Research on Automatic Defense Network Active Attack Data Location and Early Warning Method

Jian-zhong Huang[1(✉)] and Wen-da Xie[2]

[1] Modern Education Technology Center, Jiangmen Polytechnic, Jiangmen 529030, China
baihuahualai2018@163.com
[2] Computer Engineering Technical College (Artificial Intelligence College), Guangdong Polytechnic of Science and Technology, Zhuhai 519090, China

Abstract. The traditional automatic defense network active attack data location and early warning method has the shortcoming of poor localization performance, so the research of automatic defense network active attack data location and warning method is put forward. The active attack data is detected by the space distance of the network node data, and the active attack data is judged whether there is active attack data in the network, which is based on the detected active attack data. The multi-objective binary particle swarm optimization (BPSO) algorithm is used to obtain the optimal task allocation scheme for active attack data location. Based on it, the algorithm of extreme learning machine is used to realize the location and early warning of active attack data. Through the experiment, put forward the automatic Compared with traditional methods, the convergence value of active attack data location and early warning method of defensive network increases 23.61 and the error rate of location decreases by 15. It is fully explained that the proposed automatic defense network active attack data location and early warning method has better localization performance.

Keywords: Automatic defense · Network · Active attack data · Location · Early warning

1 Introduction

With the continuous development of Internet technology, the network usage rate is gradually increasing. Nowadays, the network has reached a popular state, but due to the openness of the network, the security of the network cannot be well protected. To ensure the security of the network, it is necessary to carry out corresponding positioning warning and processing of its active attack data to ensure the security of the network environment [1].

In recent years, network security has gradually been valued by many scholars, and more research has been done on the automatic defense, location, and early warning methods of network attack data. Automatic defense network active attack data location and early warning is the premise of network attack blocking and service recovery, and is the key link to ensure optical network security. The characteristics of the network

S. Liu and L. Xia (Eds.): ADHIP 2020, LNICST 347, pp. 262–272, 2021.
https://doi.org/10.1007/978-3-030-67871-5_24

itself make it face more security threats than traditional wired and wireless networks, and active attacks are one of the challenges that must be overcome in the security field [2]. In recent years, domestic and foreign scholars have studied the data and early warning of active attack data, and obtained some research results, but the active attack research in the network is still a challenging problem, which needs further research [3]. The traditional automatic defense network active attack data location and early warning method has the defect of poor positioning performance, which can not meet the needs of more and more network active attack data location and early warning. Therefore, the research on automatic defense network active attack data location and early warning method is proposed [4].

2 Design of Automatic Defense Network Active Attack Data Location and Early Warning Method

2.1 Active Attack Data Detection

In order to locate and alert the active attack data, it is first necessary to detect whether there is active attack data in the network data. In this paper, the active attack data is detected by the spatial distance of the network node data. The specific process is as follows.

Suppose there are n beacon nodes and m unknown nodes in the network. For an unknown node, its node i data can be represented by a vector as

$$RSS_i = \left\{ s_{i1}, s_{i2}, \cdots, s_{ij}, \cdots, s_{in} \right\}, i = 1, 2, \cdots, m \tag{1}$$

Where RSS_i represents the i th node data; s_{ij} represents the signal strength of the unknown node i sent to the j th beacon node,Then the node data of each unknown node is equivalent to a point in an n-dimensional space. The node data of the same physical location node is close in the signal space, and will fluctuate up and down at a mean value, and there is a certain distance between the node data of different physical location nodes [5].

According to the "distance-loss" model, the calculation formula of s_{ij} is:

$$s_{ij}\left(d_{ij}\right)[dBm] = P(d_o)[dBm] - 10\gamma \log\left(\frac{d_{bj}}{d_{aj}}\right) + \Delta F \tag{2}$$

Where $P(d_o)$ represents the transmit power of node i; d_o indicates the reference distance; d_{ij} represents the ranging distance between the unknown node i and the beacon node j; γ represents the path loss factor. For beacon nodes j. The same $P(d_o)$ of any two unknown nodes a, b.

The node data difference is

$$\Delta s_j^{ab} = s_{aj} - s_{bj} = 10\gamma \log\left(\frac{d_{bj}}{d_{aj}}\right) + \Delta F \tag{3}$$

Where d_{aj}, d_{bj} represents the ranging distance between the node a, b and the beacon node j, respectively.

For n beacon nodes, the node data of Node B is equivalent to two points in the n-dimensional space, and the spatial distance between the two nodes is:

$$D^{ab} = \|RSS_a - RSS_b\| = \sqrt{\sum_{j=1}^{n}\left(\Delta s_j^{ab}\right)^2} \tag{4}$$

Where D^{ab} represents the Euclidean distance of the node a, b.

According to the principle of non-central χ^2 distribution, when two nodes are in different physical locations, $\Delta s_j^{ab}, j = 1, 2, \cdots, n$ obey $N\left(10\gamma \log\left(\frac{d_{bj}}{d_{aj}}\right), 2\sigma^2\right)$ distribution $N\left(10\gamma \log\left(\frac{d_{bj}}{d_{aj}}\right), 2\sigma^2\right)$. Then the probability density function of the node data is

$$f\left(\frac{X}{same}\right) = \frac{1}{2^{\frac{n}{2}}\Gamma\left(\frac{n}{2}\right)} X^{\frac{m}{2}-1} \cdot D^{ab} \tag{5}$$

Where $\Gamma()$ represents the Gamma function; X represents random node data.

The detection of active attack data is implemented according to the comparison of the probability density function of the node data with the threshold. The detection performance depends on the selection of the threshold. If the threshold is too large, the probability that the attacking node is misjudged as a legitimate node increases; if the threshold is too small, the probability that the legitimate node is misjudged as an attacking node increases. After selecting the appropriate threshold, the active attack data is detected. If the probability density function is greater than the threshold, it means that there is no active attack data in the network. If the probability density function is less than the threshold, it means that the network contains active attack data [6]. Through the above process, the detection of the active attack data is realized, and the following is prepared for the positioning and early warning of the active attack data.

2.2 Active Attack Data Location Task Assignment

Based on the above-mentioned detected active attack data, the positioning tasks are allocated correspondingly, and multiple active attack data positioning is realized at the same time, which can greatly improve the efficiency of the automatic defense network active attack data positioning and early warning method. The multi-target binary particle swarm task assignment algorithm is used to allocate active attack data location

tasks. The specific process is as follows [7]. The active attack data location tasks in the network are allocated to obtain a long-lived network life cycle, lower network energy consumption and balanced network load. Therefore, this chapter has designed three objective functions: total task completion time, total energy consumption, and load balancing. The multi-objective binary particle swarm task assignment algorithm is used to determine the optimal allocation scheme [8]. The multi-target binary particle swarm task assignment algorithm is expressed as

$$Minimize \quad f(X_i) = \{f_1(X_i), f_2(X_i), f_3(X_i)\} \tag{6}$$

Among them, $X_i = \{x_{l1}, x_{l2}, \cdots, x_{lj}, \cdots, x_{ln}\}, l = 1, 2, \cdots, q$ represents the decision variable, which corresponds to a distribution scheme of tasks in the particle. f_1 is the total time of the target function task completion, f_2 is the total energy consumption of the objective function, f_3 is the objective function load balance. Therefore, the decision space is q-dimensional and the target space is 3 dimensions,That is, the task allocation scheme is a q-dimensional particle, and an optimal solution set under the f_1, f_2, f_3 3 dimensional objective function.

In the multi-objective binary particle swarm task assignment algorithm, the position X of the particle represents a task assignment scheme, expressed as

$$X = \begin{bmatrix} x_{11} & x_{12} & \cdots & x_{1j} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2j} & \cdots & x_{2n} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ x_{q1} & x_{q2} & \cdots & x_{qj} & \cdots & x_{qn} \end{bmatrix} \tag{7}$$

Among them, $x_{lj} = \{0, 1\}, l = 1, 2, \cdots, q, j = 1, 2, \cdots, n$, x_{lj} indicates the state in which the beacon node joins the task, 0 means unselected, and 1 means selected.

The velocity of a particle indicates the probability of a change in particle position. If the velocity of the particle is large, the probability that the particle position is taken as 1 is large. If the velocity value of the particle is small, the probability that the particle position is taken 1 is small.

The individual extremum of each particle is denoted as $pb = \left(pb_{ij}\right)_{q \times n}$, and the global extremum of the entire particle swarm is denoted as $pg = \left(pg_{ij}\right)_{q \times n}$.

The update formula for particle position A is

$$x_{lj}(t+1) = \begin{cases} 0, & if \quad rand() \geq S\left(v_{lj}(t+1)\right) \\ 1, & if \quad rand() < S\left(v_{lj}(t+1)\right) \end{cases} \tag{8}$$

Among them, $S\left(v_{lj}(t+1)\right)$ represents the transfer function.

In order to solve the problem that the binary particle swarm optimization algorithm is easy to fall into the local optimum, the global optimization ability is strong and the local search ability is strong. Therefore, the inertia weight is improved, so that the inertia weight is nonlinearly reduced as the number of iterations t increases.

In the algorithm, the inertia weight decreases nonlinearly with the increase of the number of iterations t, which is beneficial to jump out of the local extremum point, and obtain a larger value at the initial stage of the iteration. The particles in the population are quickly scattered throughout the search area to determine the optimal value. Approximate range; as the iterative nonlinearity decreases, the search space of most particles gradually decreases and shrinks to the nearest neighbor range; at the end of the iteration, when the maximum iteration $t_{\max}$ is reached, the particles are optimal. The global optimal solution is searched in the neighborhood.

The specific steps of the multi-target binary particle swarm task allocation algorithm are:

(1) Initialization algorithm: set the number of tasks to q, and generate the initial position of each particle and the individual extreme value pb under the constraint condition;
(2) Calculate the objective function: get the fitness value of the particle as $p \cdot f_1, p \cdot f_2, p \cdot f_3$;
(3) Particle update: first update the inertia weight, then update the speed and position of the particle;
(4) Constraint test: If the particle p satisfies both the workload constraint and the space constraint, go to step (5); otherwise, go to step (3) and re-update the particle;
(5) Individual extreme value selection: Calculate the fitness value of the particle. If the current position of the particle is better than the historical best position, update the individual extreme value pb ;
(6) Elite file strategy: delete duplicate members in the archive, sort the members in the file according to the descending distance, and get a better archive. At the same time, according to the dense distance, the global optimal pg is selected for each particle by the proportional selection method;
(7) If the number of iterations $t \geq t_{\max}$, the algorithm ends and the optimal solution set S is output, otherwise it goes to step (3).

The flow of the multi-objective binary particle swarm assignment algorithm is shown in Fig. 1.

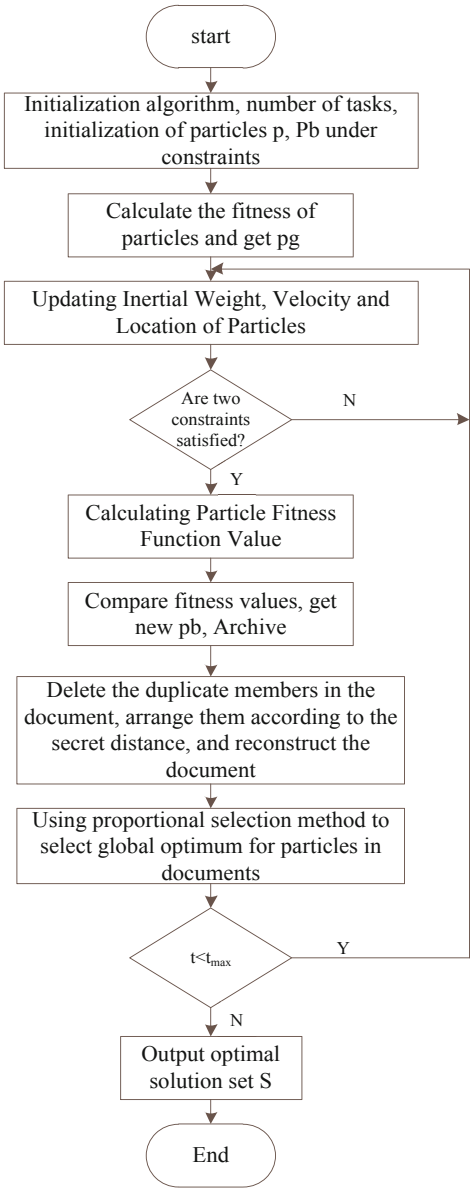

Fig. 1. Flow chart of multi-objective binary particle swarm optimization task assignment algorithm

Through the above process, the multi-target binary particle swarm task assignment algorithm is used to allocate the active attack data location task, and the optimal allocation scheme *S* is obtained, which provides support for the implementation of the following active attack data location warning [9].

2.3 Implementation of Active Attack Data Location and Early Warning

Based on the optimal allocation scheme of active attack data location tasks obtained above, the algorithm of extreme attack learning is used to locate and warn the active attack data.

The speed learning machine algorithm is proposed by Huang et al. It is a single hidden layer feedforward network, which belongs to a kind of neural network. Its advantage is that the learning of the model does not require an iterative process. Given N data $(x_i, t_i) \in R^n \times R^m, i = 1, 2, \cdots, N.x_i$ represents the $n \times 1$ input vector $x_i = [x_{i1}, x_{i2}, \cdots, x_{in}]^T$, t_i is a $m \times 1$ target vector $t_i = [t_{i1}, t_{i2}, \cdots, t_{im}]^T$. The speed learning machine has a hidden layer with L hidden nodes, as shown in Fig. 2.

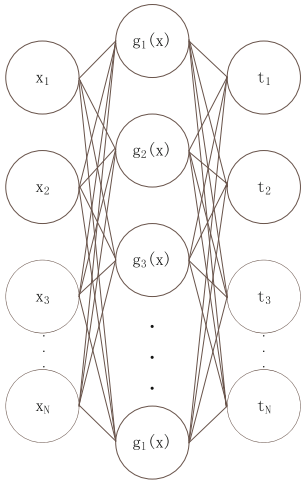

Fig. 2. Extreme learning machine model network

If the distance between the node to be located and the beacon node in the network is known, a trilateral positioning algorithm may be used to calculate the position coordinates of the node to be located [10]. The node to be located in the article is an active attack data node. Based on the data of the active attack node, a three-edge positioning algorithm can be used to locate the active attack data, and the position of the beacon node B_1, B_2, B_3 is obtained according to the algorithm of the extremely fast learning machine,$(x_1, t_1), (x_2, t_2), (x_3, t_3)$ is respectively, and the A_s coordinate of the active attack data node to be located is (x_s, t_s).

The real data value of the active attack data node A_s can be represented by a vector, The distance between the active attack data node A_s and the beacon node B_j is d_{sj}. The formula for calculating the ranging distance of the active attack data node A_s to the beacon node B_1, B_2, B_3 :

$$\begin{cases} d_{s1} = \sqrt{(x_s - x_1)^2 + (t_s - t_1)^2} \\ d_{s2} = \sqrt{(x_s - x_2)^2 + (t_s - t_2)^2} \\ d_{s3} = \sqrt{(x_s - x_3)^2 + (t_s - t_3)^2} \end{cases} \tag{9}$$

Substitute d_{sj} into the above formula, solving the equations can calculate the coordinates (x_s, t_s) of the active attack data node A_s as:

$$\begin{bmatrix} x_s \\ t_s \end{bmatrix} = \begin{bmatrix} 2(x_1 - x_3) & 2(t_1 - t_3) \\ 2(x_2 - x_3) & 2(t_2 - t_3) \end{bmatrix}^{-1} \begin{bmatrix} x_1^2 - x_3^2 + t_1^2 - t_3^2 + d_{s3}^2 - d_{s1}^2 \\ x_2^2 - x_3^2 + t_2^2 - t_3^2 + d_{s3}^2 - d_{s2}^2 \end{bmatrix} \tag{10}$$

Iteratively optimize the positioning results. After multiple iterations, the positioning result closest to the real coordinates of the active attack data node can be obtained, thereby achieving accurate positioning of the active attack data node [11–13]. The prompt sound device is used to prompt and display the above-mentioned active attack data, and the operator processes the data according to the corresponding result [14].

Through the above process, the application of automatic defense network active attack data location and early warning method is realized, which fully proves the feasibility of the method. The positioning performance of the method was analyzed by comparative experiments as described below.

3 Analysis of Location Performance of Active Attack Data Location and Warning Method

Through the above process, the application of automatic defense network active attack data location and early warning method is realized, which fully proves the feasibility of the method. The positioning performance of the method was analyzed by comparative experiments as described below.

Two evaluation indexes of convergence and positioning error are used to compare and analyze the performance of the proposed method and the traditional method. Using NS2.35 as the network simulation platform, The difference between a common node and a beacon node is that the beacon node can locate, while the ordinary node does not have the localization function, 101 sensor nodes are arranged in the network area, where the location of the aggregation node is (0, 0), and 80 common nodes and 20 beacon nodes are randomly generated uniformly using the NS2.35 scene generation tool covering the entire network. The network environment parameter values are shown in Table 1.

Table 1. Network environment parameter value

Parameter	Numerical value
Mac protocol	MAC/802_15-4
Routing protocol	AODV
Energy model	EncrgyModel
Initial energy of nodes	11520 J
Communication radius	200-250 m
Wireless propagation model	Shadowing
Path loss factor	2
Transmitting power	0.282 W
Simulation time	100 s

The multi-objective binary particle swarm task assignment algorithm has a population size of 20, a particle velocity of [−6,6], a maximum number of iterations of 200, a learning factor of 2, and an inertia weight of [0.4, 0.9], which can be set by algorithm parameters. Get a good solution in a short period of time。

3.1 Convergence Analysis

The convergence comparison is shown in Fig. 3

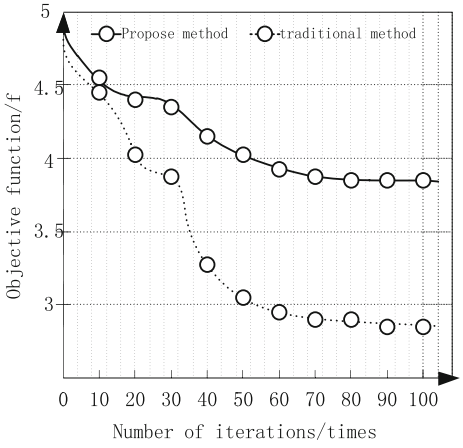

Fig. 3. Convergence contrast graph

As shown in Fig. 3, the proposed method converges to 3.78 and the traditional method converges to 2.89. The convergence value of the proposed method is 23.61% higher than that of the traditional method.

3.2 Positioning Error Analysis

The positioning error of the proposed method and the conventional method is shown in Table 2.

Table 2. Positioning error Table

Number of experiments	Proposed method error rate	Error rate of traditional methods
10	10%	23%
20	23%	30%
30	5%	25%
40	8%	28%
50	11%	21%
60	5%	25%
70	9%	29%
80	16%	26%
90	4%	24%
100	11%	21%

As shown in Table 2, the error rate of the proposed method is reduced by 15% compared with the conventional method.

Through the above two experiments, it can be seen that the proposed automatic defense network active attack data location and early warning method has better recognition performance.

4 Conclusion

The proposed automatic defense network active attack data location and early warning method improves the convergence, reduces the positioning error rate, and greatly improves the performance of the automatic defense network active attack data positioning and early warning method. However, the interference of the influencing factors is neglected in the experiment process. Therefore, further research and analysis on the automatic defense network active attack data location and early warning method are needed.

References

1. He, Y.: Research on active security defense system of campus network based on honeypot technology. Comput. Fans **12**(4), 21–22 (2016)
2. Zhu, C., Zhao, D.: A packet allocation protection method for network attack crime prevention. Sci. Technol. Bull. **32**(8), 203–206 (2016)
3. Dong, X., Lin, L., Zhang, X., et al.: Application of active defense technology in communication network security engineering. Inf. Secur. Technol. **7**(1), 80–84 (2016)

4. Pujiang, L.L.: Research on network security early warning and defense system based on three-domain model. Inf. Secur. Technol. **8**(8), 68–72 (2017)
5. Jiang, S., Luo, T.: Research on detection method of network small disturbance intrusion source location under non-uniform noise environment. Sci. Technol. Eng. **17**(5), 247–251 (2017)
6. Luo, X.W., Tao, H.: Research on Simulation of attack signal location and recognition in wireless communication networks. Comput. Simul. **33**(11), 320–323 (2016)
7. He, C.: Design of computer network security active defense model in big data era. J. Ningbo Vocat. Tech. Coll. **20**(4), 97–99 (2016)
8. Di, Z.: Research on the current situation and defense measures of network security management in Colleges and Universities. Electron. Technol. Softw. Eng. **56**(13), 221–221 (2016)
9. Liu, S., Li, Z., Zhang, Y., et al.: Introduction of key problems in long-distance learning and training. Mob. Networks Appl. **24**(1), 1–4 (2019)
10. Chaocheng, Q., Jianhong, Q.: Network security defense model of metal trading based on attack detection. World Nonferrous Metals **23**(7), 77–78 (2016)
11. Huang, R., Huang, R.: Simulation research on privacy information protection of network users. Comput. Simul. **51**(11), 319–322 + 423 (2017)
12. Liu, S., Bai, W., Srivastava, G., Machado, J.A.T.: Property of self-similarity between baseband and modulated signals. Mob. Networks Appl. **25**(4), 1537–1547 (2019). https://doi.org/10.1007/s11036-019-01358-9
13. Shuai, L., Weiling, B., Nianyin, Z., et al.: A fast fractal based compression for MRI images. IEEE Access **7**, 62412–62420 (2019)
14. Shuke, Yu.: Research on target intrusion detection based on mobile wireless sensor networks. Digital Commun. World **59**(12), 6–8 (2017)