International Journal of Security and Its Applications
Vol. 9, No. 4 (2015), pp. 141-152
http://dx.doi.org/10.14257/ijsia.2015.9.4.14

Based on the Ant Colony Algorithm is a Distributed Intrusion Detection Method

Yiran Wang and Chunxia Wang

School of Computer Science and Technology, Zhoukou Normal University, Henan Zhoukou, 466001, China
Department of Computer and Information Technology, Shangqiu Normal College, Henan Shangqiu, 476000, China
wangyiran76@163.com

Abstract

This paper analyzes the present situation of the current network security problems and points out the research and development of intrusion detection system has very important significance on the basis of comparative analysis of the traditional static security model and PPDR dynamic security model, and according to this model, using ant colony algorithm is a distributed computing network intrusion of metrics, the determination of index contrast and invasion route, increase the accuracy of testing operation and calculation results show that the effectiveness of the solution and the convergence speed. For distributed network intrusion is put forward a new kind of means.

Keywords*: Network security; Intrusion detection; The invasion of the path; Precision*

1. Introduction

With finding wider and wider with the application of network technology, computer network has become the indispensable part of people's life not only, also has become the important platform of e-commerce and e-government, at the same time the network space is likely to become the main battlefield of the future war[1]. As a result, governments have attached great importance to the network security technology research and product development work, and even put it on the height of the political. So the network security technology research and development is a very necessary and very urgent task.

With the development of computer network technology and its application, the traditional security model cannot adapt to the new network environment, static security model gradually transition to the dynamic security model. IIS PPDR model is put forward, PPDR model including strategy, protection, detection and response to four parts.Detect the intrusion detection, it is PPDR model as the key to a dynamic security model.Intrusion detection is a kind of active safety technology, it can be for external attacks, internal real-time monitoring and defense, attack and mis operation is the complement of traditional computer security technology. At present, foreign intrusion detection products have 155 company Realsecure, Cisco CiseoSeeureIDS, NFRS NID and NAI company, etc. In 155 the company of the most advanced intelligent detection technology; And domestic most products still adopts the traditional intrusion detection pattern matching method, the traditional pattern matching detection method has a lot of disadvantages such as low efficiency. Now many companies have invested on international energy for the next generation of intrusion detection technology research, some domestic research institutions and enterprises also began in-depth intrusion detection technology research and product development work. Intrusion detection technology will play an increasingly important role in network security, and so on intrusion detection technology research is of great significance. The goal of this article is to design a distributed intrusion detection system based on network, it has high efficiency, scalability, and security[2-4].

ISSN: 1738-9976 IJSIA

But with the further development of the network, these standards cannot meet the needs of the current technology. Because these standards are based on the environment of host terminal environment model, so they cannot adapt to the rapid development of distributed, dynamic and network environment. The traditional information security technology is concentrated in the reinforcement and protection of the system itself. For example, the class B operation system database, export configuration in the network firewall, encryption techniques are used in information transmission and storage, using a centralized identity authentication products, etc. Simple protection technology, however, there are many problems: first, pure protection technology is easy to cause system construction blindly, this blind includes two aspects: on the one hand, do not understand security threats and the current security situation of serious; On the other hand is a safe investment is too large and there is no real grasp security key link, cause unnecessary waste.For example, a reservoir dam should be built? Have any bugs fixed dam dam is a state of dangerous now. In fact, need corresponding detection mechanism, for example, using engineering testing technology to check the quality of the dam is in line with the requirements, observe whether the current water level exceeded the warning level. Such detection mechanisms to ensure the safety of the dam is very important. Second, the firewall policy to prevent hackers have their obvious limitations. Firewall technology is one of the most important security technology in the Intranet, its main function is to control unauthorized access to the protected network, it by monitoring, the limit, change the flow of data through the network, on the one hand, as far as possible external shielding Intranet topology structure, internal shielding external dangerous site on the other hand, to prevent internal, external illegal access.(1) inside the firewall is hard to prevent. Firewall security control can only be applied to internal or external, namely: the external shielding Intranet topologies, blocking external Internet users connected to the Intranet site or some important port, internal shielding external dangerous sites, but it is difficult to solve the problem of Intranet control internal personnel's safety, prevent outside rather than inside. And that, according to the statistical results show that the authorities on the network security attacks more than 70% from internal attack.(2) the firewall is hard to management and configuration, easy cause security vulnerabilities. Firewall configuration and management of complex, to successfully maintaining a firewall, firewall administrator to the requirements of the network security attack means and its relationship with the system configuration is quite profound understanding of, and the firewall security strategy can't for centralized management.(3) maintain the security of information system, the classical approach is "access control" or "access control", this means in the classical and the modern theory of security is a system security strategy is the most important means. But so far, the software engineering technology haven't reached A2 level required in the form of a generation or prove the degree of a system of security system, it is not possible one hundred percent guarantee on any system (especially the underlying system) doesn't exist in security vulnerabilities. And, whether in theory or in practice, trying to fill a system security vulnerabilities are not possible, also is not a viable solution to legitimate users through the "identification" or "identity" abuse the privilege[5-7].

PPDR model thought is in the overall security strategy of control and guidance, on the basis of the integrated use of protective tools, use the current detection tools to understand and evaluate the system safety state, and then through the appropriate Response measures to adjust the system to (Response) "the safest, and" the lowest risk "status. Protection, detection and Response of a complete cycle, dynamic security. Intrusion detection is detection of PPDR model, its role is to connect the process of protection and Response. Intrusion detection is the key to PPDR model, we can use this 155 is a leading global supplier of intrusion detection system of the fact that the core of the intrusion detection technology in the whole PPDR model.

2. Related Research

Intrusion detection is defined as recognition for computer or network resources malicious intent and behavior, and respond to process. Intrusion detection system is the system to complete the above function. Intrusion detection system can detect unauthorized object (or program) for intrusion attempts or behavior of the system, at the same time monitoring the illegal operation of system resources authorization object. Intrusion detection system generally includes three parts: information collection and pretreatment, data analysis and response system. Intrusion behavior mainly refers to the unauthorized use of system resources, may cause the loss of the system data and damage as well as the system the dangers of denial of service. For intrusion detection of network attack can be divided into the following four categories: (1) by examining a single IP packet header (including TCP and UDP) can be found in attack (2) by examining a single packet header, but at the same time to check all the data segment information can be found, (3) the top frequency detection can detect attack, (4) using fragmentation attacks, such attacks using the loopholes in shard reorganization algorithm avoid intrusion examining fin system inspection and attack. If you want to check such attacks, must be restructuring try in advance [8].

An intrusion detection system design requirements include: (l) real-time requirements: if you attempt to attack or attacks can be found as soon as possible, it makes possible to find out the location of the attacker, to prevent further attacks, and could control the damage in minimal, system, at the same time can record the process of all the attackers activities, and can be used as evidence for playback. Real-time intrusion detection can reduce administrator through the audit system log to find clues to intruders or invasion behavior of many inconvenient.(2) scalability requirements: because there are thousands of different means of known and unknown attacks, they attack behavior characteristics are different. So it is necessary to establish a mechanism, the system architecture of intrusion detection system and use strategies. For establishing a intrusion detection system must be able to ensure that, in the presence of new attack types can through some mechanism, such as update feature library mechanism) without the need to change under the condition of intrusion detection system itself, the system can detect new attacks. On the function of the intrusion detection system design, also want to use an extensible architecture, so that the system structure itself to adapt to the future possible extension requirements.(3) the adaptability requirement: intrusion detection system must be able to apply to a variety of different environments. For example: in the high speed large capacity computer network environment, increase the number of the computer system in the environment, change the computer system types, intrusion detection system should still be able to normal work. Adaptability requirements including the adaptability of intrusion detection system itself to its host platform, namely: the ability to work across platforms, and adapt to its host platform of software and hardware configuration of all kinds of different situations.(4) the security requirement: intrusion detection system must be robust (robust), not to its host computer systems and its computer environment, the introduction of new security issues and safety concerns.(5) the validity requirements: must be practical and effective intrusion detection system, that is to say, to attack the misstatement can be controlled within a certain range and omission[9].

At present, intrusion detection technology has two types: anomaly detection and pattern matching detection technology. Anomaly intrusion detection technology based on user behavior or resource use to judge whether the invasion, and does not depend on the specific behavior whether to test; And pattern matching detection technology is based on some specific behavior judgment reasoning, so as to detect intrusions. Anomaly detection is trying to find some unknown intrusion behavior, and pattern matching detection is identified some known intrusion behavior. With real-time requirements of network security tool, first of all, it must be safe, that means does not bring system because of the

introduction of other security issues. It has a reasonable system structure to ensure that the detection of real-time and effectiveness, at the same time, we must give full consideration to the demand of the practical application environment, so you can determine the following design principles and strategies of distributed intrusion detection systems:

(l) USES the distributed monitoring and centralized management mode, through a management site monitoring distributed in several monitor on the network;

(2) applying the idea of modular components to make the system has good expansibility to detect new intrusion behaviors are always present;

(3) to minimize the impact on the system and network performance and resource usage.

(4) through the knowledge base to detect intrusion rules, can adapt to hundreds of different from a single computer system to computer system made up of different computer environment;

(5) the intrusion of omission and false positives can control in a reasonable range.

Distributed intrusion detection system based on network is mainly composed of five parts: the network engine, storage system, analysis system, response system, the console.

Storage system is used to store raw data from the network engine and analysis of the system to produce the results of the analysis, and other important data. Raw data stored in the invaders during the legal sanction to present solid evidence. Storage system is also between different components of Shared database, it's different for the system components provide data of particular interest. Therefore, the storage system should provide flexible data maintenance, processing and query service. Analysis system is used to analyze the data packets from network engine, and processing. Analysis system including pretreatment module, rule knowledge base, protocol analysis module, data analysis module and secure communication of five parts. Analysis system is the core of the intrusion detection system, pattern matching detection based on protocol analysis technology is the guarantee of system efficiency. The height of the protocol analysis technology using the network protocol standardization features to quickly detect attacks. The detection technology of small amount of calculation, even in a high load on the network, can also detect various kinds of attacks, without packet loss. Response system is take corresponding measures to the invasion of the has been recognized by the behavior of systems. The response measures include: (l) the alarm measures, such as: E-mail administrator, send the console warning message;(2) the protective measures, such as: to cut off the invaders TCP connection, modify the router access strategy, etc. The console is the interface of the intrusion detection system and user interaction. Each monitor user can through the console configuration in the system, and by understanding the operating condition of monitor console.

3. The Model of Network

The function of the network engine is set the network interface to mixed mode to monitor the network interface, and reach the network packet interception down, for the use of analysis system. Engine will read all of the network traffic, including all protocol port, all subnets, host of all the data, but in practice, there are a number of users do not need to be concerned with data, called the garbage data, garbage data occupies a great proportion in all traffic, improve work efficiency, seriously affected the system therefore efficient information filtering system is an important part of information to monitor, it allows the user to specify a particular subnet, and host specific protocol such as HTTP, FTP, SMTP port for filter, only will users concerned about sensitive data submitted to the top, thus enhances the working efficiency of the system.

Analysis system is to lead climb from the network, the network data analysis and processing system. Analysis system is the core of the whole distributed intrusion detection system based on network, and analyzing system adopted by the analysis of the detection method is the key to the whole system performance level, we use the improved

method of traditional pattern matching, that is, the pattern matching detection based on protocol analysis technology. Rule knowledge base is a known network attack behavior characteristics of library, and if there is no rule knowledge base, the system can't identify any aggression. How to use the simple and easy to use and effective language to describe an attack behavior characteristics, is a key problem of the system. In judging whether a network packets for judging when an attack is mainly port of the packet and the data content, and IP address, protocol type, and TCP marks just auxiliary feature codes.So should analysis the raw network packet in the first place, the matching port directly and the content of the data segment? For some network packet inspection, directly determine port and data content, detection efficiency is higher. But as a result of intrusion system is aimed at all network packets on a test to determine whether any aggression, so you should follow the first detection of all the common features of aggressive behavior and then the principle of individual characteristics, for example, if the first detection of 1 p address, once found that does not belong to test scope, test as soon as the next packet and not continue to test other fields in the packet. This not only ensure the efficiency of the system of the whole test, and improve the real-time alarm.

Each rule in logically divided into two parts: the rules the head and options. Header defines the rules of behavior, to match the network packet protocol, source address, destination address, net mask, source port and destination port. Rule options including the alarm information is used to display to the user and used to judge whether this packet to attack packets of other information. Rules of the rules of the general format is: < operation > < agreement > < source host IP > < source port > < direction operator > < target host IP > < port > (< rule option 1:1 > : < rule option 2: value 2 >,..., n > < n rules options: value; the head, the rules of parentheses to the left of the part is in parentheses is part of the rule option. Rules option a colon in front part is called option keywords. Not any rules rules options section is required, it is used to define a certain attack behavior, and need to take some actions (such as Sue on behalf of) the packets. Only composition rules of each part must meet to perform the corresponding operation at the same time, limit the various elements of a message is "logical relationship with the"; at the same time, the rules between various rules in the knowledge base is a logical "or" relationship. Rules contain the address of the packet header information, protocol information, and when the packet conform to attack what action to take when each component of the rules of the information. Rules of the first field is the behavior of the head, the second field is the agreement, the third field is the address and port information. Rules of behavior that when found eligible packets should do something. Include three operating behavior: alert, log, pass.

Rule knowledge base of the rule set is divided into two kinds: one kind is depending on the type of service application layer to establish the set of rules. Such as FTP. Ural's set contains FTP service rules, DNS. rules set contains DNS service attack rules, Telnet. Urels set contains at P service attack rules; Another kind is classified depending on the type of attack, such as DOS. The rules set contains a denial-of-service attack class rules, backdoor. Urels set contains the back door of the related rules. Through the classification management rules, we can easy to update rule knowledge base management.

Pretreatment is mainly completed restructuring of network packets. Protocol analysis includes each child in specific protocol analysis module: HTTP protocol analysis, the FTP protocol analysis, TENLET protocol analysis, SMTP and POP3 protocol analysis, the IMAP protocol, TFTP protocol analysis and RPC protocol analysis module. Protocol analysis: to complete the following two main work TENLET, SMTP, IMAP, POP3 protocol is character-oriented protocol, so data preprocessing transmitted to come from a single protocol message, need to deal with the protocol processing module for caching, command as stipulated in the agreement to end (end with a carriage return said), successive a few packets restructuring into a full command to attack feature matching pattern detection, in the process of restructuring of data packets, and to some special type

of package to specific client agreement characters for the corresponding processing, including the agreement itself commands, whitespace, etc. In the protocol analysis, to determine some simple intrusion behavior. HTTP protocol analysis, for example, after receive the FTP protocol message, judge the integrity of the first message, and then calculate the length of the HTTP commands and parameters, if you find that is greater than the length of a given, can be considered to be the HTTP command buffer overflow attack. Generate alarm signal to the response module directly. Without having to continue to the data analysis module, can enhance the real-time intrusion detection system detection, and reduces the attack features matching resources burden of pattern detection intrusion behavior.

4. Path Search based on Ant Colony Algorithm

The most short circuit search algorithm, compared with other in large-scale network is the most short circuit search, ant colony algorithm has the advantage that the model is simple and fast computing speed.But there are also two problems: first, ant colony is the movement of the individuals in random, although through information exchange can towards the optimal path of evolution, but a large number of chaotic search in the path of a shorter path is difficult, especially at the beginning of the iteration, due to the information in the network element uniform distribution, the ants in the absence of any induction search path is very long, and the path to the poor quality, not only reduce the efficiency of the algorithm and does not favor the algorithm convergence; Second, the pheromone update rule is the core of the ant colony algorithm, determine the advantages and disadvantages of the final solution. An update that will accelerate the algorithm convergence leads to fall into local optimal solution, and too low update will reduce the efficiency of the algorithm, the algorithm convergence not a short time. Under the large-scale network, each path searching starting point and end point, fixed pheromone values cannot satisfy the convergence condition of optimal solution under different query conditions, according to the above problem, this paper puts forward the corresponding improvement program. In order to avoid the ant choice of path is too "remote", made the new travel rules of the ant, can ensure that every ant from starting point to find a shorter route to the finish. When ants every reach a new node, first of all determine whether the current track table is a shorter path to the current node, ants is deleted when the track of the current table in the middle of the node, and then the next node selection.

Add 1 attribute values, when other ants to path selection, can combine cuts time value to a certain degree of path selection probability weighted, induction of ants to avoid the "remote" sections. After weighting of ants by node I to node j path selection probability calculation method as shown in type (1) :

$$P_{ij}^{k}=\begin{cases}\dfrac{\tau_{ij}^{\alpha}\eta_{ij}^{\beta}0.88^{c_{ij}}}{\sum_{s}\tau_{is}^{\alpha}\eta_{is}^{\beta}0.88^{c_{is}}}, & j\in \text{all nodes}\\ 0, & \text{otherwise}\end{cases} \quad (1)$$

Among them, τ_{ij}^{α} for each node between the score probability, η_{ij}^{β} represents the probability of expectation between two nodes. According to the different topology structure, can according to need, for different needs α and β different length of topological structure of the node.

Other qualified an ant's longest distance, when the distance is too long to stop its path choice behavior and put it as a starting point to choose. For improving design search search results before and after the experiment, the experiment set species, including 30 ant iterations for 200 times, the search for the shortest distance path. shows the improved path search strategy before and after the initial population to complete the search of the time,

the contrast between the average path length, therefore, after the improved algorithm of initial population before completing the search time is improved by 29.9%, and the improved search path length was 78.7% lower than before.

Slave swarm algorithm can see as a kind of based on parameterized probability distribution model of the solution space, solution space parameterized probability model parameters is pheromones, therefore the pheromone update rule is the core of the ant colony algorithm, directly affect the convergence speed and quality of the optimal solution, all the ants in completing a path search process from start to finish, usually for the update of velocities of the information, update methods m. own had given three different model to calculate the pheromone increment, respectively is week of ant system, ant system and ant system, calculation method, such as type (2) :

$$\Delta\tau_{ij}^{k}=\begin{cases} M & \text{routing} \\ 0 & \text{otherwise} \end{cases} \quad (2)$$

The number system can be calculated as (3)

$$\Delta\tau_{ij}^{k}=\begin{cases} M/d_{ij} & \text{routing} \\ 0 & \text{otherwise} \end{cases} \quad (3)$$

Around the system such as type (4) can be calculated

$$\Delta\tau_{ij}^{k}=\begin{cases} M/L_{ij} & \text{routing} \\ 0 & \text{otherwise} \end{cases} \quad (4)$$

M on behalf of each path of which needs the amount of information, and d_{ij} represents the distance between two nodes, L_{ij} on behalf of the transmission time between two nodes. All three of these systems, the different paths on the amount of pheromone in the search operation, is a fixed value, depending on the search path, however, the size of the pheromone update every time there is a big difference, and three kinds of calculation methods for all path search to put a certain amount of pheromone, not only large amount of calculation, and caused the pheromone on the waste, played down the preferential rules, due to slow convergence speed of algorithm. Some researchers think they can find the optimal solution in the current loop or trajectory of the global optimal solution according to the three kinds of update policy updates, but easy to make pheromone concentration in one of the shortest path to the prematurity of the algorithm. So research how to update the pheromone distribution of diversification, after make the path selection of presents diversification, to make the algorithm faster convergence to the best path.

Using ant colony algorithm to solve dynamic route choice question, generally choose the path travel time as the main evaluation standard in the shortest path, according to the size of the travel time to update information so as to induce convergence to the optimal solution. Application is another advantage of ant colony algorithm to solve the problem, in the most short circuit, to solve the dynamic can need not consider the time characteristic of the network, the search process and route travel time calculation points in the process of me alone, in the search is complete, you can have a choice of some paths for the calculation of travel time, so that we can avoid unnecessary calculation.

According to the improved ant colony algorithm thought and based on the average speed of the dynamic travel time calculation method, this paper get the most short circuit implementation of the algorithm is used to calculate the dynamic steps are as follows:

Step 1: global parameters initialization, including road network data structure (including the section number, node number, and some corresponding road network according to the query time choice of period of time average velocity), each section of road network global pheromone initial value;

Step 2: the initialization of C = C + 1 N ant, will only ^ ant path table set to null, set its starting point and end point;

Step 3: for each ant carried out in accordance with the rules of type (2-4) route choice, for each ant, in front of the search for new path, first check whether the pre-given trajectory can be optimized and the optimized sections cut attribute value plus one, and

then according to the path selection method to the next node, if choose the road cuts attribute values greater than zero, then the road cuts attribute value minus 1, will search for the new path to put in the table of the path, and more temporary pheromone value of the road.

Step 4: repeat step 2 to step 3, until the iterative coefficient C is equal to the NC;

Step 5: select in the local optimal solution of each iteration to get the global optimal solution, the shortest path for global shortest path, and outputs the trajectory, distance and travel time.

Most of existing research and application of ant colony algorithm for smaller problems, only for large-scale problem does not have many research and application of ant colony algorithm. And actual application problem tends to be large and even very large scale problems, aiming at such problems, choosing the right to design the ant colony algorithm for solving the parallel strategy, will greatly reduce the computing time, make the algorithm more time sensitive.

For some complex model, the solution space giant complex system dynamic optimization problem solving, artificial intelligence algorithm as the most promising method. But artificial intelligence algorithm is also need a lot of computing resources and storage space, when to solve some dynamic optimization or mass optimization is still a certain degree of restriction. A single processor computing power is the main bottleneck, with the development of computer technology, distributed parallel computing system based on network connection to solve complex large system dynamic optimization problems become the research focus in the today. In parallel to solve the key problem to solve in accordance with the data and tasks divided into several pieces. In the application of ant colony algorithm for solving large-scale shortest path search, from the perspective of data on algorithm it is difficult to divide, because the network characteristics of space and time, obviously, the distribution of stored in different computer, can lead to the ant search in different computer nodes, which can lead to traffic is larger, with poor efficiency. But from the perspective of task partitioning, ant colony algorithm has the advantages of natural ant colony algorithm in essence is a parallel search technology, every time because of the ant colony algorithm to send iv ants from starting point to find a path to the finish, this process is very suitable for parallelization.

5. Simulation Results

Path search experimental run in a distributed cluster based on network environment, the node as the ordinary PC, through 10 MBPS Ethernet connectivity between nodes, each node are installing Linux operating system, in this paper, in this paper, we adopt the Ubuntu system, and install MPICH2 configuration software. In addition, network information is stored in every node can be in the same way to access the database, this paper USES the Mysql database. MPICH way is to use file sharing and remote access to distributed computing, need to make some special configuration in the environment: first of all on each PC build the same user name and password; And then set the same Shared directory path; Run the MPI program node should be turned off at the end of the firewall or add to run the program to its own firewall trust list, other configuration shall be carried out in accordance with the manual of MPICH. Ant colony algorithm, there are many parameters in the parameter value of the set have the potential to influence the overall performance of algorithm, this section mainly studies the ant number m, the number of iterations m, coefficient of pheromone and heuristic information coefficient's influence on the algorithm, and through the simulation experiments to determine the various parameters in ant colony algorithm of the optimal set value.(1) the number of ants and the selection of number of iterations, ant colony algorithm is through more sets of feasible solution of group evolution to find the optimal solution, in the evolutionary process, the feasible solution of each iteration is the adaptability of single group, the whole process of

iterative process performance for the evolution of the population, the more the ants population adaptability, the better, the longer the evolution was the greater the probability of the global optimal solution, but the excessive number of search will cause too big amount of calculation and affect the computational efficiency. This article will through the simulation experiment method to determine the optimal number of ants m and the number of iterations NC. Pheromone coefficient reflects the ants accumulated in the process of sports information relative important degree, in the ant colony search heuristic information coefficient reflects the ant heuristic information in the process of movement (expected) relative importance in the ant search. The duty is too big, can lead to the ants, according to the guide to search of pheromone, if the value is big, can lead to local convergence of the path, and instead if the value is too small, and value is small, ant colony of random search process, algorithm convergence. The scope of selection and appropriately, ant colony algorithm can not only achieve good results, but also can improve the performance of the algorithm.

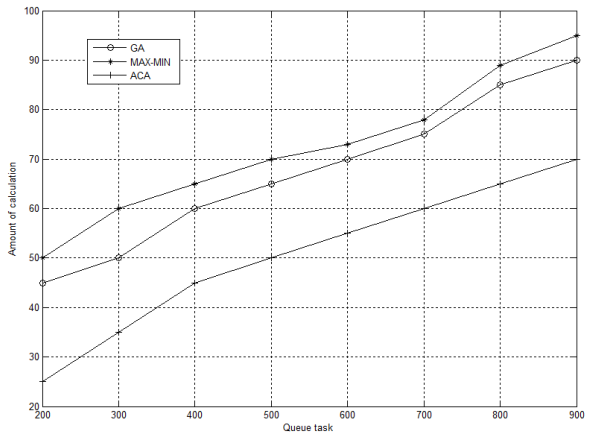

Figure 1. Amount of Calculation V.S. Queue Task

See from figure 1, intelligent algorithms such as ant colony optimization scheduling algorithm with Max - min and Mm - Mm compared to the traditional scheduling algorithms such as load balancing degree is higher. This is because in the process of task scheduling, intelligent algorithm can adjust system resource nodes of real-time load, the node will not only focus on advantage, let more idle resources nodes assigned to the task. In three intelligent algorithms, the swarm algorithm of load balance degree is best, this is because the colony algorithm is better than other intelligent algorithms pay close attention to the results of the system resource load. The intersections of both said that the scheduling algorithm in the time span of the scale under heterogeneous task queue, milliseconds. According to the time span algorithm time span of the experimental data contrast diagram is shown in figure 2.The abscissa for heterogeneous task queue size, the unit for a heterogeneous task. Ordinate of time span, the smaller the value represents the system execution time faster, the higher the efficiency, also more balanced load, the better the performance of load balancing algorithm.

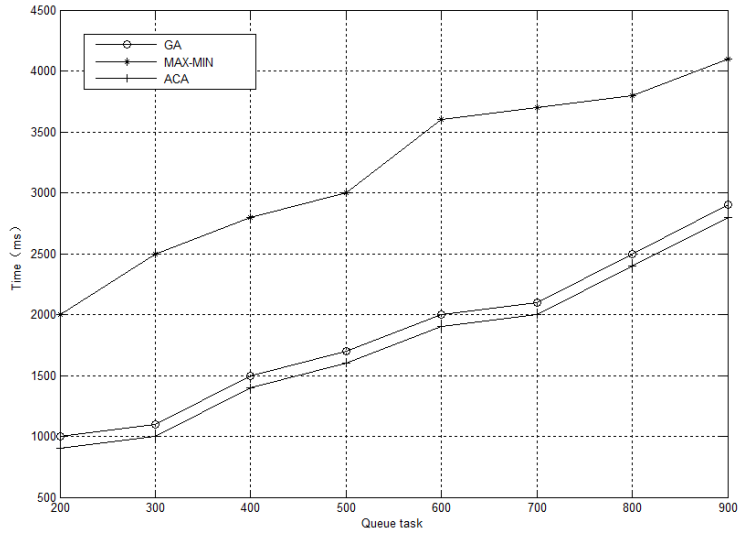

Figure 2. Time V.S. Queue Task

Can be seen from figure 2, intelligent algorithm in the time span is also superior to the traditional with the Max - min algorithm. Although intelligent algorithm needs to be collected in the process of scheduling system load information and update the maintenance information, it will cost some time. But this is relative to the Max - min algorithm and min - min algorithm need to sort the amount of time is much smaller. And ordering in large quantity of data when the time will be rapid growth. Intelligent algorithm of the time have a relatively flat growth, its update of system information to maintain the amount of the quantity of the change of time and task is always in the same order of magnitude .In three intelligent algorithm, the scheduling time is the smallest of genetic algorithm, this is because the genetic algorithm focuses only on the load of the whole system change, only to have obtained the solution of comment, greatly reduced the amount of time spent by information collection system, able to quickly produce scheduling scheme according to the previous generation solution.

6. Conclusions

This article through to the invasion of the network topology structure and transmission characteristics of the model, and on this basis, the ant colony algorithm was realized according to the probability calculation for invading path search, the results of simulation has great advantage in search of convergence, can in the shortest possible time to invasion path search, and according to the search path, you can get better network load.

Acknowledgements

This work is financially supported by basic and frontier project of Science and Technology Department of Henan province, China (No 142300410334), the funding scheme for young backbone teachers of colleges and universities in Henan Province, China.

References

[1] A. Perrig, J. Stankovic and D. Wagner, "Security in wireless sensor networks", Communications of the ACM, vol. 47, no. 6, **(2004)**, pp. 53-57.
[2] P. C. Hershey, "Network security system and method using a parallel finite state machine adaptive active monitor and responder", vol. 414,833, no. 9, **(1995)**.
[3] K. Vieira, "Intrusion detection for grid and cloud computing", It Professional, vol. 12, no. 4 **(2010)**, pp. 38-43.
[4] S. X. Wu and W. Banzhaf, "The use of computational intelligence in intrusion detection systems: A review", Applied Soft Computing, vol. 10, no. 1, **(2010)**, pp. 1-35.
[5] E. S. Shakshuki, N. Kang and T. R. Sheltami, "EAACK—a secure intrusion-detection system for MANETs", Industrial Electronics, IEEE Transactions, vol. 60, no. 3, **(2013)**, pp. 1089-1098.
[6] R. Berthier, W. H. Sanders and H. Khurana, "Intrusion detection for advanced metering infrastructures: Requirements and architectural directions", Smart Grid Communications (SmartGridComm), First IEEE International Conference, IEEE, **(2010)**.
[7] F. Bao, "Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection", Network and Service Management, IEEE Transactions, vol. 9, no. 2, **(2012)**, 169-183.
[8] R. Berthier and W. H. Sanders, "Specification-based intrusion detection for advanced metering infrastructures", Dependable Computing (PRDC), IEEE 17th Pacific Rim International Symposium, IEEE, **(2011)**.
[9] Y. H. Li, "An efficient intrusion detection system based on support vector machines and gradually feature removal method", Expert Systems with Applications, vol. 39, no. 1, **(2012)**, pp. 424-430.

Authors

Yiran Wang, he received B.Eng and M.Eng Degree in Computer Science and Technology from ZhengZhou University, China in 1997 and 2005 respectively. He is currently researching on Internet of things, enterprise informationization.

Chunxia Wang, she received B.Eng and M.Eng Degree in Computer Science and Technology from ZhengZhou University, China in 1997 and 2004 respectively. She is currently researching on Internet of things, Data mining.