Mathematical Biosciences and Engineering

http://www.aimspress.com/journal/mbe

MBE, 20(6): 11176–11195.
DOI: 10.3934/mbe.2023495
Received: 24 October 2022
Revised: 24 March 2023
Accepted: 02 April 2023
Published: 25 April 2023

Research article

An approach to generate damage strategies for inter-domain routing systems based on multi-objective optimization

Wendian Zhao, Yu Wang*, Liang Liang, Daowei Liu and Xinyang Ji

Chinese People's Liberation Army 63893 Troops, Luoyang 471000, China

* **Correspondence:** Email: zwd19@nudt.edu.cn.

Abstract: Inter-domain routing systems are important complex networks on the Internet. It has been paralyzed several times in recent years. The researchers pay close attention to the damage strategy of inter-domain routing systems and think it is related to the attacker's behavior. The key to the damage strategy is knowing how to select the optimal attack node group. In the process of selecting nodes, the existing research seldom considers the attack cost, and there are some problems, such as an unreasonable definition of attack cost and an unclear optimization effect. To solve the above problems, we designed an algorithm to generate damage strategies for inter-domain routing systems based on multi-objective optimization (PMT). We transformed the damage strategy problem into a double-objective optimization problem and defined the attack cost related to the degree of nonlinearity. In PMT, we proposed an initialization strategy based on a network partition and a node replacement strategy based on partition search. Compared with the existing five algorithms, the experimental results proved the effectiveness and accuracy of PMT.

Keywords: inter-domain routing systems; complex networks; damage strategy; optimal attack node group; multi-objective optimization

1. Introduction

The Internet of Things is an extended network based on the Internet. As an important infrastructure of the Internet, the inter-domain routing system is closely related to the security and stability of the Internet of Things. The inter-domain routing system is a dynamic system composed of multiple autonomous systems. Its main function is to exchange routing information between autonomous systems and ensure that the data requested by users can be transmitted stably between autonomous systems. The border gateway protocol (BGP) is a routing protocol for inter-domain routing systems to exchange routing information. When users accessing the Internet send data requests, the BGP can realize the optimal routing path selection of data transmission so that data can be transmitted between routers quickly and effectively. Ideally, the inter-domain routing system will not be affected, so everything can run smoothly and all data requests of users can be easily met.

However, the reality always backfires. Based on the security defects of BGP, a failure or malicious attack on the BGP router can affect the whole inter-domain routing system. The spread of Code Red II and Nimda worms led to the continuous shock of the routing system of the global Internet in 2001 [1]. Due to a BGP routing error of CenturyLink, the Internet had a cascade reaction in 2020 [2]. As a result, many services connected to the Internet were paralyzed, such as Steam, AWS, Discord and other services. In 2021, BGP route leakage occurred in India's autonomous network (AS55410), resulting in a 13-fold surge in traffic on the wrong path. More than 20,000 autonomous networks around the world were affected by the event because of cascading. As shown in the above security events, cascading failures occur frequently in the inter-domain routing system. If maliciously exploited by attackers, cascading failures will have wider impacts on the inter-domain routing system. Therefore, studying the possible damage strategies of attackers against inter-domain routing systems is crucial for defending against threats.

Think of a BGP router as a node; the damage strategy refers to a group of attack node sequences. At present, damage strategies for complex networks are mainly based on the assumption of no cost. No cost means that all nodes are considered to be the same without considering the attack cost. The damage strategy without considering the cost only considers the damage to the network, which belongs to a single objective optimization problem. The common method to solve the single objective optimization problem is to evaluate the important nodes in the network and give the importance value of each node. The sequence obtained by sorting nodes according to their importance is the group of attack node sequences. In the past, the identification methods of important nodes in the network mostly depended on a single indicator [3,4]. Recent studies have assessed the importance of nodes using indicators that are closely related to the node, including the weak connection attribute of nodes [5], the connection ability of edges [6], the substitutability of nodes [7] and so on. In practice, the cost of attacking the router nodes of the inter-domain routing system varies widely. Therefore, the attack cost of damage strategy based on node importance ranking is higher. At this time, it is particularly important to find a group of important nodes through the damage strategy based on cascading failures, and by considering the cost in the inter-domain routing system. A group of important nodes is not of high importance individually, but the combination has the advantages of low attack cost and great damage to the coupled inter-domain routing system [8]. Our work studies the damage strategy considering attack cost, which is a multi-objective optimization problem.

For the strategy considering attack cost, researchers mainly focus on three aspects. The first is the definition of attack cost. To facilitate the calculation, Zhang et al. [9] did not consider the attack cost of each node separately, but defined the total number of attack nodes as the attack cost. Qin et al. [10] considered the attack cost of each node and defined it as the attack cost related to degree of linearity. The second area of concern is the impact of cascading failures in the network. In the existing research, the cascading failures process is only considered in general complex networks [11–14]. However, there are few studies on inter-domain routing networks based on BGP because of the complexity of cascading failures. The third concern is the optimization effect. Wang et al. [15] defined three indicators to measure the criticality of each node and used an exhaustive method to find the optimal solution. To improve efficiency, the researchers propose a method based on search space reduction [16]. After that, the researchers introduce heuristic algorithms to solve the problem and generate low-cost and high-yield damage strategies as much as possible [17]. Although the existing research results are abundant, the following problems still exist:

1) The definition of attack cost in existing methods is vague. For example, the number of attack nodes is the attack cost, which cannot distinguish the difference in attack cost between different nodes, nor can it reflect the real situation of attacking key nodes and non-key nodes.

2) The existing methods do not consider the cascading failures mechanism in the inter-domain routing system.

3) The double objective optimization effect of the existing methods is not obvious, and the cost is still high.

Based on the above problems, we propose a method to generate damage strategies for inter-domain routing systems based on multi-objective optimization (PMT). We transform the damage strategy problem into a double-objective optimization problem. The main work is as follows:

1) We transform the damage strategy problem into a double objective optimization problem and propose the attack cost related to degree of nonlinearity.

2) We propose an initialization strategy based on network partition. First, partition the network, and then generate the initial population based on the partitioned network. It enriches the diversity of the initial population and makes the population evenly distributed in the network.

3) We propose a node replacement strategy based on partition search, which can accelerate the convergence speed and improve accuracy.

4) In two real inter-domain routing networks, we compared PMT with five common damage strategy algorithms. The experimental results verified the effectiveness and accuracy of PMT.

The follow-up arrangement of the article is as follows. Section 2 gives the related work and preliminaries, including the cascading failures principle and NSGA-II. In Section 3, the damage strategy problem based on cascading failures is transformed into a multi-objective optimization problem. Section 4 introduces the PMT proposed in detail. Section 5 presents the experimental results and analysis. The last is the conclusion.

2. Related work and preliminaries

2.1. Related work

The increasing scale of networks has prompted scholars to increase their enthusiasm for the study of cascading failures. Zhao et al. [18] proposed a cascading failures model based on cellular automata for road networks. It introduces the time characteristics of load distribution and node recovery ability into the previous cascading failure model. Finally, they analyze the vulnerability of road networks through the use of improved maximum connectivity and the node failure rate based on node degree.

Huang et al. [19] developed a model to analyze the cascading failures of multistate loading-dependent systems. The model depicts the cascading failures phenomenon after load overload. Zhou et al. [20] proposed a resilient network recovery framework against cascading failures with deep graph learning. It can obtain network topology in real time and prioritize the maintenance of failed nodes based on customer preferences. Zhou et al. [21] optimized the resiliency-based recovery method for cascading failures in the network. Different restoration prioritization strategies are applied to network systems subject to cascading failures that take into account system dependencies.

For the cascading failures model of complex networks, we have proposed the CFM-RFM [22] in our previous work and verified the effectiveness of the model. Therefore, the work of this article directly refers to the CFM-RFM.

Evolutionary algorithms are used to solve complex problems. Based on the MSIQDE algorithm, Deng et al. [23] proposed an enhanced MSIQDE (EMMSIQDE) algorithm based on mixing multiple strategies. EMMSIQDE introduces a new differential mutation strategy of a difference vector and a new multi-population mutation evolution mechanism, which can effectively solve complex optimization problems. To effectively dispatch railway trains, Song et al. [24] designed an evolutionary algorithm with a dynamic hybrid mechanism comprised of a quantum evolutionary algorithm and genetic algorithm (QGDEC). QGDEC innovates the quantum variable decomposition strategy and the increment mutation method. In order to solve problems of premature convergence and local optimization, Deng et al. [25] proposed an adaptive differential evolution algorithm based on belief space and generalized opposition-based learning for resource allocation.

A multi-strategy particle swarm and ant colony optimization algorithm were proposed for airport taxiway planning [26]. It designs a new pheromone allocation mechanism and develops a pheromone update strategy based on the principle of wolf predation, which can effectively solve the traveling salesman problem. In addition, deep learning methods [27] are also used to solve complex problems.

A method of damage strategy considering the cost needs to optimize not only the degree of damage to the network, but also the attack cost, which is a multi-objective optimization problem. For complex networks, the cost is seldom considered in the existing damage strategy methods. Wang et al. [11] studied how to efficiently allocate limited resources to minimize network damage when complex networks face various damage strategies. They found that, under the premise of considering the cost, the network has an optimal allocation scheme of defense resources, which can maximize the protection of the network. The optimal defense scheme is related to the basic parameters of the network. The experimental results show that the network with sparse connections is more conducive to protecting the network.

Tan et al. [12] analyzed the effectiveness of the attack strategy considering the cost and proposed two new evaluation indicators: the compactness coefficient of closeness and the compactness coefficient of betweenness. The experiment shows that the degree attack strategy is the worst for the same network. Under the same average degree, the attack strategy with a smaller closeness compactness coefficient or betweenness compactness coefficient performs better.

Ye and Jun [13] proposed a cost constraint model to solve the problem of an attack strategy in complex networks. The model thinks that the nodes with a higher degree will be attacked preferentially when the constraints are lower. The nodes with the smaller degree will be attacked preferentially when the constraints are higher. In addition, it was found that there is a cost evaluation threshold. If the cost of the attacked node is less than this threshold, the node with the lower degree will be attacked first. Hong et al. [28] mainly studied the robustness of complex networks when they are attacked under the premise of considering the cost. The relationship between node attack and edge attack is not clearly explained.

Wang et al. [14] proposed a complex network edge attack strategy considering the attack cost based on existing research. In this strategy, the weight of the edge is defined as the attack cost of the edge, and the average path length and maximum connected subgraph are used to evaluate the damage degree of the network. In ordinary scale-free networks and exponentially adjustable scale-free networks, the edge attack strategy with adjustable weight parameters is simulated. The experimental results show that the attack effect is not affected when the parameters of edge weight are different. It shows that the edge weight parameter is not an important influential condition. When the attack cost is small, the edge attack with a larger weight is better.

Zhang et al. [9] solved the damage decision-making problem from the perspective of multi-objective optimization, and they proposed a cascading key node detection algorithm (MO-BCVND) based on multi-objective optimization for complex networks. Based on an NSGA-II framework, MO-BCVND improves the search strategy and speeds up convergence. In 12 complex networks, the effectiveness of MO-BCVND is proved by simulation attacks. At the same time, MO-BCVND can generate different levels of attack node groups, which can provide a basis for network vulnerability analysis. MO-BCVND is a cascade key node detection algorithm that considers both the cost and the effect of the attack. However, the attack cost is relatively simple and it cannot reflect the difference between attacking critical nodes and non-critical nodes. The application scenario is only for general complex networks. For the special network of inter-domain routing systems, the initialization strategy needs to be improved.

In view of the problems in the existing methods, we proposed a method for generating damage strategies based on multi-objective optimization (PMT). It can not only approximate the attack cost of nodes, but it can also consider the cascading failures mechanism in inter-domain routing systems. The experimental results show that PMT is effective.

2.2. *Cascading failures*

The analysis of the failure principle can be divided into two parts. As shown in Figure 1, there are the failure causes of nodes and links and the causes of cascading failures.

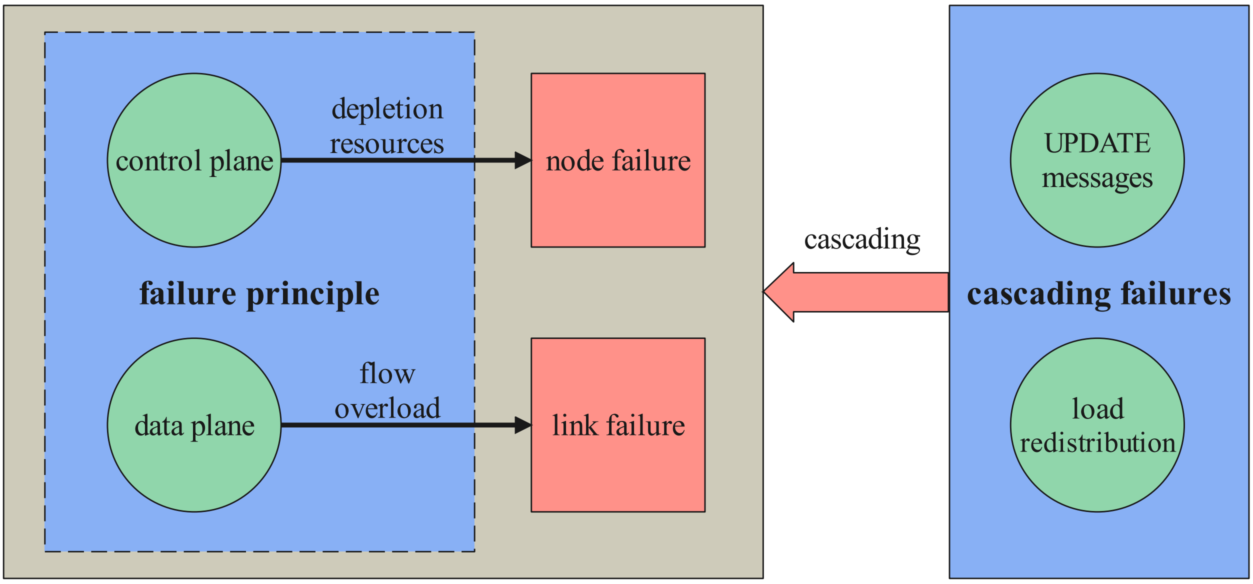


Figure 1. Failure principle.

1) Failure causes of nodes and links.

Data plane load and control plane load cannot be confused in inter-domain routing systems. Data plane load refers to the data load forwarded by routing nodes. Control plane load refers to the load used to maintain the connection relationship between inter-domain routes, such as UPDATE messages. A node failure occurs when a large number of UPDATE messages arrives at the control plane at the same time, resulting in node CPU, memory and other resources being exhausted. A link failure is caused by the surge and overload of the data plane load that needs to be forwarded in a short time.

2) Causes of cascading failures.

When a node fails, it is temporarily removed from the network and its neighbors send UPDATE messages to notify other nodes on the network. This process is the propagation of UPDATE messages. When the link fails, the forwarding task of the data load is completed by other working links. This process is called load redistribution, which redistributes the load of the failed link to other working links. The propagation process of UPDATE messages and load redistribution are the main causes of cascading failures.

2.3. NSGA-II

A multi-objective optimization algorithm refers to an algorithm used to solve multi-objective optimization problems. Schaffer [29] proposed an algorithm based on vector evaluation to solve related multi-objective optimization problems, which is the first time that an evolutionary algorithm has been applied to the field of multi-objective optimization. Then, more and more researchers became able to solve the multi-objective optimization problem based on evolutionary algorithms.

The concept of Pareto ranking was proposed by Goldberg [30]. It points out that the distribution should be maintained in the algorithm, which provides important support for the mainstream algorithms studied later [31]. NSGA-II, proposed by Deb et al. [32], was the most representative. PMT is based on the NSGA-II framework, and NSGA-II is introduced in detail below.

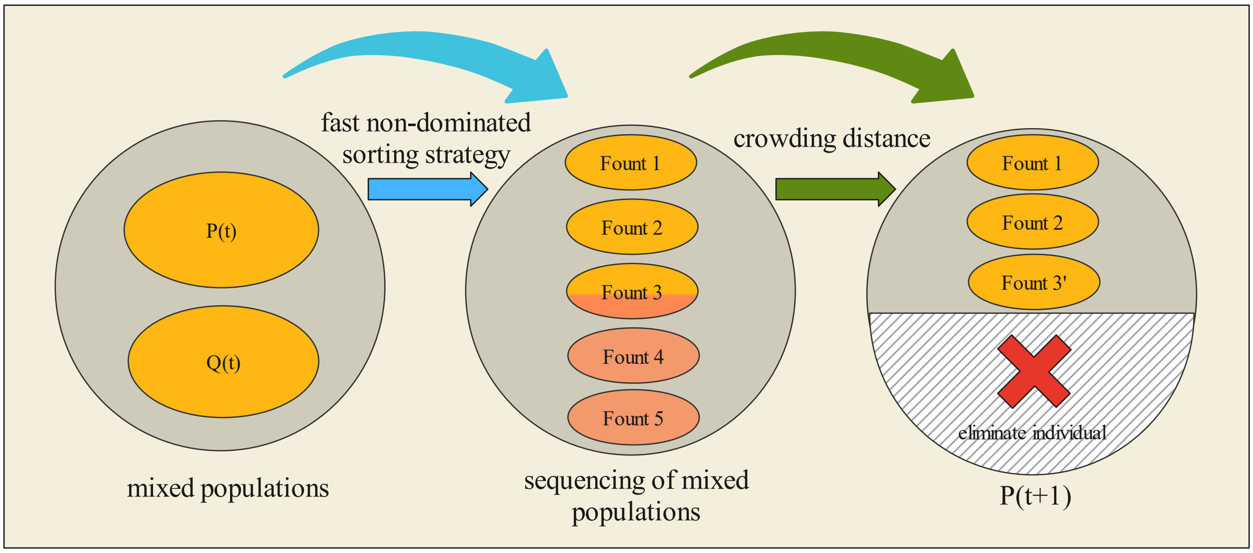


Figure 2. NSGA-II.

NSGA-II is an improved version of NSGA. Compared with NSGA, NSGA-II has the following advantages.

1) A fast non-dominated sorting strategy is designed in NSGA-II. The algorithm complexity is reduced from $O(mN^3)$ to $O(mN^2)$, which greatly improves the running speed of NSGA-II.

2) NSGA-II proposes an evaluation method of crowding distance to judge the advantages and dis-

advantages of individuals on the same front, which can ensure the accuracy of population evolution.

3) To maintain the quality of the population and avoid the loss of excellent individuals in the process of evolution, NSGA-II adopts the elite retention mechanism. That is, the individuals with good performance in the parent generation are retained and merged to participate in the new generation process of the next generation.

Figure 2 shows the basic flow of NSGA-II. The evolutionary process consists of three steps. For the process of evolution from generation t to generation t+1:

Step 1: First, the parent population *P(T)* generates the offspring population *Q(T)* through the cross and mutation strategy. According to the elite retention strategy, the parent population *P(T)* is put into the offspring population *Q(T)* to form a mixed population.

Step 2: By using the fast non-dominated sorting strategy to sort the mixed population, we can get the front serial number of all individuals.

Step 3: The last is the environmental selection, which selects the new population with the number *N* from the mixed population with the number 2*N*. As shown in Figure 2, the number of individuals selected for the first three fronts exceeds *N*, so the individuals in the third front can only select a part. At this time, the individuals in the third front are sorted through the crowding distance strategy, and the individuals satisfying the total number *n* are selected. The third front part of the unselected individuals, the fourth front and the fifth front of all individuals were eliminated. The loop continues until the algorithm reaches a preset termination condition.

3. Transformation of the problem

For the damage strategy of cascading failures, most previous studies have transformed this problem into a single objective optimization problem. Specifically, they rank the importance of nodes according to various attributes of the network from the perspective of the attacker. Only the damage degree of the network is taken as the objective function, so attacking the nodes with the highest importance ranking can cause the maximum damage to the network. This kind of research does not consider the cost of nodes. By default, the attack cost of nodes is the same. This is not reasonable in reality. Nodes with higher importance are more difficult to attack. To get closer to reality and find low-cost and high-yield damage strategies, we transform the damage strategy problem based on cascading failures into a multi-objective optimization problem, that is, minimizing the attack cost and maximizing the attack effect simultaneously.

The damage strategy problem for inter-domain routing systems based on cascading failures is expressed as follows:

$$\begin{aligned} &Minimize\ \mathbf{T}(P) = (C(P), -F(P))^T \\ &s.t. \qquad P \in PS, C(P) \in [0,1], F(P) \in [0,1], \end{aligned} \tag{3.1}$$

where, $\mathbf{T}(P)$ is an objective function vector, *P* denotes the initial attack node group and *PS* denotes the collection of all attack node groups. *C(P)* denotes the normalized cost of the initial attack node group. *F(P)* denotes the degree of network damage after failure caused by the attack, which is expressed by the failure rate in this paper. To minimize the whole, *F(P)* takes the opposite number. From Eq (3.1), we can see that the objective of optimization in this paper is to attack the node group with the lowest cost as much as possible while causing maximum damage to the network.

3.1. Attack cost

Due to the limited attack resources, we must pay attention to the attack cost. Qin et al. [10] defined that the attack cost is related to the degree, which has low complexity and can reflect the importance of nodes to a certain extent. It is considered that this definition is reasonable. In real attack scenarios, the attack cost of a node is equivalent to the strength of node defense resource deployment. From the perspective of the defender, the deployment of defense resources of nodes with a high degree is usually several times or more powerful than that of nodes with a low degree. Therefore, the attack cost related to the degree of nonlinearity is defined in this paper. The attack cost after an attack on the network can be expressed as follows:

$$C(P) = \frac{\sum\limits_{u \in P} (d(u) + \delta d(u)^{\gamma})}{\sum\limits_{v \in V} (d(v) + \delta d(v)^{\gamma})}, \tag{3.2}$$

where $d(u)$ is the degree of u and V is the set of all nodes in the network. $C(P)$ is the normalized cost. For the convenience of calculation, set $\delta = 1$, $\gamma = 2$.

3.2. Failure rate

After cascading failures, both nodes and links may fail. Therefore, to evaluate the damage degree of the network, both the failed node and the failed link should be considered. To quantify the impact of cascading failures for inter-domain routing networks, the average failure rate is defined as follows:

$$f_{\mathrm{FR}} = \frac{N_{Fv} + N_{Fe}}{W}, \tag{3.3}$$

where N_{Fv} denotes the number of failed nodes, N_{Fe} denotes the number of failed links and W denotes the total number of initial nodes and links. It is generally believed that the failure rate is directly proportional to the degree of damage to the network.

4. Methods

After the transformation of the previous problem, the next main work is how to find the Pareto optimal solution set in the multi-objective optimization problem. This section proposes an algorithm to generate damage strategies for inter-domain routing systems based on multi-objective optimization (PMT) to find an optimal group of attack nodes.

4.1. The general framework of PMT

Based on the basic framework of NSGA-II, we propose PMT, which can better solve the damage strategy problem of cascading failures of inter-domain routing systems.

Algorithm 1 shows the steps of PMT, which mainly includes three processes. The first is population initialization. We propose an initialization strategy based on network partitioning. First, the network is divided into several small regions based on the locations and attributes of nodes in the inter-domain routing systems. Then, the initial attack nodes are selected according to the rules, and a diverse population can be obtained. The second process is population evolution, which first mutates and crosses over to produce offspring. Then, the node replacement strategy based on partition search is used to optimize the offspring. Finally, according to the elite retention strategy, the offspring population and the parent population were combined, and the non-dominated ranking and crowded distance were applied to select individuals and update the population. The third process is to obtain the Pareto optimal solution set from the final population by using an efficient non-dominated sorting algorithm.

Algorithm 1 PMT

```
Input: network $G$; model parameters $\alpha$, $\beta$; population size NPop; binary individual length Nbits;
    iterations Niter; probability of variation Pm; probability of crossover Pc
Output: non-dominated solutions ParetoPops; non-dominated fitness value ParetoFits
Step1: population initialization
Pops ← Initpops (G, Nbits, NPop)
Fits ← Fitness (Pops)
Step2: population evolution
while $iter \leq Niter$ do
    Chrpops←Crossover (Pops, pc)
    Chrpops ← Mutate (Chrpops, pm)
    Chrpops ← PAC (Chrpops)
    Chrfits ← Fitness (Chrpops)
    Pops, Fits ← optSelect (Pops, Fits, Chrpops, Chrfits)
    iter ← iter + 1
end while
Step3: obtain the non-dominated solutions and fitness value
ParetoPops, ParetoFits ← SelectNonDominatedsets (Pops, Fits)
```

The core idea of PMT is to divide the network into multiple regions and attack some nodes in each region respectively. "Crush one by one" in all areas so that a small number of nodes can damage the entire network. It can be seen from Algorithm 1 that the initialization strategy based on network partitioning and the node replacement strategy based on partition search are two important parts of PMT.

4.2. Initialization strategies based on network partitioning

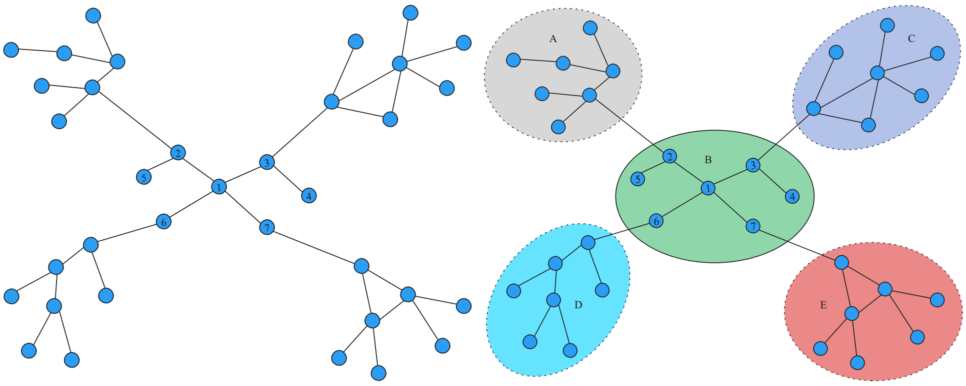
In multi-objective genetic algorithms, the initial population is generated by randomly initializing the population to meet the generalization ability of the population. In general problems, random initialization of the population has good results. However, for the damage decision problem of inter-domain routing systems, the random initialization population is prone to the clustering of nodes or too large a search space. To ensure the superiority of the algorithm and avoid the above problems, we propose an initialization strategy based on network partitioning.

4.2.1. Network partitioning

Algorithm 2 shows the process of partitioning. Partitioning is based on the logical location of nodes. Neighboring nodes are divided into an area as far as possible. First, find the edge-nodes v in the network, that is, the node with degree 1. Then, it takes v as the starting point to find neighbor nodes of *j*-order. When the number of *j*-order neighbor nodes < $\lceil N/K \rceil$ (the number of nodes in each region), continue to find (*j*+1)-order neighbor nodes. The search is stopped when the number of (*j*+*r*)-order neighbor nodes ≥ $\lceil N/K \rceil$. If the number of nodes exceeds $\lceil N/K \rceil$ and the difference is *d*, then the *d* nodes with the largest degree are removed from the neighbors of (*j*+*r*)-order. This can make the number of nodes in each region meet the requirements, and *v* forms a region with the neighbors of (*j*+*r*)-order and removes it from the network. This loop continues until the network is divided into *K* regions. Figure 3(a) is a simple network, and Figure 3(b) is the result of partitioning. It can be seen that the nodes in the network are orderly divided into five regions, A, B, C, D and E. The nodes in the regions are closely connected. When a few nodes are attacked, cascading failures are likely to occur in the region. Therefore, network partitioning is conducive to generating the strategy.

Algorithm 2 Network partitioning

```
Input: network G; number of nodes N; number of partitions K
Output: node group after partition PartitionSet
Step1: find the set of edge-nodes NodeDgreeOneSet
for node ∈ G do
    if G.degree (node) = 1 then
        NodeDgreeOneSet.add (node)
    end if
end for
Step2: get PartitionSet
for i ← 1 to $\lceil N/K \rceil$ do
    node ← Random (NodeDgreeOneSet, 1)
    temp.add (node)
    for j ← 1 to ∞ do
        NeigborsNodeSet ← Getneigbors (G, node, j)
        temp.add (NeigborsNodeSet)
        if len (temp) ≥ $\lceil N/K \rceil$ then
            d ← len (temp) - $\lceil N/K \rceil$
            if d = 0 then
                PartitionSet.add (temp)
                Update (G, NodeDgreeOneSet)
                break;
            else
                RemSet ← SelectMaxDegree (NeigborsNodeSet, d)
                temp.delete (RemSet)
                PartitionSet.add (temp)
                Update (G, NodeDgreeOneSet)
                break;
            end if
        end if
    end for
end for
```



(a) Before partition (b) After partition

Figure 3. A simple network partition.

4.2.2. Encoding

PMT uses binary encoding to represent individuals $pop = (p_1,p_2,...,p_i,...,p_n)$, which indicates the attack node group. The parameter p_i indicates the state of the node. $p_i = 1$, indicating that node i is the invalid state after being attacked. $p_i = 0$ indicates that node i is not attacked and is working properly. For example, $pop = \{1,0,0,1,0,1,0,0\}$ indicates that the attacked node is {1,4,6}. Since binary coding is used, PMT uses uniform crossover and bitwise mutation.

Algorithm 3 Initialization strategies

```
Input: network $G$; number of nodes $N$; number of partitions $K$; population size $NPop$; binary individual length $Nbits$; node group after partition $PartitionSet$
Output: initial population $Pops$
Step1: remove edge-nodes
for $node \in G$ do
    if $G.degree\ (node) = 1$ then
        $G.ndoe.delete\ (node)$
    end if
end for
$N \leftarrow$ Len $(G.ndoe)$
Step2: select the initial attack node according to the partition
for $i \leftarrow K\ to\ nPop$ do
    $TempIndividual \leftarrow [0] * Nbits$
    for $z \leftarrow 1\ to\ i + 1$ do
        $z \leftarrow z\ \%\ K$
        $Index \leftarrow$ RandomNodeIndex $(Partitionset, \lceil N/K \rceil, z)$
        $TempIndividual\ [Index] \leftarrow 1$
    end for
    $Pops.add\ (TempIndividual)$
end for
```

4.2.3. Initialization strategies

After the network is divided into several regions, the population can be initialized. Algorithm 3 gives the initialization process.

In the inter-domain routing network, there is a large number of edge-nodes and they only have small traffic requests, which is not enough to pose a threat to other nodes. Therefore, edge-nodes are removed from the range of initially selected attack nodes to improve the probability of selecting "strong" nodes. Then, select the initial attack node according to the partition. Set K to the minimum number of nodes that allows individual attacks to ensure that *pop* attacks at least one node in each region. For *pop*, it is necessary to determine the number of attack nodes and then select attack nodes at random in each region of the network. Considering the diversity of the population, the number of attack nodes of *pop* is different, which can ensure the diversity of the attack cost. It can be seen that the initialization strategy based on network partitioning can ensure that the attack nodes of *pop* are spread all over the network, which can damage the network to the greatest extent.

4.3. Node replacement strategies based on partition search

For PMT, although the evolution of the population can be realized through the crossover process and mutation process, this kind of universal evolution mode is not stable. For the damage strategy of inter-domain routing systems, the convergence speed is limited. Therefore, we propose a node replacement strategy based on partition search to realize population evolution. Node replacement is based on the principle of priority of the node damage conversion rate (DCR). This can not only improve the convergence speed, but it can also accurately search and reduce unnecessary search actions.

4.3.1. Damage conversion rate

DCR refers to the ratio of failure rate to attack cost. It is defined as

$$DCR(P) = \frac{f_{\mathrm{FR}}}{C(P)}. \tag{4.1}$$

It can be seen that the DCR is proportional to f_{FR} and inversely proportional to $C(P)$. When the DCR of *pop* is higher, it indicates that the attack cost performance of *pop* is higher.

4.3.2. Implementation process

Algorithm 4 shows the implementation of this strategy. It includes three stages: calculating the DCR of nodes, deleting nodes and adding nodes. Specifically, first calculate the DCR of attack nodes in *pop*. In the stage of deleting nodes, delete the node v with the lowest DCR in *pop*. Then, *pop* becomes pop^a. In the stage of adding nodes, calculate the region P where the deleted v is located, and find the node w with the largest DCR in region P. If w is not in pop^a, add it to pop^a and change it to pop^d. If w is in pop^a, delete the w in region P. Continue searching for the node in region P with the largest DCR until w is not in pop^a to end the search. Finally, if DCR (w) > DCR (v), pop^d is output as the evolved individual. The strategy only searches in the region where nodes are deleted, which can not only complete the search quickly, but it can also accurately improve the DCR of *pop*.

Take the simple network in Figure 3(b). There is *pop* containing node 4 of region B that assumes that node 4 has the lowest DCR. Step 1: Calculate the DCR of nodes in region B, assuming that the order from largest to smallest is {1,3,2,6,7,5,4}. Step 2: Remove node 4 from *pop*. Step 3: Since node 1 has the largest DCR, it waits to be added to *pop*. If node 1 is not in *pop*, it is added to *pop* to evolve into a new *pop*′. If node 1 is in *pop*, the search continues until the search node is not in *pop* or the search space is empty to stop the search.

Algorithm 4 Node replacement strategies based on partition search

```
Input: network $G$; number of nodes $N$; number of partitions $K$; population size $NPop$; $pop$
Output: evolutionary individuals $pop'$
Step1: calculate the DCR value of the node
DCR ($v$) $\leftarrow$ GetPopDCR ($pop$)
Step2: remove node
$v \leftarrow \arg\min_{v \in pop'}$ (DCR ($v$))
$pop^a \leftarrow$ Remove ($pop,v$)
Step3: add node
for $P \leftarrow PartitionSet$ (0) to $PartitionSet$ ($\lceil N/K \rceil$) do
    if $v \in P$ then
        $pop^d \leftarrow pop^a$
        while $pop^a = pop^d$ do
            DCR (w) $\leftarrow$ GetPopDCR (pop)
            w $\leftarrow \arg\min_{v \in pop'}$ (DCR ($w$))
            if w $\notin pop^a$ then
                $pop^d \leftarrow$ Add ($pop^d$, $w$)
            else
                $P.remove$ ($w$)
            end if
        end while
    end if
end for
if DCR ($w$) > DCR ($v$) then
    $pop' \leftarrow pop^d$
else
    $pop' \leftarrow pop$
end if
```

5. Experimental results and analysis

5.1. Parameter setting

Topological structures of the UK and Canada were selected from the AS-Relationships dataset of the CAIDA project [33] to establish the basic network of the experiment, including the connection relationship and business relationship between nodes. The CFM-RFM model proposed in the previous work [22] can accurately simulate the cascading failures of inter-domain routing systems after verification. Therefore, to ensure the accuracy and authenticity of the comparative experiment, the experiment was run on the CFM-RFM model. Network and simulation-related parameters are shown in Table 1.

Table 1. Parameter settings.

Parameter	UK	Canada
V	1191	1523
E	2946	2508
α	1	1
β	0.3	0.3
R	120	150

In this section, PMT is compared and analyzed against five existing algorithms of damage strategies to verify its effectiveness. The comparison algorithm includes two algorithms based on single objective optimization, AIPR [34] and SD-KNI [35], which do not consider the attack cost. The other three are based on multi-objective optimization algorithms NSGA-II [32], MO-BCVND [9] and DSCT [36].

AIPR is an autonomous systems importance attack policy based on preferred routes. The policy considers that the more valid paths passing through a node, the higher the priority of the node being attacked.

SD-KNI is an attack strategy for inter-domain routing systems based on propagation dynamics. Although the dynamic process is considered, it is based on the premise of no cost assumption.

DSCT has two indicators: the load of the link connected to the node and the number of reachable nodes of neighbor nodes. Then, it introduces the attack cost related to degree of nonlinearity and finally calculates a group of node attack sequences through the use of TOPSIS.

NSGA-II is a classical multi-objective optimization genetic algorithm. Our proposed PMT is similar to the NSGA-II framework, and the comparison results are persuasive.

MO-BCVND is a cascade critical node detection algorithm based on multi-objective optimization in complex networks. In MO-BCVND, an initialization strategy based on cost reduction is proposed to increase the diversity of the population. To improve the convergence rate of the population, an adaptive local search strategy is proposed.

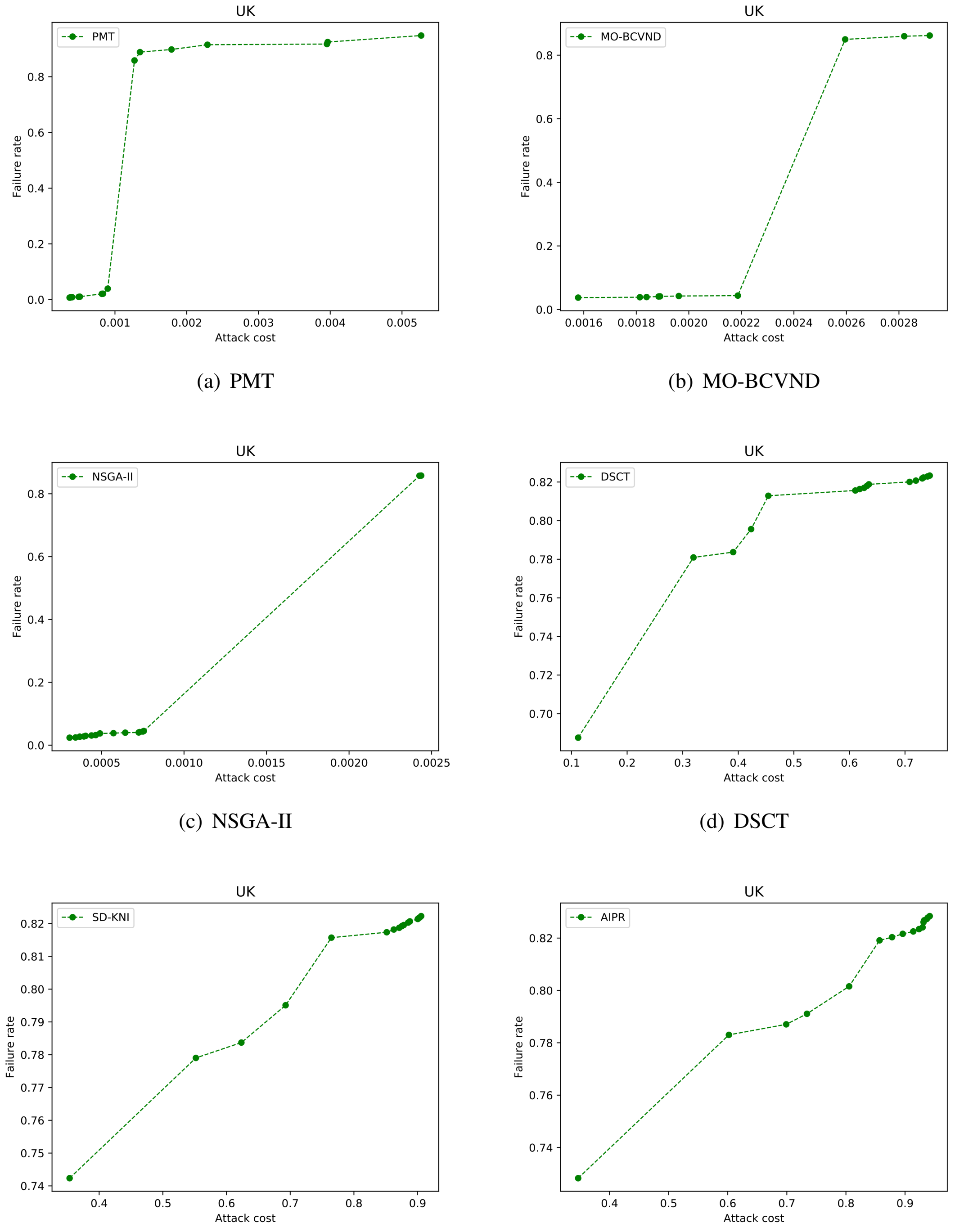
PMT and all comparison algorithms were implemented in Python. All of the experiments were completed under the conditions of a Windows 10 operating system; the computer was configured with an i7-10700 processor and 16GB RAM. For PMT, the population size was set to 100, the mutation probability to 0.01, the crossover probability to 0.6 and the total number of iterations to 100. All comparison algorithms apply the parameters suggested in the paper.

5.2. Effectiveness analysis of PMT

This section shows the comparison results between PMT and the other five algorithms on two real inter-domain routing networks. The effectiveness of PMT is verified by the failure rate, and the attack cost performance of PMT is evaluated by the DCR.

1) Verification of failure rate

Each method was applied to calculate the respective solution, that is, the optimal node attack set with different attack costs. In two networks, the network is attacked according to the node attack set of each method. The relationship between attack cost and failure rate is shown in Figures 4 and 5. The attack cost of abscissa is the result of normalization.



(a) PMT

(b) MO-BCVND

(c) NSGA-II

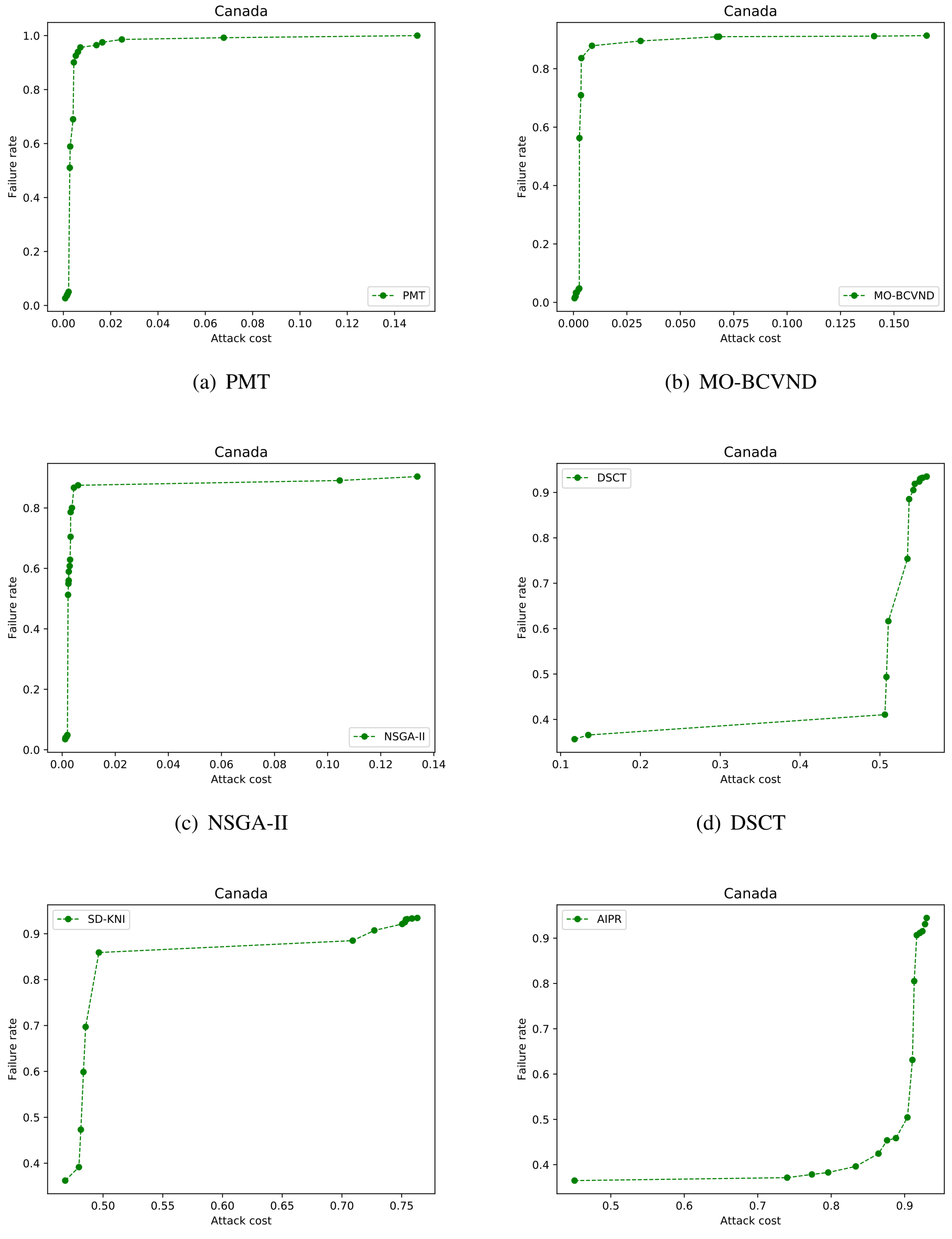
(d) DSCT

(e) SD-KNI

(f) AIPR

Figure 4. Relationship between attack cost and failure rate in the UK.

As can be seen in Figures 4 and 5, the effects of PMT, DSCT, NSGA-II and MO-BCVND based on multi-objective optimization are much better than those of AIPR and SD-KNI based on single objective optimization in the two networks. When the attack cost is small, it has an obvious attack effect. Therefore, the abscissa magnitude of Figure 5(a)–(c) is small. The optimization ability of the



(a) PMT

(b) MO-BCVND

(c) NSGA-II

(d) DSCT

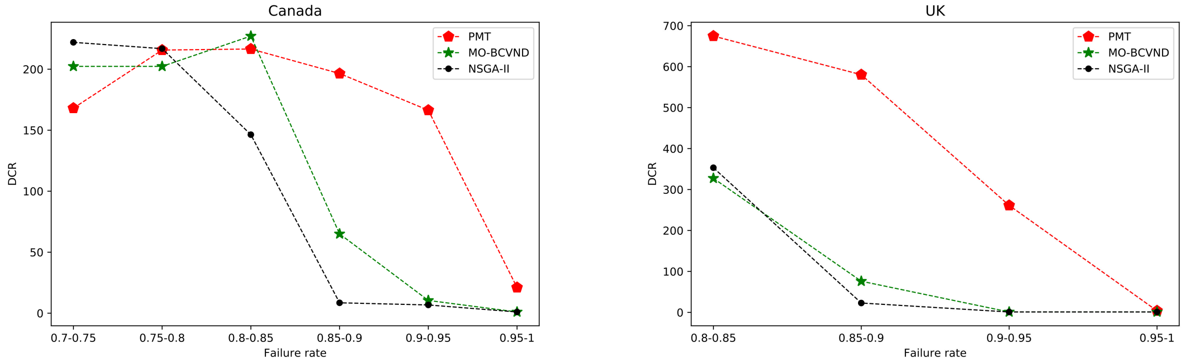
(e) SD-KNI

(f) AIPR

Figure 5. Relationship between attack cost and failure rate in the UK.

algorithm in Figure 5(d)–(f) is general. When the attack cost of the abscissa is large, there is an obvious attack effect. Only by increasing the attack cost of the abscissa can we see the attack effect in the plot. This is also the reason for the large difference in the abscissa orders of magnitude in Figure 4.

It can be found that the results of PMT, NSGA-II and MO-BCVND are seriously divided. The node attack set with low cost and a high failure rate accounted for the majority, and the sets with intermediate values were few. This phenomenon is mainly caused by multi-objective optimization. In Canada's network, the best non-dominated solution of PMT among the four multi-objective optimization algorithms can paralyze the network. That is, the failure rate is 0.95, and the cost is only 0.149. However, the non-dominated solution of NSGA-II and MO-BCVND maximally increases the network failure rate to about 0.9, and the attack cost is larger than that of PMT under the same condition.



(a) Canada

(b) UK

Figure 6. Comparison of DCR.

2) Evaluation of DCR

As can be seen in Figures 4 and 5, the orders of magnitude of PMT, NSGA-II and MO-BCVND are close. To further analyze the attack cost performance of PMT, the DCRs of PMT, NSGA-II and MO-BCVND were calculated and compared for the two inter-domain routing networks. Figure 6 shows the relationship between the failure rate and the DCR of the network caused by different methods. Since the failure rate of the final solution obtained by each method is not consistent, the failure rate of the abscissa is reflected by the interval, and the DCR is the average of the corresponding interval.

Figure 6(a) shows that, when the failure rate is between 0.7–0.8, the DCRs of NSGA-II and MO-BCVND are slightly higher than that of PMT in Canada. However, when the failure rate is between 0.8–0.85, PMT and MO-BCVND have similar cost performance, which is higher than NSGA-II. When the failure rate is greater than 0.85, it can be seen that the DCRs of NSGA-II and MO-BCVND decrease significantly. At this time, PMT is undoubtedly the most cost-effective attack algorithm. As can be seen in Figure 6(b), the DCR of PMT in the UK is better than the other two algorithms, and it is the preferred algorithm for damage strategies. In general, PMT has the advantage of high-cost performance compared with common damage strategies algorithms. It can generate low-cost and high-yield damage strategies and provide decision-makers with different levels of damage strategies.

6. Conclusions

As an important infrastructure of the Internet, inter-domain routing systems play a significant role in supporting the stable operation of the Internet. To better analyze the vulnerability of inter-domain routing systems, we have proposed a method for generating damage strategies in inter-domain routing systems based on multi-objective optimization (PMT). The damage strategy based on cascading failures is transformed into a multi-objective optimization problem, that is, the attack cost and attack effect of nodes are optimized simultaneously. We define the attack cost related to the degree of nonlinearity, and the attack effect is the failure rate of the network after cascading failures. For PMT, we propose an initialization strategy based on network partitioning and a node replacement strategy based on partition search. In the experimental part, PMT was compared with five common damage strategies methods, and the experimental results verify the effectiveness and accuracy of PMT. Our algorithm can output node sets of low cost and high yield, which can meet the needs of attackers. And, it can provide multi-angle information for the defender and make it possible to predict an unknown attack.

Acknowledgments

Thanks for the experimental environment provided by the School of Electronic Engineering, National University of Defense Technology.

Conflict of interest

The authors declare that there is no conflict of interest.

References

1. J. Cowie, A. Ogielski, B. Premore, Y. Yuan, *Global Routing Instabilities Triggered by Code Red ii and Nimda Worm Attacks*, Tech. Rep., Renesys Corporation, 2001.
2. R. Durairajan, Robustness and the internet: A geographic fiber-optic infrastructure perspective, in *Geographies of the Internet*, Routledge, (2020), 47–62.
3. P. Bonacich, Factoring and weighting approaches to status scores and clique identification, *J. Math. Sociol.*, **2** (1972), 113–120.
4. L. Freeman, A set of measures of centrality based upon betweenness, *Sociometry*, (1977), 35–41.
5. Y. Ruan, J. Tang, Y. Hu, H. Wang, L. Bai, Efficient algorithm for the identification of node significance in complex network, *IEEE Access*, **8** (2020), 28947–28955. https://doi.org/10.1109/ACCESS.2020.2972107
6. J. Liu, Q. Xiong, W. Shi, X. Shi, K. Wang, Evaluating the importance of nodes in complex networks, *Physica A*, **452** (2016), 209–219. https://doi.org/10.48550/arXiv.2111.13585
7. W. Zhao, Y. Wang, X. Xiong, F. Yang, Finding key nodes in complex networks: An edge and local partition approach, in *2020 IEEE 6th International Conference on Computer and Communications (ICCC)*, (2020), 1053–1057. https://doi.org/10.1109/ICCC51575.2020.9345096
8. C. Fan, L. Zeng, Y. Sun, Y. Y. Liu, Finding key players in complex networks through deep reinforcement learning, *Nat. Mach. Intell.*, **2** (2020), 317–324. https://doi.org/10.1038/s42256-020-0177-2
9. L. Zhang, J. Xia, F. Cheng, J. Qiu, X. Zhang, Multi-objective optimization of critical node detection based on cascade model in complex networks, *IEEE Trans. Network Sci. Eng.*, **7** (2020), 2052–2066. https://doi.org/10.1109/TNSE.2020.2972980

10. J. Qin, H. Wu, Y. F. Yi, B. Zheng, Effectiveness of attack strategies of complex networks with cost, *Trans. Beijing Inst. Technol.*, **33** (2013), 67–72.

11. X. Wang, S. Guan, C. H. Lai, Protecting infrastructure networks from cost-based attacks, *New J. Phys.*, **11** (2009), 033006. https://doi.org/10.1088/1367-2630/11/3/033006

12. J. Tan, H. Wu, Y. Yi, B. Zheng, Research on the effectiveness of complex network attack strategy under cost, *Trans. Beijing Inst. Technol.*, **33** (2013), 67–72. https://doi.org/10.15918/j.tbit1001-0645.2013.01.008

13. D. Ye, W. Jun, Optimal attack strategy based on limited cost model on complex network, in *2015 IEEE International Conference on Systems, Man, and Cybernetics*, IEEE, (2015), 105–108. https://doi.org/10.1109/SMC.2015.31

14. E. Wang, Y. Wang, P. Qu, Analysis of the effectiveness of cost based side attack strategy in complex networks, *Syst. Eng. Electron. Technol.*, **40** (2018), 919–926.

15. W. Wang, Q. Cai, Y. Sun, H. He, Risk-aware attacks and catastrophic cascading failures in us power grid, in *2011 IEEE Global Telecommunications Conference–GLOBECOM 2011*, IEEE, (2011), 1–6. https://doi.org/10.1109/GLOCOM.2011.6133788

16. Y. Zhu, J. Yan, Y. Sun, H. He, Revealing cascading failure vulnerability in power grids using risk-graph, *IEEE Trans. Parallel Distrib. Syst.*, **25** (2014), 3274–3284. https://doi.org/10.1109/TPDS.2013.2295814

17. M. Wang, Y. Xiang, L. Wang, Identification of critical contingencies using solution space pruning and intelligent search, *Electr. Power Syst. Res.*, **149** (2017), 220–229. https://doi.org/10.1016/J.EPSR.2017.04.027

18. Y. Zhao, B. Cai, H. H. S. Kang, Y. Liu, Cascading failure analysis of multistate loading dependent systems with application in an overloading piping network, *Reliab. Eng. Syst. Saf.*, **231** (2023), 109007. https://doi.org/10.1016/j.ress.2022.109007

19. W. Huang, B. Zhou, Y. Yu, D. Yin, Vulnerability analysis of road network for dangerous goods transportation considering intentional attack: Based on cellular automata, *Reliab. Eng. Syst. Saf.*, **214** (2021), 107779. https://doi.org/10.1016/j.ress.2021.107779

20. J. Zhou, W. Zheng, D. Wang, D. W. Coit, A resilient network recovery framework against cascading failures with deep graph learning, in *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, (2022), 1748006X221128869. https://doi.org/10.1177/1748006X221128869

21. J. Zhou, D. W. Coit, F. A. Felder, D. Wang, Resiliency-based restoration optimization for dependent network systems against cascading failures, *Reliab. Eng. Syst. Saf.*, **207** (2021), 107383. https://doi.org/10.1016/j.ress.2020.107383

22. W. Zhao, Y. Wang, X. Xiong, Y. Li, Cfm-rfm: A cascading failure model for inter-domain routing systems with the recovery feedback mechanism, *Information*, **12** (2021), 247. https://doi.org/10.3390/info12060247

23. W. Deng, J. Xu, X. Z. Gao, H. Zhao, An enhanced msiqde algorithm with novel multiple strategies for global optimization problems, *IEEE Trans. Syst. Man Cybern. Syst.*, **52** (2022), 1578–1587. https://doi.org/10.1109/TSMC.2020.3030792

24. Y. Song, X. Cai, X. Zhou, B. Zhang, H. Chen, Y. Li, et al., Dynamic hybrid mechanism-based differential evolution algorithm and its application, *Expert Syst. Appl.*, **213** (2023), 118834. https://doi.org/10.1016/j.eswa.2022.118834

25. W. Deng, H. Ni, Y. Liu, H. Chen, H. Zhao, An adaptive differential evolution algorithm based on belief space and generalized opposition-based learning for resource allocation, *Appl. Soft Comput.*, **127** (2022), 109419. https://doi.org/10.1016/j.asoc.2022.109419

26. W. Deng, L. Zhang, X. Zhou, Y. Zhou, Y. Sun, W. Zhu, et al., Multi-strategy particle swarm and ant colony hybrid optimization for airport taxiway planning problem, *Inf. Sci.*, **612** (2022), 576–593. https://doi.org/10.1016/j.ins.2022.08.115

27. H. Zhao, J. Liu, H. Chen, J. Chen, Y. Li, J. Xu, et al., Intelligent diagnosis using continuous wavelet transform and gauss convolutional deep belief network, *IEEE Trans. Reliab.*, (2022), 1–11. https://doi.org/10.1109/TR.2022.3180273

28. C. Hong, X. B. Cao, W. B. Du, J. Zhang, The effect of attack cost on network robustness, *Phys. Scr.*, **87** (2013), 55801. https://doi.org/10.1088/0031-8949/87/05/055801

29. J. D. Schaffer, Multiple objective optimization with vector evaluated genetic algorithms, in *ICGA*, 1985.

30. D. E. Goldberg, K. Deb, A comparative analysis of selection schemes used in genetic algorithms, *Found. Genet. Algorithms*, **1** (1991), 69–93. https://doi.org/10.1016/B978-0-08-050684-5.50008-2

31. N. Srinivas, K. Deb, Muiltiobjective optimization using nondominated sorting in genetic algorithms, *Evol. Comput.*, **2** (1994), 221–248.

32. K. Deb, S. Agrawal, A. Pratap, T. Meyarivan, A fast and elitist multiobjective genetic algorithm: Nsga-ii, *IEEE Trans. Evol. Comput.*, **6** (2002), 182–197.

33. CAIDA, *The Caida AS Relationships Dataset*, 2022. Available from: http://www.caida.org/data/active/as-relationships.

34. L. Hong, Technique of evaluating as importance based on preferred route, *J. Software*, **23** (2012), 2388–2400.

35. H. H. Zhu, H. Qiu, J. H. Zhu, Z. Y. Zeng, Spreading dynamics based key nodes identification in inter-domain routing system, *Chin. J. Network Inf. Secur.*, **5** (2018), 9.

36. W. Zhao, Y. Wang, X. Xiong, M. Wang, DSCT: A damage strategy for inter-domain routing system considering cost and based on topsis, in *2021 4th International Conference on Data Science and Information Technology*, (2021), 218–225. https://doi.org/10.1145/3478905.3478949

AIMS Press