Eng Int Syst (2022) 2: 105–114
© 2022 CRL Publishing Ltd

Engineering
Intelligent Systems

Communication Network Active Defense Method Based on Multi-Objective Evolutionary Algorithm

Yunting Tang and Xihui Lin*

Department of Electronic Information Engineering, Beihai Vocational College, Beihai 536000, China

In order to improve the security of communication networks, in view of the existing network defense methods that have low convergence, low defense success rate and so on, this paper proposes an active defense method for communication networks based on the multi-objective evolutionary algorithm. Applying the theory of pre-attribution reduction, the network scale is reduced, and the fault tolerance of error points in the subplot is determined to detect the intrusion nodes. Using the multi-target evolution algorithm based on TE decomposition, the common attack point location and attack mode of the attack side are analyzed. Based on the kernel density estimation value, the sensing position is set to obtain the optimal target, and the communication network is actively defended. Experimental tests show that under the influence of different levels of attack events, the probability of success of the proposed defense method against different types of attack events is higher than that of traditional defense methods, and is more in line with the current defense requirements.

Keywords: multi-objective evolutionary algorithm, communication network, active defense, network detection, intrusion node, network scale

1. INTRODUCTION

The openness of the network environment enables people to communicate conveniently through the network, but because most people pay insufficient attention to network security, it is very easy to be the target of attackers; breaches of network environment security are often due to the negligence of administrators or users who disregard potential problems. In recent years, the increasing number of cyber security incidents in various countries has caused great harm to the network systems of many governments and enterprises, and the network security situation has become increasingly serious (Wang et al., 2017).

The traditional communication network defense methods, such as those in Vo et al., (2019) and Ishtiaq et al., (2019), use the fuzzy clustering algorithm to select a small neighborhood with a relatively large probability to apply an reorganization and substitution strategy, and select the same neighborhood as the population size with a very small probability. At the same time, the algorithm uses one parameter to limit the number of old solutions to be updated with a new solution. Under the multiple applications of this method, due to the shortcomings in the original replacement strategy, the solution to the overall problem is mismatched with the solutions to sub-problems. This mismatch is not conducive to tackling issues of diversity and convergence. For example, with this replacement strategy, if the potential solution to the problem does not perform well on adjacent sub-problems but performs better on other sub-problems, it may be discarded, thus decreasing convergence efficiency and the capture of attack nodes. Moreover, high inappropriate solutions may cause

*Corresponding Author Email: lxh18077952341@163.com the population to lose diversity, thus causing the algorithm to fall into local optimization. The improved data-weighted fuzzy cluster intrusion defense algorithm applied by Cao et al., (2019), using the index structure of Kd-tree, uses the weighted density to select the initial cluster center of the K-means algorithm in the high-density sample area. The clustered data is divided into three class clusters, and the labeled clusters and hybrid clusters are expanded into the labeled dataset with Tri-training with the use of weighted voting rules. Using the hierarchical classification model of binary tree structure design, experimental verification was carried out on the NSL-KDD data set. This method effectively improves the detection rate of R2L and U2R attacks, which reduces the false alarm rate of the system. However, this method has fewer types of defense attacks and a lower success rate. (Chen et al., (2016) propose an intrusion detection defense algorithm based on IPMeans-KELM and that uses the improved PSO optimization K-means algorithm (IPMeans) to cluster the intrusion data and increase the aggregation of the same data type. The processed data are divided into 10-cv segments, which are trained in turn by the KELM classifier. The test data are tested through the trained KELM classifier to obtain the average detection rate of the classifier. If the test effect does not meet the desired condition, the loop treatment will be carried out until the condition is satisfied. This algorithm can improve the intrusion detection rate and reduce the false alarm rate. However, this method is less accurate in perceiving intrusion network nodes, resulting in a lower defense rate.

To address the shortcoming of the existing methods, this paper proposes an active defense method for communication networks based on a multi-objective evolutionary algorithm in order to establish a detection strategy for these networks. By applying the prereduction theory, the network scale is reduced and intrusion nodes are detected. A multi-objective evolutionary algorithm based on TE decomposition is used to analyze the location and attack mode of attack points. The sensing position is set according to the kernel density estimation value to realize the active defense of the communication network. The proposed method resolves the problems inherent in traditional methods and provides strong technical support for communication network security.

2. COMMUNICATION NETWORK ACTIVE DEFENSE METHOD BASED ON MULTI-OBJECTIVE EVOLUTIONARY ALGORITHM

2.1 Setting up Communication Network Detection Program Based on Multi-Objective Evolutionary Algorithm

The first step of communication network active defense method based on multi-objective evolutionary algorithm is to set up a communication network detection strategy. This strategy can reduce the evolutionary search space, allowing dynamic attack structures to be found in large-scale communication networks. Suppose H is a network comprising 12 nodes, H_0 is a network composed of 4 subgraphs, and $H_1, H_2, \ldots, H_n$ are networks comprising three subgraphs. Using the characteristics of cluster nodes present in complex networks, using the community detection in the process of the evolution and multi-objective evolutionary algorithms, in the course of evolution between individual species in the same local features, for complex communication network to H subtract, step-by-step to obtain the new networks $H_0, H_1, \ldots, H_m$; H_1 is the network obtained by the first reduction in the evolution process; H_m is the network obtained by the m-th reduction; After shrinking, a new network is obtained. At this time, the size of network is much smaller than, and the response time is also small (Mehmood et al., 2017).

According to the theory of prereduction, the scale of the network is reduced in the pre-evolution stage of the detected multi-objective evolutionary algorithm. Because of the clustering characteristics of the complex network, it is highly likely that the closely connected points in the network will all be within a certain region. The pre-reduction method is described below.

Firstly, a point in the complex network p is randomly selected, and the point with the highest density in the neighbor node is selected as the core point c_p of p. Then, n_p, the node with the most common neighbor nodes of c_p, was found from the neighbor nodes of c_p. Taking H_m as the core subgraph of c_p, H_m satisfies Equation (1):

$$H_m = c_p \cup n_p \cup common\_connect(c_p, n_p) \qquad (1)$$

In Equation (1): $common\_connect(c_p, n_p)$ is the set of all common nodes of c_p and n_p. Finally, if the neighbor node of the core subgraph H_m is closely connected with H_m, it will be extended to H_m until the neighbor node cannot be added. After that, we follow the above steps for the remaining points in the network and finally obtain several subgraphs: $H_0, H_1, \ldots, H_{m+1}, \ldots, H_n$. When using the prereduction method to reduce the size of the network, it is possible to merge points that are not closely connected into a subgraph; these are known as error points. The error points in these subgraphs have a very negative impact on evolution, so the following fault-tolerant processing methods are proposed:

For the selected individual $p'(i = 1, 2, \ldots, a)$ of a, if in individual p', the point inside region j exists in the neighbor node in other Spaces, then the point is put into other Spaces; If the individual p' increases, the point is added to the error point set $f(p')$, and then all regions of p'_i are processed as above. Loop a times to put all the error points into $f(p')$, and finally remove each point in $f(p')$ from the subgraph of the current network H_n as a separate subgraph, while updating the H_n. The advantages of fault-tolerant processing are obvious: the internal points of subgraphs do not have to be necessarily together, absoluteness is eliminated, and the population evolution achieves better community division (Wang et al., 2018; Anugrah et al., 2019).

The subgraph network H_n is obtained after the complex network has been reduced. Therefore, the coding mode of the neighbor subgraph is used to set up the detection strategy for the communication network. In this coding mode, each individual in the multi-objective evolutionary algorithm population is represented as

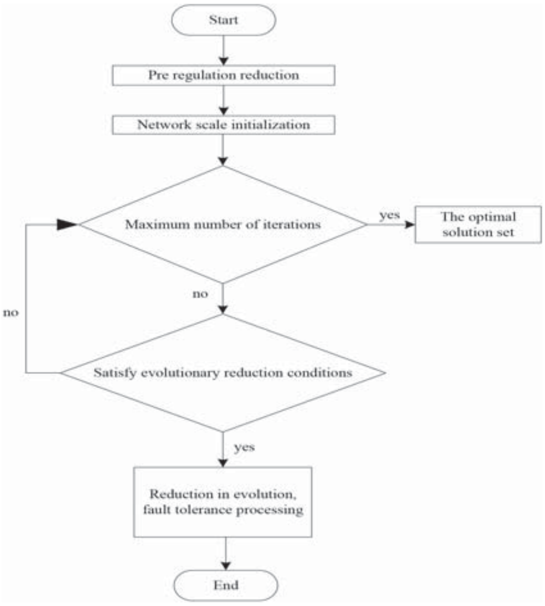

Start
Pre regulation reduction
Network scale initialization
Maximum number of iterations
yes
The optimal solution set
no
no
Satisfy evolutionary reduction conditions
yes
Reduction in evolution, fault tolerance processing
End

Figure 1 Communication network detection process.

$$\begin{cases} K\ H\cdots W\cdots \\ f(K)\ f_H\cdots f_w\cdots \end{cases} \tag{2}$$

In Equation (2), $W \in \{K, H\cdots\}$, W is the subgraph of network H_n; f_w is the corresponding gene of subgraph w; the value of f_w can be the neighbor subgraph of the subgraph w or the subgraph W itself. The detection process is shown in Figure 1.

The detection process described above establishes a detection strategy to ensure real-time monitoring of the communication network and takes active defensive measures against sudden offensive network behaviors.

2.2 Perception of Attack Location Based on Multi-Objective Evolutionary Algorithm

Following the establishment of the detection strategy, the next step is to analyze the preference of the attacking user. Ten, two objective functions are designed to determine the intentions of the attackers.

The multi-objective evolutionary algorithm first decomposes the original problem into multiple sub-problems, then searches for the optimal solution in the decision space by applying the evolutionary algorithm, and finally combines the solutions of sub-problems to form a Pareto frontier for the multi-objective problem. In addition, the algorithm adopts a diversity-preserving strategy in the process of evolutionary search; that is, the evolutionary operation is applied only to adjacent sub-problems. There are three methods for decomposing a multi-object problem into several single objects: weighted sum method, Tchebycheff (TE) method and Boundary Intersection (BI) method. Of these, the TE method is the most commonly used strategy as it produces good results. Hence, this study adopts a multi-objective evolutionary algorithm based on TE decomposition (Tang et al., 2018). A multi-objective problem can be decomposed into the following single-objective sub-problems with this equation:

$$f^{te}(x|\beta^j, z^*) = \max\left[\beta_i^j|h_i(x) - z_i^*\right] \tag{3}$$

In Equation (3), $\beta^j = (\beta_1^j, \ldots, \beta_m^j)$ represents a weight vector corresponding to m objective functions. The multi-objective evolutionary algorithm based on TE decomposition can optimize m objective functions simultaneously. A weight vector represents a direction in the value space of the objective function. The multi-objective evolutionary algorithm based on TE decomposition will carry out search optimization along this direction, as shown in Figure 2.

According to Figure 2, q represents a point in the direction corresponding to a weight vector, and z^* represents a target point in this direction. The two perpendicular lines passing through point q indicate the distance of point z^* from the target point on the two objective functions. Applying Equation (3), the result $f^{te}(x|\beta^j, z^*)$ represents the longest of the two perpendicular lines. In the continuous optimization process, point q will approach the target point z^* continuously in this weight direction, and the optimization process in other weight directions is also the same, and the solution set finally obtained will approach the theoretical Pareto frontier. The positions and attack modes of common attack points at the attack end were analyzed, and the perceived positions were set according to the estimated kernel density (Yuan et al., 2017; Biswas et al., 2019).

Kernel density estimation is a non-parametric density estimation technique. Unlike the parametric estimation method, the non-parametric estimation technique does not need to assume a certain distribution form, but learns to approximate the real distribution through data. Therefore, kernel density estimation can be based on arbitrary distribution. Equation (4) is:

$$f(x) = \frac{1}{n\varepsilon^2}\sum_{i=1}^{n} f^{te}(x|\beta^j, z^*)\cdot\gamma\cdot\left(\frac{x - B_i}{\varepsilon}\right) \tag{4}$$

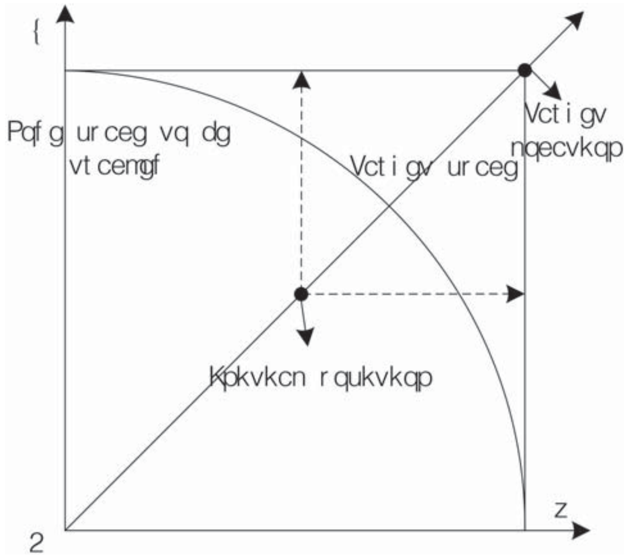


Figure 2 Schematic diagram of multi-objective evolutionary algorithm searching.

In Equation (4): $B_i = (b_1, b_2, \ldots, b_n)$, represents the common attack position of the attack end; $b_i = (lat_i, lon_i)^T$ is a two-dimensional vector made up of latitude and longitude; γ stands for kernel; ε represents a smoothing parameter. The kernel function adopts the two-dimensional gaussian function, and the equation is:

$$\gamma(x) = \frac{1}{2\pi}\exp\left(-\frac{1}{2}x^T x\right) \tag{5}$$

In a new network structure, the calculation of the probability of attack on a node is obtained with Equation (6) below:

$$p(A|f(x)) = \frac{1}{2\pi n\varepsilon^2}\sum_{i=1}^{n}\exp\left(-\frac{1}{2\varepsilon^2}(1-B_i)^T(1-B_i)\right) \tag{6}$$

In Equation (6), represents the predicted position node of the attack end; through the above process, the target evolutionary algorithm of TE is used to make multi-target perception of the attack position of the attack ends, so as to ensure that the communication network will not ignore any attack point when conducting active defense (Benmessahel et al., 2018).

2.3 Selecting and Developing the Reorganization Strategy of Communication Network Active Defense Based on Multi-Objective Evolutionary Algorithm

Diversity and convergence are generally considered to be two aspects of multi-objective evolutionary algorithms. Ideally, the population maintains good diversity during the search and approaches PF as quickly as possible. It is often impossible to have both. For example, if an algorithm pays too much attention to convergence in the early stages of evolution, the algorithm tends to fall into local optimization and thus cannot approach PF well. Conversely, if the algorithm focuses too much on diversity, the search efficiency of the algorithm can decrease. Ideally, an algorithm should conduct more exploration in the early stages of a search because the potential areas currently explored by the population tend to be less trustworthy. In the later stages of the search, the algorithm hopes to speed up development so that it can make better use of computing resources.

In the proposed active defense method based on the multi-objective evolutionary algorithm, the substitution strategy is used to constantly update the current solution for sub-problems, which can play a role in balancing the diversity and convergence. At the same time, the convergence is improved by improving the algorithm. When the algorithm adopts a small Tr, the number of repeated solutions in the next generation population will be less, enabling the population to maintain better diversity and be more conducive to development. When the algorithm adopts a large Tr, the differential solution in the population is much less than that of the good solution, which means the algorithm will do more development and less exploration. In addition, we have to weigh diversity against convergence. If the algorithm uses a fixed Tr throughout the search, the bounds often need to be set very carefully. Based on the multi-objective evolutionary algorithm, an adaptive substitution strategy is proposed which, by adaptively controlling the size of Tr, enables the algorithm to emphasize diversity and convergence differently at different stages of search (Li et al., 2018).

In this section, we apply the Chebyshev method to improve multi-objective evolutionary algorithm, and use this method as a new decomposition method for multi-objective problems. The formula is:

$$\begin{cases} \min imize\ k^{tch}(x|p, z_i^*) = \max\limits_{1\le i\le m} \\ \left(\dfrac{\frac{1}{p_i}}{\sum_{j=1}^{m}\frac{1}{p_j}} f(p(A|f(x))) - z_t^*\right) \\ subject\ to\ x \in \Omega \end{cases} \tag{7}$$

In Equation (7): $p = (p_1, p_2, \ldots, p_m)^T$ is a direction vector satisfying $p_i \geq 0$ and $i = 1, 2, \ldots, m$. $z^* =$

$\{z_1^*, z_2^*, \ldots, z_m^*\}^T$ is a reference point. In the improved Chebyshev method, each subproblem requires a direction vector and a reference point. In this section, we still use ideal points as reference points. Assume that $U = \{u^1, u^2, \ldots u^N\}$ is the N subproblems, and $P = \{p^1, p^2, \ldots, p^N\}$ is the direction vector to which they correspond. The N direction vectors are still obtained by the method of Das and Dennis. By calculating the Euclidean distance between any two direction vectors, the neighborhood relationship between subproblems is obtained. $\sigma(i)$ represents the index number of subproblems in the p^i neighborhood. Through the uniform sampling of the whole search space, the initial population $\{x^1, x^2, \ldots, x^N\}$ is obtained, where each x^i is regarded as the current solution of p^i (Wei et al., 2018).

The algorithm adopts a reorganization strategy. For a subproblem p^i, randomly select the current solution of the subproblem in its neighborhood with probability ξ, or randomly select three samples from the whole population with probability $1 - \xi$. Then the difference and polynomial variation operations are performed on these samples to obtain a new solution, $\hat{x}^i$. In a global substitution strategy, $\hat{x}^i$ is used to update the current solution for a suitable subproblem. The appropriate subproblem here is the subproblem where the optimal solution is closer to $\hat{x}^i$. After the above analysis and setting, an adaptive replacement strategy is proposed to change the size of the replacement neighborhood adaptively according to the search process. Then we set the adapted steady-state for the adaptive substitution strategy.

It is known that a multi-objective evolutionary algorithm tends to expect more exploration of the whole space in the initial stage of the search and more exploitation of potential areas in the later stage. In the early stage of the search, if we focus on developing some potential solutions in the vicinity of the region, it is easy to miss other potential areas. Moreover, the potential solutions found at this stage are often unreliable, and excessive exploitation may easily lead to the loss of diversity and local optimization. In the later stage of the search, the reliability of the potential solution is higher, and the computational resources can be saved by improving the convergence speed. Therefore, in the early stage of search, this algorithm adopts a small boundary to maintain a good diversity of the population so that it can explore more search space and avoid falling into local optimization. A large Tr is used in the late stage of the search to improve the convergence rate. In the early stages of evolution, much of the breakdown in a population tends to be far from PF. At this point, if a new solution has a high quality, and the algorithm adopts a relatively large Tr, then the high-quality solution can almost replace the entire population, so that most of the sub-problems fall into the local optimum, thus leading to the prematurity of the algorithm. In the later stages of evolution, the population tends to be closer to PF, where even if the algorithm adopts a large Tr, a new solution will not replace most of the old ones. On the contrary, a larger Tr can make a high-quality solution replace relatively more differential solutions, thus improving the convergence speed (Wang et al., 2018). Based on the above analysis, we propose to use an offline adaptive mode to control the size of Tr. Here we consider the following three ways:

$$\begin{cases} Tr_1 = \frac{sT_{\max}}{S} \\ Tr_2 = \frac{\left[\exp(\frac{es}{S})-1\right]T_{\max}}{\exp(e)-1} \\ Tr_3 = \frac{T_{\max}}{1+\exp\left[-e(\frac{s}{S}-\phi)\right]} \end{cases} \tag{8}$$

In the above formula: $T_{\max}$ is the maximum value of Tr; s is the current number of iterations; S represents the maximum number of iterations; $\phi \in 0, 1)$ is a control variable that determines how Tr increases with the number of iterations; Tr_1 represents the linear result; Tr_2 represents the exponential result; Tr_3 represents an s-shaped result. By using the above formula, the selection and reorganization strategy is set up to ensure the convergence speed of the communication network's active defense.

2.4 Select the Optimal Target to Achieve The Active Defense of The Communication Network

Constrained by resources, budget, and effort, communication network administrators might not be able to execute all possible defense countermeasures. Hence, in these cases, security personnel can only select a subset of the countermeasure spool, set the optimization target according to the network's information security needs, and achieve the active defense of the communication network by selecting the optimal target.Current network attacks are covered by attack events.

The premise underlying the full coverage of attack events is that there is at least one set of countermeasures that can cover all attack events. That is to say, for such problems, the optimal set of required countermeasures can cover all attack events at least, and full coverage is the basic requirement. According to the basic definition of qualitative and quantitative analysis methods, there are many optimization objectives to choose from. Here, the optimization objective is to minimize the number of countermeasures implemented. "Minimize the number of countermeasures" is the optimization target, the minimum number of defense mechanisms must be selected under the premise that all attack events in the tree are covered (Elhag et al., 2019). This optimization problem becomes a special case of set coverage and is organized into a binary integer programming problem. If the countermeasure in the optimal countermeasure set OPT covers the attack events of all leaf nodes in the attack game tree to achieve complete coverage, the objective function can be written as:

$$F_1 = Tr \times \min_{D} \sum_{i}^{n} \prod_{OPT} (Q_i)\text{: coverd, set} = M \tag{9}$$

In Equation (9), $M = \{M_1, M_2, M_3, \ldots, M_n\}$ represents the set of attack events; $Q = \{Q_1, Q_2, Q_3, \ldots, Q_n\}$ represents the set of all countermeasures; in the attack game tree, $n = |Q|$, there are n countermeasures; D stands for all possible combinations of games, so $|D| = 2^n$, each combination is a strategy. $\prod_{OPT}(Q_i)$ in the above formula is the indicative function of Q_i, as shown in Equation (10):

Table 1 Active defense level value table.

Operational difficulty	Easily	Ordinary	More difficult	Extremely difficult
E$_1$	I	II	III	IV
E$_0$	1	4	9	16

$$\prod_{OPT}(Q_i) = \begin{cases} 1, Q_i \in OPT \\ 0, Q_i \notin OPT \end{cases} \tag{10}$$

This optimization problem is a function coverage problem. Partial coverage of an attack event refers to the proposed security model for the communication network such as an attack countermeasure tree. These models are then searched for attack paths to identify attack scenarios that will result in losses, which may provide some defense against some of the most threatening or interesting attacks. The notion of "partial coverage" can be divided into two categories: intentional partial coverage and unintentional partial coverage. The following formula is the target function of partial coverage of attack events:

$$F_2 = \min Tr \times \sum_{i}^{n} \prod_{OPT} (Q_i)\text{: coverd,set} = N \tag{11}$$

In Equation (11): N represents the attack event of partial coverage, and other variable values are explained by reference to Equation (9). Based on the above strategy selection and classification introduction, and combined with the above defense preparations based on multi-objective evolutionary algorithm, the active defense strategy for the communication network is obtained after selecting the optimal target. The operation level of this program is presented in Table 1 (Zhu et al., 2018).

In Table 1, E_1 and E_2 represent initial operation difficulty and process operation difficulty. Suppose the defense target is I_i, where i represents the number of defense targets, and the constraint matrix T is generated from the minimum cut set of the attack game tree, where the column represents the countermeasure Q_i. The row represents the attack event M_i or N_i. If Q_i overwrites M_i, it corresponds to $t_{ij}((i, j)^{th}) = 1$ in the constraint matrix T, where t_{ij} represents the overwrite result on row i and column j, otherwise $t_{ij} = 0$. In order to ensure the accuracy of coverage, the constraint of attack event on coverage should also be considered in the active defense of a communication network. Formula (12) is the constraint condition of an attack event on defense coverage:

$$\forall M_{ij} \in M, \sum_{i=1}^{n} t_{ij} F_1 \geq 1 \tag{12}$$

According to the above constraints, the constraint matrix of attack events is obtained to determine the extremum of active defense feedback:

$$\mu = \sum_{i=1}^{n} t_{ij} F_1 - \frac{ROI_{OPT} \times F_1 + \Delta F}{\sigma} \tag{13}$$

In Equation (13), ROI_{OPT} represents the optimal countermeasure set; ΔF represents other secondary attack events caused by an attack event. With the above formula, the feedback extremum μ is obtained. When $\mu > 0.4$, the communication network can quickly defend itself and realize fast defense against network attacks (Mousa et al., 2018); when $\mu \leq 0.4$, the communication system locks only the attack event and does not launch a counterattack. At this point, the communication network's active defense method based on multi-objective evolutionary algorithm is realized.

3. EXPERIMENTS AND ANALYSIS

At present, the increasingly mature virtual machine technology for saving hardware resources makes it convenient and quick to build a computer network experimental environment that is ideal. The virtual machine system generates a new virtual image of the existing operating system, giving it the same function as the real system, and after entering the virtual machine system, all the operating systems are run in this new independent virtual system, which can install and run the software independently. Virtual machines can also simulate the underlying hardware instructions. Hence, to a large extent, the virtual machine system and the real operating system are not very different, and can fully meet the experimental needs of the general computer network system. The experimental design platform, by means of virtual machine technology, installed and ran a number of different operating systems of virtual machines on a physical machine. The physical machine is connected to the wireless network by bridge mode, and the virtual machine installed on it is connected to the local area network by custom mode. One of the virtual machines is the Ubuntu operating system, which is the hardware carrier of the active defense system, and the other is the customer host, which is protected by the active defense system required for the experimental environment. The experimental test environment is shown in Figure 3.

As shown in Figure 3, the service host is the hardware carrier of active defense system, clients 1–5 are the virtual machines used to build a local area network (Cao et al., 2019) (LAN) environment, and the gateway is set to service host. The data conveyed between each client and the Internet all go through the service host. The IP addresses of the Intranet are controlled by the service host, and are generated and transformed dynamically. The experimental environment configuration is shown in Table 2.

Next, the experimental environment is tested. The normal communication performance test of the system access host is divided into four steps: enable routing and forwarding, run system files, test the network access from each host to the Internet, and the communication among the hosts. During the test, the routing and forwarding function of the system service host needs to be enabled so that the packets after the replacement of the IP address can be forwarded, and transparent and sensitive communication can be realized. Test

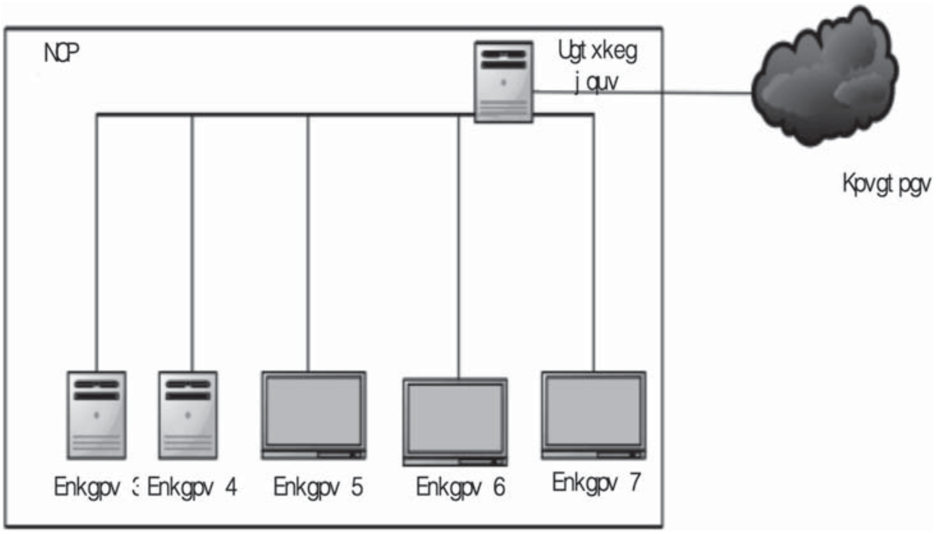
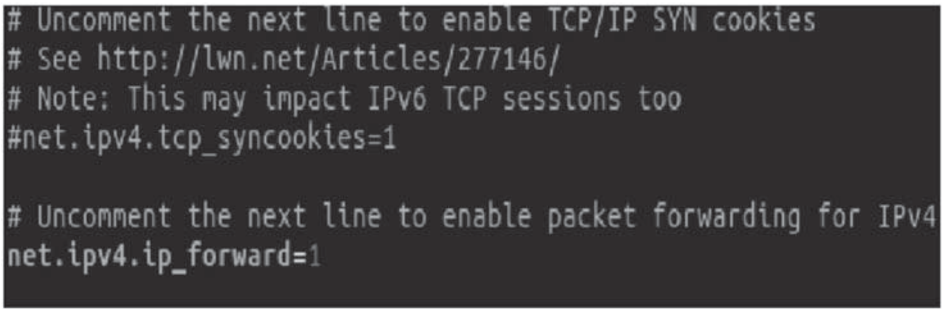


Figure 3 Experimental test environment.

Table 2 Experimental environment configuration table.

Machine type	Hostname	OS	Memory	Hard disk	IP address
Physical machine	Lab Server	Windows Server 2016	64G	16T	
Virtual machines	Service host	Ubuntu 14.4	4G	100G	172.16.100.254
	Client1	Windows Server 2013	2G	50G	172.16.100.1
	Client2	Ubuntu 14.4	2G	50G	172.16.100.2
	Client3	Windows 10 Pro	2G	50G	172.16.100.3
	Client4	Windows 10 Pro	2G	50G	172.16.100.4
	Client5	Windows 7 Pro	2G	50G	172.16.100.5



```
# Uncomment the next line to enable TCP/IP SYN cookies
# See http://lwn.net/Articles/277146/
# Note: This may impact IPv6 TCP sessions too
#net.ipv4.tcp_syncookies=1

# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1
```

Figure 4 The profile for enabling routing and forwarding in the experimental environment.

instructions are run on the system service host to turn on routing and forwarding, which is still valid when the system service host restarts. The profile is shown in Figure 4:

The .py and rip vip.py interfaces.py are the python script files for the network module, and rip vip.py is the python script file for the dynamic transformation module. After successful operation, the host in the local area network connected to by the system service host will be protected by the active defense system, each host in the local area network is connected to the Internet through the system service host, the traffic of each host is through the system service host, and the dynamic transformation function of the active defense system will play a role in detecting whether the access host can communicate normally and set up the attack node after completion. The specific information is shown in Table 3 and Table 4.

In Table 3 and Table 4, the attacks on nodes 01–010 are general attacks, and attacks at 001–0010 nodes are sudden attacks that can be detected.

Three kinds of active defense methods are used to defend against the simulated attack events shown in the table. Experiment group A is the proposed defense method based on the multi-objective evolutionary algorithm. Experiment group B is the traditional defense method based on fuzzy clustering (FCM). Experiment group C is the improved defense method based on data-weighted fuzzy clustering (DWFCM). The defense success rates of these three methods against general attack events in the experimental environment are shown in Figure 5.

Table 3 Simulation parameters of general attack events.

Attack node	Attack probability/p	Attack level	Attack cost	Attack impact value
01	0.15	I	1.3	12
02	0.08	I	1.3	12
03	0.08	II	2.2	12.5
04	0.1	II	2.2	30
05	0.03	III	3.7	12
06	0.04	III	3.7	12
07	0.15	I	1.3	12
08	0.08	I	1.3	12
09	0.08	II	2.2	12.5
010	0.1	II	2.2	30

Table 4 Simulation parameters of sudden attack events.

Attack node	Attack probability/p	Attack level	Attack cost	Attack impact value
001	0.03	III	3.7	12
002	0.04	III	3.7	12
003	0.001	III	3.7	12
004	0.005	IV	5.8	12
005	0.005	IV	5.8	12
006	0.03	IV	5.8	8
007	0.06	IV	5.8	8
008	0.06	IV	5.8	8
009	0.05	III	3.7	1
0010	0.08	III	3.7	12

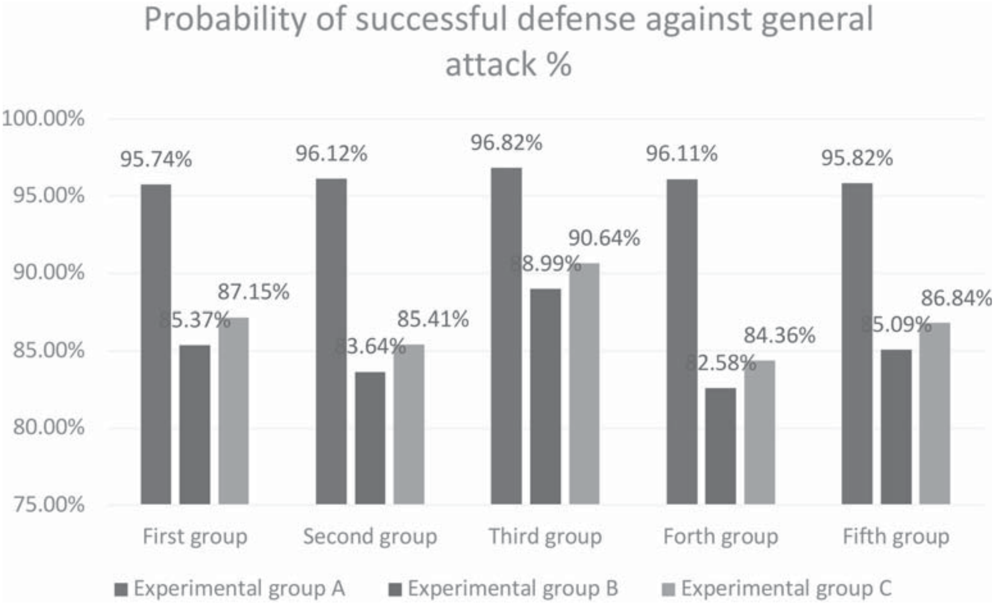


Figure 5 Probability of successful defense against general attack.

According to Figure 5, the active defense method based on the multi-objective evolutionary algorithm has an average probability of successful defense of 96.12% against a general attack. For the defense method based on fuzzy clustering, the average probability of successful defense against general attack is 85.13%, and the average probability of the defense method based on data-weighted fuzzy clustering is 86.88%. The comparison shows that the successful defense rate of the defense method based on the multi-objective evolutionary algorithm is 10.99% higher than that of fuzzy clustering and 9.24% higher than that of the defense method of data-weighted fuzzy clustering. The successful defense rate of the three defense methods against sudden attacks with strong impact and strong attack performance, are shown in Figure 6.

As indicated in Figure 6, under a high-intensity attack, the active defense method based on multi-objective evolutionary algorithm proposed in this paper has decreased the probability of successful defense the same as the traditional defense methods, but the average probability of successful defense based on the multi-objective evolutionary algorithm is 93.39%

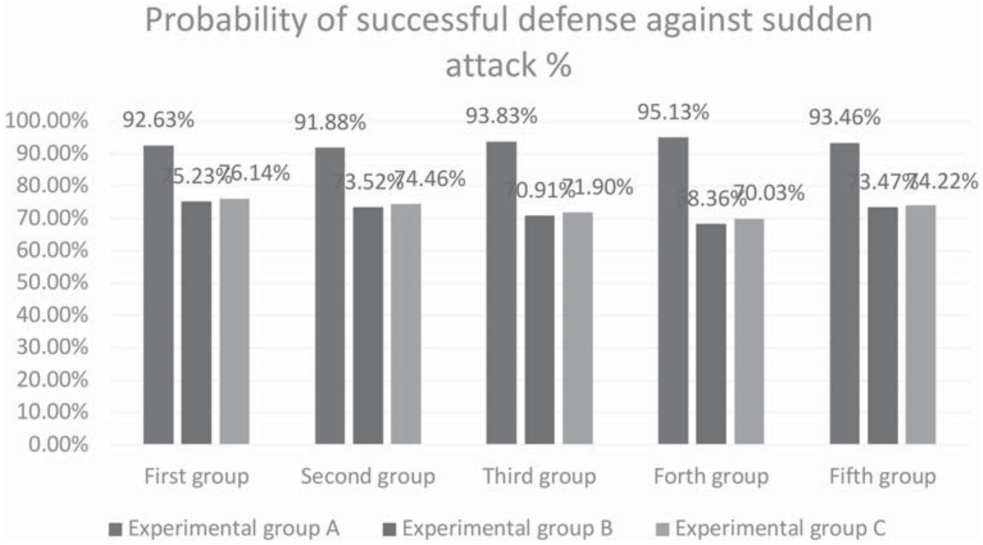


Figure 6 Probability of successful defense against sudden attack.

after statistical knowledge. The average probability of successful defense in fuzzy clustering decreased to 72.30%, which was 21.09% lower than that of the multi-objective evolutionary algorithm, while the average successful defense probability of the defense method based on data-weighted fuzzy clustering decreased to 73.35%, which was 20.04% lower than that of the multi-objective evolutionary algorithm. Taken together, these two sets of test results show that the active defense method based on multi-objective evolutionary algorithms is more capable of defending against cyberattacks.

4. CONCLUSIONS

The defense vulnerabilities and general vulnerabilities of communication networks are unavoidable, as absolutely secure network systems do not exist. Mobile target defense does not guarantee absolute security; rather, it deploys continuous security defenses in an imperfect communications system, assuming that all systems are defective. The network topology presented to the attacker changes in random dynamics, making the attack surface unpredictable, keeping the system under the protection of dynamic defense technology, and achieving the goal of providing advance and active defense.

To address the shortcomings of existing network defense methods, such as low convergence and low defense success rate, the active defense method proposed in this paper is based on the idea of mobile target defense, combined with the actual security requirements within the LAN, designed and implemented by means of a multi-objective evolutionary algorithm, and was tested to determine the effectiveness and reliability of communication systems. The specific work carried out is explained below.

Given the increasingly serious network security problems, this paper analyzes the research background and significance, and compares the current situation of research in dynamic network active defense in China and abroad. This paper analyzes and studies the traditional network defense technology, points out the shortcomings of the traditional defense methods, and compares the advantages of active defense technology in dynamic network environments. To address the security protection needs of LAN environment, the active defense system architecture is constructed, the active defense system scheme is designed, and the active defense system based on the dynamic change of network topology is realized. In order to verify the effectiveness and stability of the proposed active defense system, the experimental platform is built, the testing process is designed, and the proposed defense strategy is tested. The test results show that the average probability of active successful defense against general attack is 96.12%, and the probability of successful defense against sudden attack is 93.39%, which is higher than the success rate of two comparative methods, and is therefore more practical.

The active defense method proposed in this paper challenges the concept of traditional static defense, constructs a randomized and dynamic network environment, uses multi-objective evolutionary algorithm, strengthens the dynamic defense mechanism, and ensures that active defense has the characteristics of initiative and anticipation. Compared with traditional defense methods, the method studied in this paper has superior defense performance. In future research, we intend to adopt the dynamic defense mechanism of a network, in the scanning and detection stage of the network attack, give the attacker false dynamic change of node and network attribute information, confuse and mislead the attacker's judgment, so that the attacker "can't find the target, can't determine the location, can't keep up with the state, can't figure out the situation." It is difficult to rely on this information to launch subsequent attacks, thus exposing the identity of the attacker, increasing the attacker's attack cost, and improving network security.

REFERENCES

1. Anugrah G., Hermawan P. 2019. Pre-trip Decision on Value Co-Creation of Peer-to-Peer Accommodation Services. *Acta Informatica Malaysia, 3*(2), 19–21.

2. Benmessahel, I., Xie, K., Chellal, M. 2018. A new evolutionary neural networks based on intrusion detection systems using multiverse optimization. *Applied Intelligence, 48(*8), 2315–2327.
3. Biswas S., Biswas N., Mondal K.C. 2019. Parallel and Distributed Association Rule Mining Algorithms: A Recent Survey. *Information Management and Computer Science, 2*(1), 15–24.
4. Cao, W.D., Xu, Z.X. 2019. Efficient semi-supervised multi-level intrusion detection algorithm. Journal of Computer Applications, *39*(7), 1979–1984.
5. Chen, X.L., Li, Y.Z., Yu, Y.Z. 2016. Intrusion detection algorithm based on IPMeans-KELM. *Computer Engineering and Applications, 52*(22), 118–122.
6. Elhag, S., Fernández, A., Altalhi, A., et al., 2019. A multi-objective evolutionary fuzzy system to obtain a broad and accurate set of solutions in intrusion detection systems. *Soft Computing, 23*(4), 1321–1336.
7. Ishtiaq S., Sajid A., Wagan R.A. 2019. Review Paper on Wearable Computing: Its Applications and Research Challenges. *Acta Electronica Malaysia, 3*(2), 37–40.
8. Li, W., Hu, L., Xie, Z., et al., 2018. Cyclic di-GMP integrates functionally divergent transcription factors into a regulation pathway for antioxidant defense. *Nucleic Acids Rsearch, 46*(14), 7270–7283.
9. Mehmood, A., Khanan, A., Umar, M.M., et al., 2017. Secure knowledge and cluster-based intrusion detection mechanism for smart wireless sensor networks. *IEEE Access, 22*(6), 5688–5694.
10. Mousa, F., Almaadeed, N., Busawon, K., et al., 2018. Indoor visible light communication localization system utilizing received signal strength indication technique and trilateration method. *Optical Engineering, 57*(1), 11–17.
11. Tang, Y., Zhang, D., Ho, D.W.C., et al., 2018. Tracking control of a class of cyber-physical systems via a flexray communication network. *IEEE Transactions on Cybernetics, 49*(4), 1186–1199.
12. Vo, T.T., Luong, N.T., Hoang, D. 2019. MLAMAN: A novel multi-level authentication model and protocol for preventing wormhole attack in mobile ad hoc network. *Wireless Networks, 25*(7), 4115–4132.
13. Wang, G.C., Gong, C., Xu, Z.Y. 2018. Signal characterization for multiple access non-line of sight scattering communication. *IEEE Transactions on Communications, 66*(9), 4138–4154.
14. Wang, W., Sheng, Y., Wang, J., et al., 2017. HAST-IDS: Learning hierarchical spatial-temporal features using deep neural networks to improve intrusion detection. *IEEE Access, 19*(6), 1792–1806.
15. Wang, Y.L., Wang, J.S. 2018. Simulation of worm optimization detection in network security defense. Computer Simulation, *35*(7), 249–252.
16. Wei, Z.K., Hu, W.X., Han, D.H., et al., 2018. Simultaneous channel estimation and signal detection in wireless ultraviolet communications combating inter-symbol-interference. *Optics Express, 26*(3), 3260–3267.
17. Yuan, Y., Ong, Y.S., Gupta, A., et al., 2017. Objective reduction in many-objective optimization: Evolutionary multiobjective approaches and comprehensive analysis. *IEEE Transactions on Evolutionary Computation, 22*(2), 189–210.
18. Zhu, L.H., Li, M., Zhang, Z.J., et al., 2018. Big data mining of users' energy consumption patterns in the wireless smart grid. *IEEE Wireless Communications, 25*(1), 84–89.