the different threshold value is different, thus forming a kind of the dynamic clustering figure, the comprehensive understanding of classification of the sample is more image and intuitive as list steps. (1) According to correlation coefficient matrix and covariance matrix of principal component analysis, calculate the variance contribution rates of the principal component and the distance weighting, and combining the factor loading matrix of principal component name. (2) Input sample observation value, on the basis of the index dimensional difference degree decides the necessity of data standardization. (3) To the principal component instead of the original indicators, this paper defined the weighted distance to classification statistic clustering analysis that combined with the actual situation to determine the category of the classification samples will ultimately.

**The Intrusion Detection Model.** Wireless local area network (LAN) consists of wireless network card, wireless access point AP, computers and related equipment, USES the unit structure, the whole system is divided into many units, each unit is called a basic service BSS, there are three ways of BSS.

- **Distribution of equation.** BSS in any two terminals can communicate directly, without having to transfer station. This way has simple structure, easy to use, but smaller BSS region.
- **Centralized control.** Each BSS is controlled by a central station, and the terminal under the coordinate of the center in the net and other terminal communications. In this way need to use more expensive center, but the BSS area is larger.
- **In the wireless local area network (LAN) in many areas can use an external antenna connect remote LAN and local networks, enlarge the coverage of network.**
In unknown protocol identification process, the stand or fall of the unknown protocol bit-stream feature extraction results will have great influence on later clustering division. In this paper, the unknown protocol bit-stream feature extraction analysis, put forward the agreement is not related to the unknown bit-stream feature extraction method, the unknown protocol for subsequent bit-stream clustering division lay the foundation. Intrusion detection system is a kind of active defense system based on network real-time monitoring the system of network of illegal attacks can advance warning. Network firewall, though to some extent prevent foreign user illegal access to the server, but is unable to effectively prevent internal users, especially for data driven type of attack means, and intrusion detection system can make up the defects of firewall in this respect. It is the telecom network security problem gets a better solution [7].

The Improved Particle Swarm Optimization Algorithm. In terms of individual optimal solution selection strategy, although most of these algorithms in order to reduce the computational overhead and retain only a Pareto optimal solution, but only an individual optimal solution is not enough to describe the individual Pareto optimal front. Branke and Abido respectively to study the individual using external files saved Pareto optimal solution method, obtained better performance than a single individual Pareto optimal solution. In addition, to maximize minimum distance between individual and weighting and strategy is used to select individual optimal solution as the standard.

Determination of correlation analysis is to study the relationship of things, they contact closely, reveals the changes of the specific form and regularity of statistical methods. In relevance theory, the linear correlation coefficient analysis of the correlation between random variables is an important tool. But in recent years has found that the linear correlation coefficient in describing the correlation has certain defects, the comprehensive analysis of copulas connects function for correlation provides new way and we should revise the traditional PSO with the listed guidelines.

Individual fitness evaluation determines the multi-objective particle swarm optimization algorithm to select the global optimal solution and maintain files the two key strategies. But the current individual fitness measure is a single, or is based on the density of the diversity of evaluation to examine the individual potential, or is based on the Pareto dominant relationship of convergence of assessment to examine the individual potential [8].

The global optimal solution changed frequently and fast convergence characteristics, the development and exploitation of equilibrium problem is more outstanding in multi-objective particle swarm optimization algorithm: excessive development will lead to lack of convergence and optimization precision, and excessive exploitation will lead to fall into local extremum lack of the diversity. Although there have been the adaptive particle swarm optimization algorithm for single target.

With no constraint optimization problem, the initial particle population have not consume a lot of time, and for a optimization problem with constraints, if still using randomly generated, it is difficult to
produce to meet the constraint condition of initial particles, so in the process of generating of initial population will consume large amounts of time, in order to solve the generating the initial particle swarm quickly, in this paper, using the following ways to produce.

\[
Random_{k,m} = \left[ K \frac{f_{k,m} - f_{m}^{\text{min}}}{f_{m}^{\text{max}} - f_{m}^{\text{min}}} \right]
\]  

(3)

The Novel Computer Network Architecture Enhancement. The demand of general network management is various, the function of network management is also with the development of the demand and technology and general constantly improve. From a technical perspective, the network management system should be able to realize network fault diagnosis and management, configuration management, security management, network traffic control, billing management function and general management functions such as network routing strategy that can be organized as the listed aspects. (1) Performance management: monitoring network of all kinds of performance data, the examination of the threshold value, and to automatically analyze the current performance data, history data. (2) The configuration management: its main functions include basic network topology relations, network equipment configuration of the monitoring and management, according to the prior condition of the definition of refactoring network, etc. (3) Safety management: mainly is the management of the access network resources including user authentication, permissions, approvals and network access control (firewall), and other functions. (4) Failure management: its main function is to fault detection, diagnosis and treatment, discovery, report.

The traditional information system security model is aimed at single system environment, the network environment security is not well described and dynamic threats as system vulnerability of no response, the traditional security model is the static security model. But with the further development of network, it cannot fully adapt to the dynamic change of Internet security issues. After found the intrusion behavior, to cut off the invasion, timely action against further damage of the attacker, make timely and accurate response is a must. Using the real-time response blocking system, attack source tracking system, evidence system and the necessary response system to ensure the accurate, effective and timely response and to prevent similar events happen again and to provide possible to capture the attacker, to provide effective protection against hackers.

Conclusion

In this paper, we conduct research on the novel computer network intrusion detection model based on improved particle swarm optimization algorithm. With the rapid development of network, the user for the security of the network data communication put forward higher requirements, especially for an increasing number of the broadband access business at present, for every household between hosts isolation from each other. The traditional solution is to assign each customer a VLAN and related IP subnet, through the use of the VLAN, in the data link layer can be isolated, each host can prevent malicious network attack behavior and Ethernet data snooping. Our paper enhances the traditional PSO with the implementation of the IDS that is innovative.

References


