Electrical Power and Energy Systems 121 (2020) 106145

Contents lists available at ScienceDirect

Electrical Power and Energy Systems

journal homepage: www.elsevier.com/locate/ijepes

An automatic algorithm of identifying vulnerable spots of internet data center power systems based on reinforcement learning

Chunjian Kang, Jianwen Huang*, Zhang Zhang, Qiang Liu, Wenping Xiang, Zhiguo Zhao, Xinpei Liu, Liwen Chong

National Computer Network Emergency Response Technical Team /Coordination Center of China, Beijing, China

ARTICLE INFO

Keywords:
Internet data center
Power system
Vulnerability
Reinforcement learning
Maintenance

ABSTRACT

The internet data center (IDC) power system provides power guarantee for cloud computing and other information services, so its importance is self-evident. However, the occurrence time of malignant destructive events such as lightning strikes, errors in operation and cyber-attacks is unpredictable. But the loss can be minimized by formulating coping strategies in advance. So, identifying the vulnerable spots of the IDC power system come to be the key to guarantee the normal operation of information systems. Generally, the IDC power network can be modelled as a graph G, and then, the methods of finding nodes' centrality can be applied to analyse the vulnerability. By our experience, it is not the best approach.

Unlike the previous approaches, we do not solve the issue as the traditional graph problem. Instead, we fully utilize the characteristics of the IDC power network and apply reinforcement learning techniques to identify the vulnerability of the IDC power network. To our best knowledge, it is the first applying of artificial intelligence in traditional IDC power network.

In this article, we propose PFEM, a parallel fault evolution model for the IDC power network, which can accelerate the process of electrical fault evolution. Moreover, we designed an algorithm which can automatically find the vulnerable spots of the IDC power network.

The experiment on a real IDC power network demonstrate that the impact of vulnerable devices derived from our proposed algorithm after failure is about 5% higher than that of other algorithms, and tripping single-digit electrical devices of the IDC power system with our proposed algorithm will lead to loss of all loads.

1. Introduction

A data center is the place to run various information systems, including IT devices and power infrastructures. The power infrastructures play an important role in providing power support for information systems, whose reliable working is very important to the stable operation of the information systems. Without the 7×24 h guarantee of these infrastructures, information systems would not be able to perform their functions, for example, cloud computing, artificial intelligence learning, etc. These infrastructures involve power supply systems, cooling systems, lighting systems, data center infrastructure management systems, video surveillance systems, fire-fighting systems and other auxiliary but very important systems. In these infrastructures, power system is the most important. A typical data center power system is shown in Fig. 1.

At the top of Fig. 1 is the transformers that convert high voltage to low voltage. Below the transformers is the power supply bus system, which is used for transporting power. Generally, it operates in single or multiple busbars with segments, which backup each other by loop switch. The uninterruptible power supply (UPS) [1] system in the middle of Fig. 1 is used to eliminate surges, interruptions, spikes, frequency fluctuations and other anomalies in the power grid. Generally automatic transfer switches (ATS) [2], static transfer switches (STS) [3] or manual transfer switches (MTS) [4] are laid out ahead of UPS for redundant backup of power supply. On the right side of Fig. 1 is the generator system, which is connected to the busbar through ATS or MTS. The role of that system is to ensure the continuous operation of important loads for a short time during power outage. At the bottom of Fig. 1 is the IT load, which consumes the largest power in the data center.

1.1. The importance of the data center power system

From Fig. 1 we can find that the data center infrastructure,

* Corresponding author.
E-mail addresses: vithon@163.com (C. Kang), huangjw17@qq.com (J. Huang).

https://doi.org/10.1016/j.ijepes.2020.106145
Received 6 July 2019; Received in revised form 2 March 2020; Accepted 26 April 2020
Available online 02 June 2020

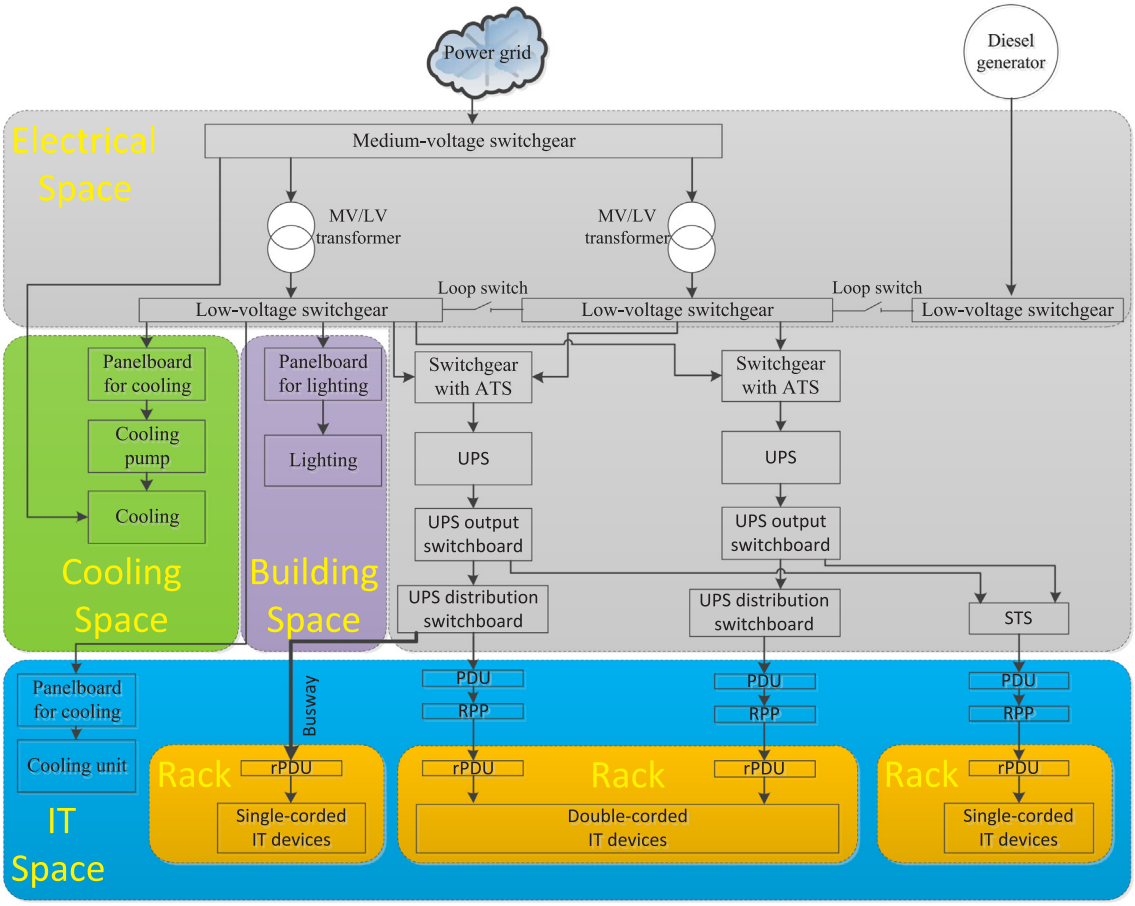


Fig. 1. A typical data center power system including cooling systems, lighting systems, power supply systems, IT systems, etc.

especially power system, is the footstone of the information systems. Correspondingly, once the power distribution system fails, it will directly affect the performance of the information services. Although the reliability of single electrical equipment is high, the IDC power system may turn into crash when some fault happens in the weak spots. Unfortunately, thunder and lightning, errors in operation of staff, fire, hacker attacks occur from time to time, and what makes the matter worse is that the occurrence time is unpredictable. Once these unpredictable accidents occur in weak spots, the consequences may be serious. For example, on July 3, 2009, a fire broke out in a power distribution room in Fisher Square, Seattle, causing the paralysis of Payment Portal, Authorize.net, Geocaching.com Service, Dotster Domain Name Registration Service, Microsoft Bing Travel Service and dozens of other websites [5]. On 23 December 2015, someone made a surprise cyber-attack on three Ukrainian regional electric power distribution companies, which cause several hours' power supply interruption [6]. So, the power system is very important in the data center infrastructure. If some key electrical devices are out-of-service, it would lead some key information services to failure. So, how to strengthen the protection of the IDC power system to avoid large-scale blackouts [7] has become a key issue in power maintenance.

1.2. Definition of vulnerability of the data center power system

However, when the accident happens is terribly hard to predict. The faults may be caused by computing, protection and control, human factors, internal faults, or internet attack. But we can estimate how much loads will loss before some fault happen. This can guide the power network maintenance schedule, help maintenance staff keep a watchful eye on critical devices which should be involved in targeted maintenance plans and contingency plans. So, it is essential to know the vulnerability of the data center power system. There are many definitions and frameworks of power system vulnerability [8]. We aim to quantify the vulnerability of the data center power system, so we define the vulnerability of the data center power system as a measure of the system's weakness with respect to a sequence of cascading events.

The vulnerable spots of the IDC power system are the devices which fail may result in large-scale loss of load. The loss of load can be evaluated by the following equation.

$$Loss = \left(1 - \frac{\sum_{i \in tl \subseteq T_\pi} load_i}{\sum_{j \in gl \subseteq G} load_j}\right) \times 100\% \tag{1.1}$$

where $Loss$ is the ratio of lost loads in the IDC power network when some devices fail, T_π is the stable operating topology of the IDC power network after some failure occurs. tl is the subset of load nodes of T_π, which involves all the working loads. G is the topology graph of the normal IDC power network without any failure. gl is the subset of load nodes of G, which involves all the working and non-working loads. $load_i$ is the power load of load i. In this work, we use the following expression as the quantitative description of vulnerability.

$$Vul = Loss \times \sum_{i \in tr} -\log_{10}(10^4 \times (1 - re(i))) \tag{1.2}$$

$$re(i) = \sum_{j \in \Gamma} \xi_{i,j} * (1 - p_{i,j})$$

$$s.t. \sum_{j \in \Gamma} \xi_{i,j} = 1,\ i \in tr$$

$$p_{i,j} \in (0, 1),\ i \in tr;\ j \in \Gamma$$

In this work, we look closely at the vulnerability of the power system by examining the loss of loads caused by the failure of electrical devices. Because of various factors, the probability of each electrical device failure is different, so it is inappropriate to simply use the loss of loads (Eq. (1.1)) caused by the failure of electrical devices to evaluate the vulnerability of the power system. The vulnerability of the power system should be expressed by the product of the probability of electrical devices failure and the loss of loads caused by these failures. As the electrical devices are generally reliable and the probability of failure is low, the logarithm is used to obtain a large integer in Eq. (1.2) to avoid the calculation errors caused by the computer. In this description the vulnerability of the power system is not only related to the loss of load after faults, but also related to the probability of these faults. *Vul* in Eq. (1.2) is the quantitative description of vulnerability. *Vul* is the product of lost loads and the logarithmic failure probability of the fault electrical devices. The electrical devices stop working one by one, some stop working earlier and some stop working later. *tr* is the set of initial sequential electrical devices with a fault, the earlier ones are put into the front. $re(i)$ is the reliability of node *i,* which is the probability of no fault happen in electrical device *i.* Γ is the set of all the possible events that may cause electrical device *i* failure, and *j* is one of the events. $p_{i,j}$ is the probability of occurrence of event *j* on device *i*. $\xi_{i,j}$is the weight of each probability $p_{i,j}$. *Loss* is the same as Eq. (1.1). The probability $p_{i,j}$ is evaluated for a specific time interval. But the time intervals are different for different types of failures. For natural disasters, the average failure probability is approximately constant from one year to the next. Incidents with strong randomness such as human error and equipment aging, the failure probability can be counted according to the frequency of last year's occurrence. That is because the probability of occurrence of such events is different with the increase of years, and the frequency of occurrence of such events averaged over several years cannot be used as an approximation. For irregular events such as cyber-attacks, the failure probability can be estimated according to what degree the power system exposes to the internet. This kind of event is not random, but a small probability event. It depends on the deployment of the data center power system. From Eq. (1.2), we can find that the vulnerability of the power system includes both the lost loads and the probability of losing these loads. It can also be found that the reliability of electrical equipment consists of all types of fault events. The probability of each type of fault events $p_{i,j}$ is determined by the situation of the data center.

1.3. Problem description and the proposed solutions

Then how to analyze the vulnerability is the key point. First, we want to study how the failure spread (e.g., the power flowing along one path is “transferred” to another path as the topology changes), then detect the vulnerable spots (e.g., which fail may cause power crash), and compute the lost load as well as the vulnerability in the end.

We believe that the larger the loss of load caused by the failure of electrical devices, the weaker the electrical devices are in the IDC power system. If the exhaustive method is applied, assuming that an IDC power system has n devices, the time complexity of finding the maximum lost loads caused by k fault devices is $O(C_n^k)$. The problem falls into the $N-k$ problem [8]. For large data centers, this computational complexity is unacceptable. It is a NP-hard problem.

In contrast to general power systems, in order to ensure the uninterrupted and stable operation of information system, data centers widely utilize ATS, STS, MTS, loop switch, generators, UPS and other types of electrical devices with automatic switching or non-linear power conversion. These devices can automatically transfer loads to the backup route in a short time. The impact of different electrical equipment faults varies greatly. Considering the characteristics of the data center power system, a parallel fault evolution model PFEM and a vulnerable spots identification method AIVDCN are proposed in this paper.

The model PFEM is based on our previous work [9], and is based on a recursive process for modeling the process of failure spread. However, the previous model takes a long time to achieve the stable state that is mean that no new electrical devices come to be out-of-service. Therefore, in this article, we improve this model and propose a parallel fault evolution model for the IDC power network (PFEM). This algorithm has the following advantages:

It fully reflects the power system changes after the fault of IDC electrical equipment, including electrical devices failure, load transferring, overload tripping, non-linear load conversion and linear load superposition.

There is a parallel processing of new faults in the process of fault evolution. The parallel processing can shorten the time of reach the steady state of the power system.

The established algorithm for automatic identifying the vulnerability of the data center power network (AIVDCN) is based on the Actor-Critic [10] framework of reinforcement learning. The key points of AIVDCN are as follows:

characterizing the working state of the power system

constructing each action by the serial number of the fault equipment

constructing rewards by the quantitative representation of vulnerability

The advantage of AIVDCN is that it can automatically search for the weaknesses of the IDC power system without prior knowledge. The objective of AIVDCN is that it produces the devices whose failure would result in the greatest loss of load. In other words, strengthening the maintenance of the weak devices which are associated with vulnerabilities of the power system will reduce the probability of large loss of loads. By applying the algorithms on a real data center power network, the impact of vulnerable devices derived from AIVDCN after failure is about 5% higher than that of other algorithms.

The rest of this paper is organized as follows: Section 2 introduce the related works and contributions which involves the classification of blackouts and the methods to analyze the vulnerability of the power systems. In Section 3, we design a parallel fault evolution model for the IDC power network (PFEM). In Section 4, we propose an artificial intelligent algorithm AIVDCN to identify the vulnerable spots of the data center power network. In Section 5, we present the experimental results. Finally, conclusions are provided in Section 6.

2. Related works and contributions.

2.1. Events causing power outage

Since almost all the devices in the data center are powered by electricity, the impacts are tremendous when the power system outage [11]. There are mainly three categories of power system failures, which are natural disasters [12,13], random failures [14,15], intentional attacks [16,17,18,19,20]. Natural disasters, e.g. lightning, earthquakes, extremely cold or heat weather, often typically damage components of the power system, and the scope of influence can be enormous. The interruptions of power usually last for a long time, ranging from hours to days, resulting in heavy losses. Random failures, e.g. due to power system facility aging [15], incorrect removal of the power system components, human errors [14], usually make local damage of the power system. Intentional attacks, e.g. tripping transmission lines, sudden bursts of electromagnetic pulse [17], cyber attacks [19], target the critical elements of the power system. So the impact of blackouts may be significant. For example, attacking a selected set of nodes, edges, or paths in the power network may sabotage the power system [18]. As the supervisory control and data acquisition (SCADA) [21] systems are typically used in modern power system, it becomes possible for intentional attackers to remotely monitor power flows and make corresponding attack strategies to cause blackouts. Many strategies can be applied to achieve the malicious purpose. Cuffe compared eight

attack strategies in [16], which are standard genetic algorithm, method of minimized fitness function by link survivability [22], mixed integer linear programming method, random method, removing the most-heavily loaded K lines, electrical betweeness method, betweeness centrality method and topological metric of edge range method.

The problem of how to identify the vulnerable spots of such power system falls within a body of work on the identification of severe/critical multiple contingencies [23,24], also sometimes framed as a network interdiction problem, here applied to so-called cascading outages in a data center power system.

Multiple contingencies are the phenomenon that some failures occur simultaneously or in short succession. In the field of power grids, only a small number of facility outages (e.g., 3–5) can cause catastrophic blackouts. The problem of identifying the most vulnerable set of devices of the power system falls into the N-k combinatorial problem. The objective of the optimization is to find the minimum k nodes in N nodes, so as to maximize the lost loads.

2.2. Relevant models of cascading outages of power systems

Before solving the problem of identifying the most vulnerable set of devices of the power system, we mention that many models for the cascading outages has been studied [25,26]. Vaiman, et al. studied the cascading outages from the risk assessment perspective [25]. Junjian, et al. proposed a blackout model which considers the slow process at the beginning of the blackouts. The model has two layers of iteration, which are the inner iteration that reflect the fast dynamic process and the outer iteration that reflect the long-term slow dynamics [27]. Jun, et al. proposed a new metric that considers the voltage stability and the rotor angle stability principles of power grids into the power flow-based cascading failure simulators. Some authors applied quasi-steady-state power flow models [28,29] to describe cascading overloads, which does not reflect nonlinear mechanisms. And then Jiajia, et al. proposed a dynamic model that applies both protection systems and power networks [30].

2.3. Relevant methods of identifying the vulnerable spots of the power systems

Many methods have been considered to identify vulnerable spots in power systems. The methods of identifying the vulnerable spots of the power network focus on three classes, one is the power network topology perspective, the second is the operation parameters of electrical devices perspective and the last is based on the artificial intelligent method. Analytical method and Monte Carlo method have been applied in this problem, which mainly utilize the operating parameters of electrical devices. Methods that utilize the function representing the energy flow of the power system have been presented in article [31,32]. Some authors identified the vulnerable spots of power system by analyzing the reliability parameters of electrical devices [33,34]. Donde, et al. classified the problem as a $N-k$ problem [8] which can be cast as a mixed integer nonlinear programming (MINLP) problem. Then they solve the problem through a two stage analysis [23]. Pinar, et al. studied the problem in a static sense which examines the operating point of the power system. Then they also cast the problem as a bilevel MINLP problem. The optimality conditions of the Karush-Kuhn-Tucker (KKT) conditions, the power flow Jacobian, and the Mangasarian-Fromovitz constraint qualification (MFCQ) conditions were analyzed to solve the identifying the vulnerability of the power system [24]. Delgadillo, et al. proposed a method based on Benders decomposition [35]. López-Lezamaa, et al. proposed a new model which is based on the interaction of two agents. The first agent maximizes the load shedding by performing attacks, and the other minimizes the load shedding by modifying the generation dispatch [36].

Complex network theory has also been applied in solving this problem. For example Stubna studied the occurrence mechanism of power blackouts by HOT model [37], Koeunyi and JieChen studied the hidden failures in the power system respectively [38,39], Dobson applied Cascade model [40] and OPA model [41]. Some scholars researched the vulnerable spots of large-scale power grid based on the small-world topological method [42,43,44]. They found that nodes with high degree and betweenness make the power network well connected. And in the meantime, these nodes play a key role in the fault evolution process. Cuadra, et al. reviewed the use of complex network approaches for analysing the robustness of power grids [7]. Bompard, et al. reviewed literature from topology perspective [45]. Crucitti analyzed the topology of the Italian power system by applying the complex network method and neglecting electricity transmission details [46]. As the purely topological methods may lead to inaccurate results due to lack of peculiarities of the power networks, so some authors combine the complex network with power engineering concepts [47,48]. Through review of many kinds of approaches by using complex networks concepts, Lucas, et al. find that small-world networks seem to be the best topology [7].

With the improvement of the performance of artificial intelligence algorithms, more and more researches have been done to solve the problem of identifying the vulnerable spots in the power system by applying artificial intelligence, and many promising results have been achieved. There are also recent publications considering reinforcement learning methods in an optimization approach to identify critical contingencies [49,50]. Reinforcement learning [51] belongs to a category of semi-supervised learning algorithms, whose main components are state, action, reward. This algorithm updates the objective function Q by exploration and exploitation the best actions. Zhen, et al. [49] searched for the optimal sequential attack strategy by maintaining a Q table assigned to every state action pair (s_t, a_t). $\varepsilon-$ greedy policy strategy was applied to chose the best attack/action (line switching). The reward value was set to be $+1$ when the lost load target was reached. And the state s_t was set to be a vector of line status, the element value of which was set to be 1 when the corresponding line was out-of-service. On the contrary, it would be set to be 0 when the corresponding line was in-service. Other similar methods can refer to [52,53].

2.4. Contributions

On the vulnerability analysis of the power system, a lot of promising results have been achieved in the above literature.

The major contributions of this paper are as follows:

(1) We propose a parallel fault evolution model PFEM for data center power system in this paper. The basic framework of this model is the same as that of our previous work, which utilize graph theory to establish the relationship between devices in the power system as well as consider the changes of power flow when some faults occur. The innovation in this work lies in adopting parallelization techniques to accelerate computations.
(2) In this paper, an automatic algorithm of identifying the vulnerable spots of the data center power network (AIVDCN) is proposed, which adopts the basic framework of reinforcement learning, i.e. sequentially tripping some devices, observing the reward after failure, and updating the value function Q with the reward. However, considering the characteristics of large amount of electrical devices in the data center power network, we adopt the Gaussian Radial Basis Function (GRBF) to generalize the value function Q instead of maintaining a huge Q table. At the same time, according to the characteristics of the power system, a novel method for calculating parameters of GRBF is proposed.
(3) Unlike the previous reinforcement learning method, which get + 1 reward when blackouts happen in the power system (most of the time, the reward is 0), this paper uses the quantitative representation of vulnerability when some faults occur as a reward. The

proposed method can obtain positive reward immediately after each node is tripped, which can avoid no updating the parameters of the algorithm for a long time. Thus, the proposed method can accelerate the search speed of the most vulnerable set of devices of the power system.

(4) The other researchers' previous works which also based on the reinforcement learning algorithm used ε-greedy algorithm to select the equipment to be tripped, which select one equipment to be tripped equally and randomly from N-1 nodes by the probability of $1-\varepsilon$ where N is the total number of alternative equipment. Differ from this method, we adopt the Actor-Critic [26] method that updates the tripping probability of each electrical device while updating the value function Q. Thus, the tripping effect is increased.

3. PFEM: Parallel fault evolution model

When the electrical devices fail, they act independently (i.e. there is no direct relationship between the tripping of two switches). And then the fault changes the power system topology (the dual-input devices switch automatically), which affects the distribution of power loads (loads transfer with the action of automatic switching). Because of the large amount of computation, we adopt a parallel fault evolution method to shorten the time of computing the steady state of the power system when multiple devices failure.

3.1. Model of the IDC power network

In large-scale IDC power network, there are various power loads as well as various electrical devices. All kinds of electrical devices are connected by buses or cables to transmit electricity. The power can only be transmitted from the power sending-end (power grid) to the receiving-end (load).

Therefore, the topology of large-scale IDC power network can be modelled as a directed graph $G = (V, E)$. V is the node set which is abstracted from electrical devices including transformers, switchgears, circuit breakers, ATSs, MTSs, STSs, UPSs and so on. And $E = V \times V$ is the directed edge set which is abstracted from transmission cables and power buses. $e = (x, y)$ in set E is an electrical line connecting two devices x and y.

In IDC power system, there are four main connection relationships between nodes and edges: single input and single output, single input and multiple output, two input and single output, two input and multiple output, corresponding to circuit breaker, ATS, STS, etc. The typical structures of nodes with edges like the following relationship between node d and its edges are shown in the following Fig. 2.

Unlike the power transmission network, the data center power distribution network has a tree structure. A device receives only one power input, that is, a node only has a single input. Only when the power supply at the upper end of this node fails, it can automatically switch to another power input. The connection relationship between nodes in the operation of the power distribution system is as the following Fig. 3: the red solid edge is the input power supply of node d, the green solid edges are the outputs of node d, and the black dotted edge is the standby power supply of node d. The standby edge works only when the edge e loses power. In this work, we define the power source device as "front-end" which likes "u1" and "u2" in Fig. 3, and we define the power receiving device as "back-end" which likes "d" in Fig. 3.

3.2. Characteristics of the IDC power network.

(1) In contrast to information networks, electrical devices can not automatically restore after overload tripping, that is to say, the equipment connected to these devices will be power-down after the failure of these devices. From the view of graph, the edges of the back end of the fault nodes disappear from the graph.

(2) In contrast to the traditional power system, the IDC power network applies lots of automatic switching electrical devices such as loop switch, ATS, MTS and STS by the reason of redundancy and mutual standby. When the power supply of one front-end of this kind of equipment loses power, the power load will automatically switch to the other power supply. At the same time, the power loading of all the devices in the backup supply path increases, which increases the probability of overload tripping of other devices [54,55].

3.3. Changes of the power system when faults occur

When the electrical equipment (u) fails by itself or trips because of overload, if the back-end equipment is a single-input device, then the back-end equipment directly loses power. For example, if node u fails in Fig. 4, node d in the back-end of this fault equipment loses power.

The ATS and STS can be modeled as node d in Fig. 5. If the electrical equipment ($u1$) fails and its back-end equipment is ATS or STS, such as node d in Fig. 5, then the power supply source of $u1$ is automatically switched from $u1$ to $u2$. In the meantime, all the power load of d is transferred to (…$u2$, d…) route. After the load is transferred, if any electrical equipment is overloaded at the upper end of d in (…$u2$, d…) route will lead to a power failure of d. Then the electrical loads linked to d are powered off. At this time, the operation status of equipment d is shown in Fig. 6.

For convenience, we define the symbols and its definitions in Table 1.

In the case of load transferring, according to the superposition theorem [56], the load current of each linear node is added linearly. The following equations should be satisfied when the node d works normally:

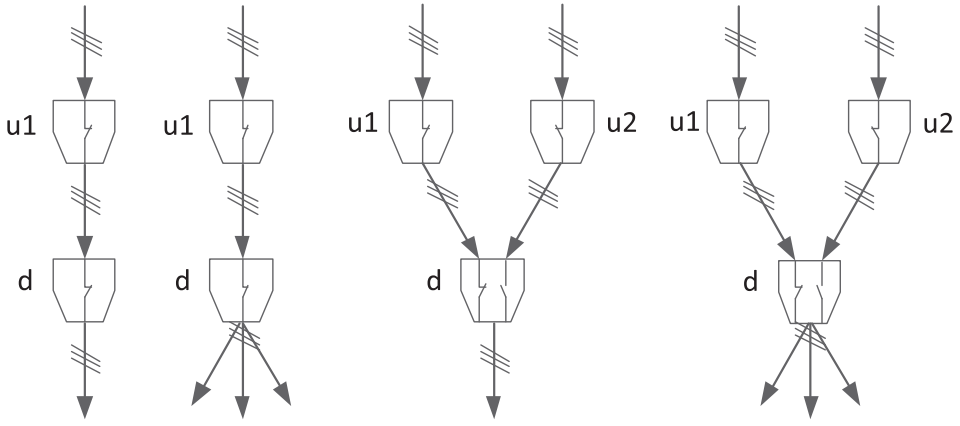


Fig. 2. Typical structure of nodes with its edges.

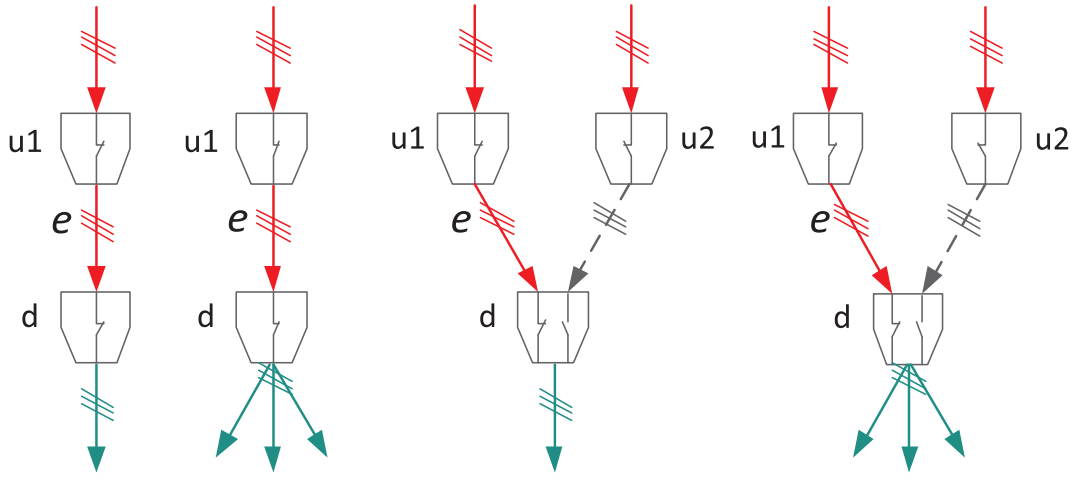


Fig. 3. Connection of adjacent nodes in normal power networks.

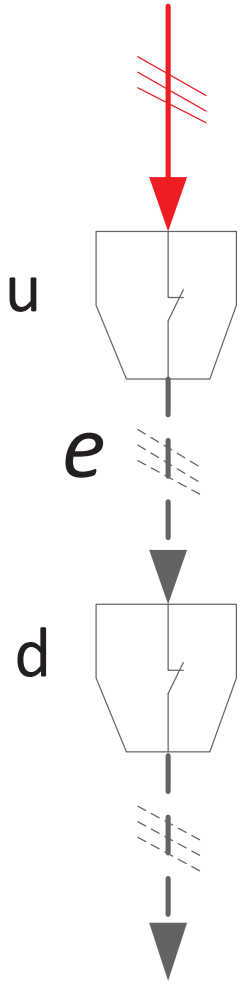


Fig. 4. Power loss of single input and output node.

$$I_d > \sqrt{\left(\sum_{j=1}^{N_d} i_j^a cos\theta_{d,a}\right)^2 + \left(\sum_{j=1}^{N_d} i_j^a sin\theta_{d,a}\right)^2}$$

$$I_d > \sqrt{\left(\sum_{j=1}^{N_d} i_j^b cos\theta_{d,b}\right)^2 + \left(\sum_{j=1}^{N_d} i_j^b sin\theta_{d,b}\right)^2} \quad (3.1)$$

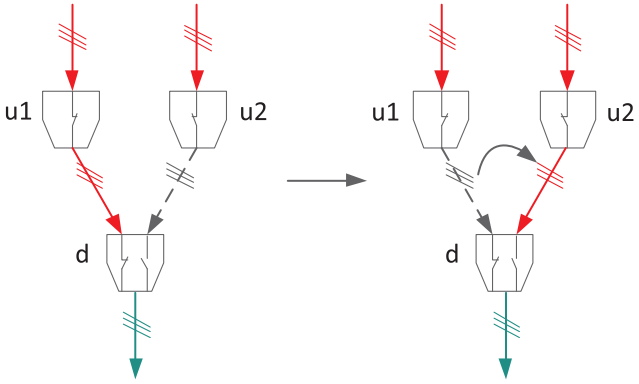


Fig. 5. Load of A is transferred from $u1$ to $u2$.

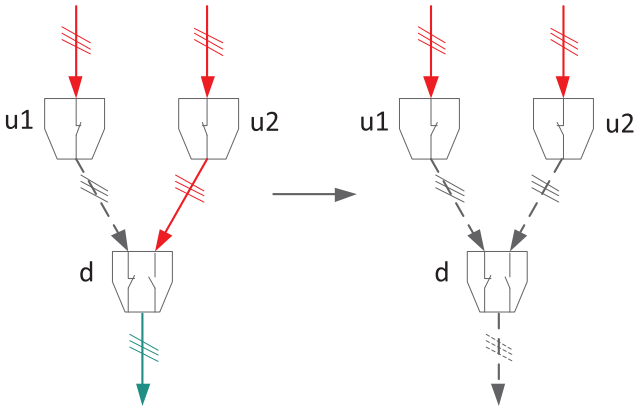


Fig. 6. Node $u2$ is tripped in the reason of overload.

$$I_d > \sqrt{\left(\sum_{j=1}^{N_d} i_j^c cos\theta_{d,c}\right)^2 + \left(\sum_{j=1}^{N_d} i_j^c sin\theta_{d,c}\right)^2}$$

Uninterruptable power supply (UPS) devices are widely used in the data center power system. They have two main uses, one is to filter out the abnormal situation of the power grid, such as surge, spike, abnormal frequency and so on, and the other is to switch to battery power supply instantaneously when power failure or electrical equipment failure occurs to ensure the stable operation of IT loads in a short time. The main components of UPS are rectifier, inverter and filter. Because the power factor correction circuit is used in uninterruptable power supply (UPS) devices, the input current's vector value of an UPS should

Table 1
Symbols and definitions.

Symbol	Definition	Symbol	Definition
I_d	Tripping current of node d.	$\dot{I}_u$	Vector of output current of UPS_u.
i_j^a	Working current of phase a of load j.	$\dot{L}_j$	Vector of working current of load j.
i_j^b	Working current of phase b of load j.	L_j	Apparent value of working current of load$j$
i_j^c	Working current of phase c of load j.	η_u	Working efficiency of $UPSu$.
N_d	The number of nodes connected to node$d$	N_u	The number of nodes connected to $UPSu$.
θ_x	Power-factor angle of load$x$.		Vector of input current ofUPS_u.
$\theta_{d,a}$	Power-factor angle of phase a of node$d$	$\theta_{d,b}$	Power-factor angle of phase b of node$d$.
$\theta_{d,c}$	Power-factor angle of phase c of node$d$		

not be simply and linearly superimposed, it should be calculated as Eq. (3.2). When modelling the UPSs in the grid topology, there is little difference with other electrical devices, but one should pay attention to the current calculation method.

$$\dot{I}_u^{in} = \frac{\sum_{x=1}^{N_u} L_x cos\theta_x}{\eta_u cos\theta_u} \tag{3.2}$$

3.4. Proposed model ***PFEM***

In this paper we propose a new model, namely, PFEM (a parallel fault evolution model for the data center power network), which tries to incorporate all the above characteristics of the IDC power network. Consequently, we would like to capture the following properties:

1) The topology of the IDC power network is a tree when working normally.
2) If several nodes fail at almost the same time, their parallel actions are executed sequentially according to the occurrence order of the faults, and the time interval between the parallel processes is very short. The processes will change the shared topology of the power system.
3) When a node fails, the back-end cables lose power. From the graph G view, the edges between the node and its child nodes disappear.
4) If the fault node is one of the inputs of the dual-power equipment, the power source of the dual-power equipment is automatically switched to the standby route. The load is transferred at the same time.
5) After the load transfer, if the nodes with superimposed power load exceed there rated value, they trip immediately. And the tripping nodes are incorporated into the new fault nodes.
6) The new fault nodes follow the same fault evolution process, that is, the IDC power fault process is a recursive process.

The framework of PFEM is shown in Fig. 7.

The input of this model is a set that consists of the serial number of sequential faulted nodes, and the outputs are the stable topology and the lost loads of the IDC power network. The algorithm is described in detail as follows:

(1) The initial stable topology of the IDC power network is T, and the input $T_r = \{v_1, v_2, \cdots, v_{nn}\}$ is a ordered set which consists of the initial fault nodes. The node in the front will be tripped earlier.
(2) Open nn processes that correspond to nn fault nodes, which share the working power network's topology T. Each process removes the connection edges from the fault node to its back end nodes. The process of dealing with the front fault node starts earlier, and the time interval between the parallel processes is very short.
(3) nn processes make use of depth-first search (DFS) algorithm to compute the set $\{s_1, s_2, \cdots, s_{nn}\}$ that consist nodes directly connected to the back end of the fault nodes.
(4) Calculate the parent nodes for each node in the affected child nodes' set s_m in process m in the IDC power network graph G. And then, enable the edge from normal parent node t to node i which belongs to s_m.
(5) When all processes are finished, the initial set of new fault nodes is set to $T_r^{'} \leftarrow \varnothing$, the edges connected to the nodes in T_r are removed within the power system's operation topology, and the working topology is transferred from T to $T^{'}$.
(6) Calculate the shortest path for every load $l_i \in L$ from power grid to load l_i in $T^{'}$.
(7) And then calculate the input current of UPS u by applying Eq. (3.2).
(8) With regard to the load of the middle nodes between source nodes and UPSs in the shortest path of load l_i, it should be superimposed by the input of UPS ($\dot{I}_u^{in}$). And the load of the other middle nodes between UPS and load l_i can be superimposed by the load of l_i.
(9) Inspect the working load of all the middle nodes in graph $T^{'}$, and judge whether it satisfies the Eq. (3.1). If any one of the middle nodes does not satisfy the Eq. (3.1), put it at the end of the new sequential fault nodes' set $T_r^{'}$. Then the working topology of the IDC power network is turned into $T^{''}$.
(10) If there are new fault nodes, go back to step 2) with the sequential fault nodes' set $T_r^{'}$. Else the IDC power network works in stable state T_π. Easily the lost loads' set (LL) can be derived by DFS whose route from the power source is empty.

The proposed parallel model is based on our previous model DCNFEM [9]. Parallelization reduces the computation time approximately by a factor equal to the number of parallel processes.

4. AIVDCN: an automatic algorithm of identifying the vulnerable spots of the data center power networks

In this work, the power system's fault process is approximated to having the Markov property. A reinforcement learning task is called Markov decision process (MDP) if it satisfies Markov property. A MDP is process of making sequential decisions of actions to carry out, where actions influence not just immediate rewards, but also subsequent states, and through those future rewards. Thus, MDP involve delayed reward and there is need to tradeoff delayed and immediate reward.

There are four properties in the MDP, which is defined as $<S, A, P, R>$. S is the space of the state of the environment that is the power system in this work. A is the action space, which involves all the possible alternative actions. R is the reward function, which is the feedback of the environment. $r_s = \mathbb{E}(r_{t+1}|s_t = s)$ is the expectation of reward under state s. P is the state transition probability matrix, which characterize the dynamics of a MDP.$p_{ss^{'}} = \mathbb{P}(s_{t+1} = s^{'}|s_t = s)$ represents the probability of the power system transferring from one working state s to another one $s^{'}$. The agent that selects actions and the environment interact at each of a sequence of time step $t = 0, 1, 2, \cdots\cdots$ that is the time passed from the time of the failure of an electrical device.

At each time step t, the agent receives the state $s_t \in S$, and selects one action $a_t \in A$ on that basis, then agent receives a new state s_{t+1} and a numerical reward $r_t \in R$. r_t is the reward from the environment at time t. The agent and MDP together give rise to a trajectory which likes this:

$$s_0, a_0, r_1, s_1, a_1, r_2, s_2, a_2, r_3, \cdots \tag{4.1}$$

As the topology of the power system is clear to the maintenance

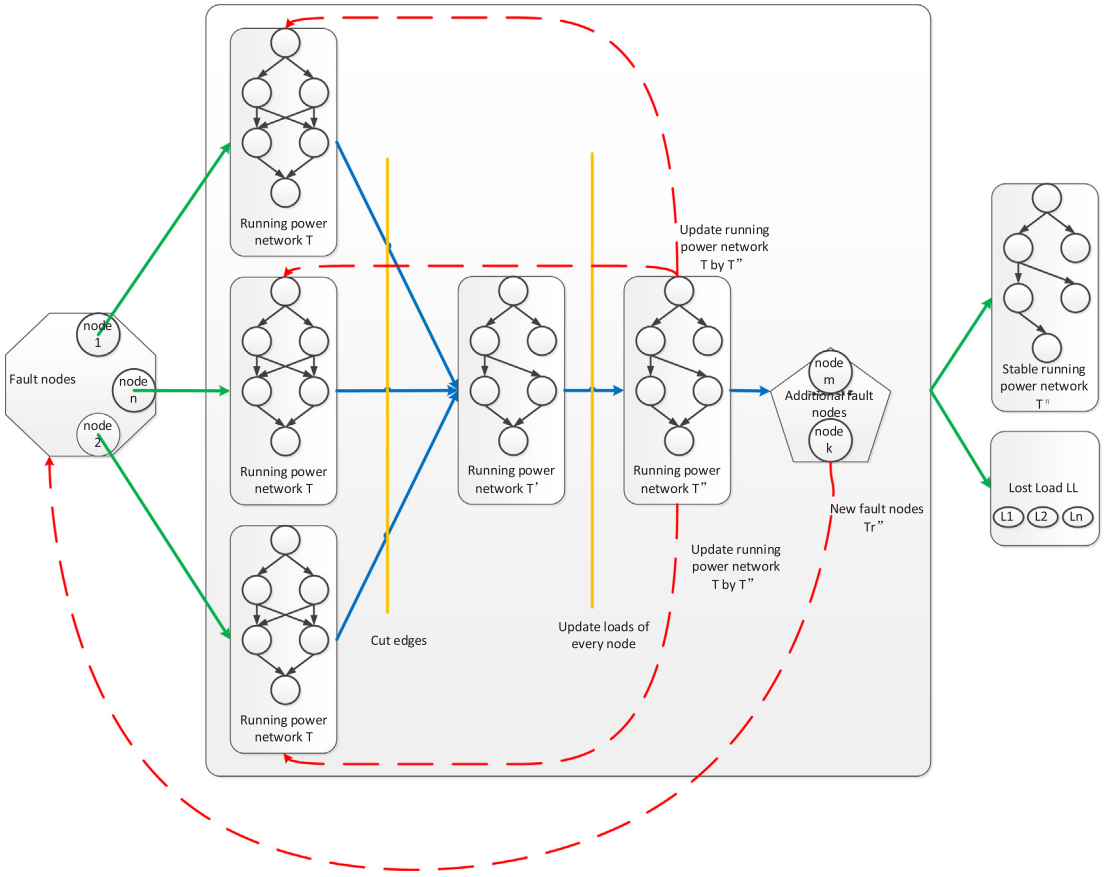


Fig. 7. Framework of PFEM.

staff, and it is sufficient information to define the state of the power system, we utilize the adjacency matrix of the power system's graph G to define the state s, where:

$$s_t(i,j) = \begin{cases} 1, & \text{if node } i \text{ is in} \\ & -\text{service and there is one edge from } i \text{ to } j, \\ & \text{so node } j \text{ can get power from node } i \\ & \text{at time } t \\ 0, & \text{if node } i \text{ is out} - \text{of} \\ & -\text{service or there is no edge from } i \text{ to } j, \\ & \text{so node } j \text{ cannot get power from node } i \\ & \text{at time } t \end{cases} \tag{4.2}$$

The state space S is the set of all possible states $s(i,j)$, where $i,j \in [0, 1, \ldots, n]$. n is the max serial number of all electrical nodes. A simple example of $s_t(i,j)$ is shown in Fig. 8.

An action is defined as the serial number σ of the selected power network node. The action $a(\sigma)$ will be sent to the PFEM model where the edges connected to node σ will be removed. That is to say the child nodes cannot get power from the fault node σ. The action space $A = [0, 1, \ldots, n]$ is the set of all possible actions $a(\sigma)$, where $\sigma \in A$. A simple example of action $a(0)$ is as Fig. 9.

Under state s of a power system, if an electrical device fail (action $a(\sigma)$, which the edges connected to would be tripped) because of some reasons. The probability of next possible power system state s' is $p_{ss'}^{\sigma} = \mathbb{P}(s_{t+1} = s' | s_t = s, a_t = \sigma)$. The expected value of lost loads is $r_{ss'}^{\sigma} = \mathbb{E}(r_{t+1} | s_t = s, s_{t+1} = s', a_t = \sigma)$. The policy adopted in selecting action $a(\sigma)$ is recorded as π, $\pi(\sigma|s) = \mathbb{P}(a_t = \sigma | s_t = s)$. During learning,

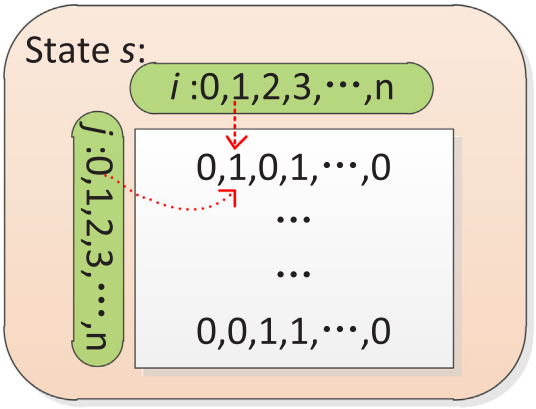


Fig. 8. A simple example of $s_t(i,j)$. $s_t(1,0) = 1$ denotes that the edge from node 0 to node 1 is in-service.

it is necessary to estimate how well the policy π performs. This estimation is called policy evaluation, the result of which is called the value function. We utilize the state-action value function $Q^{\pi}(s,\sigma)$, which obeys the Bellman equations [10] in the form of Eq. (4.3). In the equation, $\gamma \in (0, 1)$ is a discount factor, the extent to which the algorithm considers the long-term rewards.

$$\begin{aligned} Q^{\pi}(s,\sigma) &= \mathbb{E}_{\pi}(r_t | s_t = s, a_t = \sigma) \\ &= \mathbb{E}_{\pi}\left(\sum_{k=0}^{\infty} \gamma^k r_{t+k+1} | s_t = s, a_t = \sigma \right) \end{aligned} \tag{4.3}$$

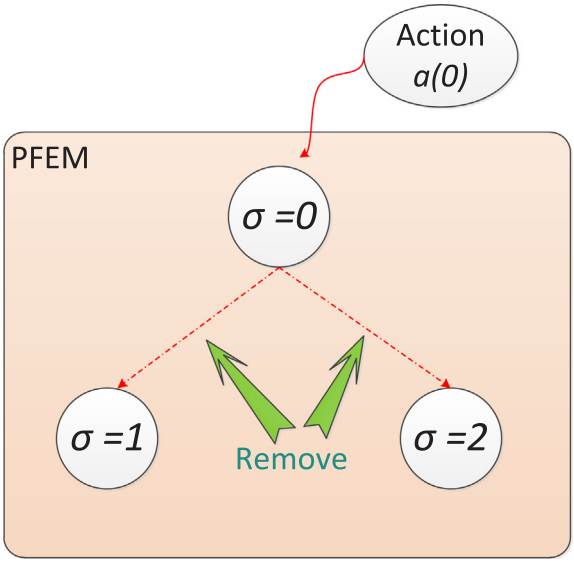


Fig. 9. A simple example of action $a(0)$. $a(0)$ denotes that node 0 is selected to be tripped. The edges from node 0 to node 1 and node 2 will be removed in the power system topology.

$$= \sum_{\sigma} \pi(s, \sigma) \sum_{s'} P_{ss'}^{\sigma} \left[r_{ss'}^{\sigma} + \gamma \sum_{\sigma' \in A} \pi(\sigma' | s') Q_{\pi}(s', \sigma') \right]$$

$$= r_{s}^{\sigma} + \gamma \sum_{s' \in S} P_{ss'}^{\sigma} \sum_{\sigma' \in A} \pi(\sigma' | s') Q_{\pi}(s', \sigma')$$

Because the value of Q^{π} is relevant to the policy π, we can solve maximum $Q_{*}(s, \sigma) = max_{\pi} Q^{\pi}(s, \sigma)$ to find out which electrical devices that will cause the largest loss of load when they fail.

There are many methods to solve the above problem by reinforcement learning [57], for example, Dynamic programming, Monte Carlo method, Temporal-Difference Learning, and so on. They fall into three categories that are critic-only, actor-only, or actor-critic algorithms. As the complexity of the data center power network is considered, the actor-critic method is selected in this work, in which the policy gradients have lower variance [10]. The actor-critic method has two independent components which are "actor" component that learns policies to select action and "critic" component that criticizes the performance of the actor's choices. The reward r_t at time t from the environment is sent to the value function Q, and then the temporal-difference error (TD error) is derived which can be represented by $\delta_t = r_t + \gamma Q_{t+1}(s_{t+1}, \sigma_{t+1}) - Q_t(s_t, \sigma_t)$. The Q value function in critic and the policy π in actor can be updated by TD error simultaneously. The next action can be chosen by the updated policy, which will be sent the environment to perform some work that represents tripping the corresponding electrical device in this work, and then the next state of the environment can be observed which will be sent into Q value function and policy π simultaneously. The above process is executed iteratively until the predetermined number of iterations is reached. The typical framework of an actor-critic method is illustrated in Fig. 10.

We propose an automatic algorithm to identify the vulnerable spots of the internet data center power network (AIVDCN) based on the Actor-Critic framework. We utilize the Gaussian Radial Basis Function (GRBF) [58] to construct the eigenvector of the power system's working state, use the softmax [59] method to select actions and propose a novel method for calculating parameters of GRBF. This algorithm sequentially trips the alternative electrical devices one by one. And the reward refers to the quantitative representation of vulnerability (Eq.1.2) caused by the tripped device is used to update the Q value and the selection policy π. Some key components of our AIVDCN algorithm are as follows.

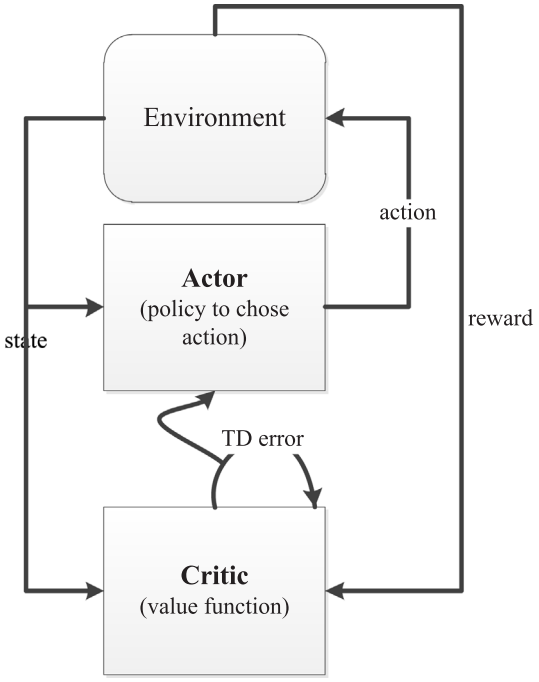


Fig. 10. The typical framework of an actor-critic method.

4.1. Q value design

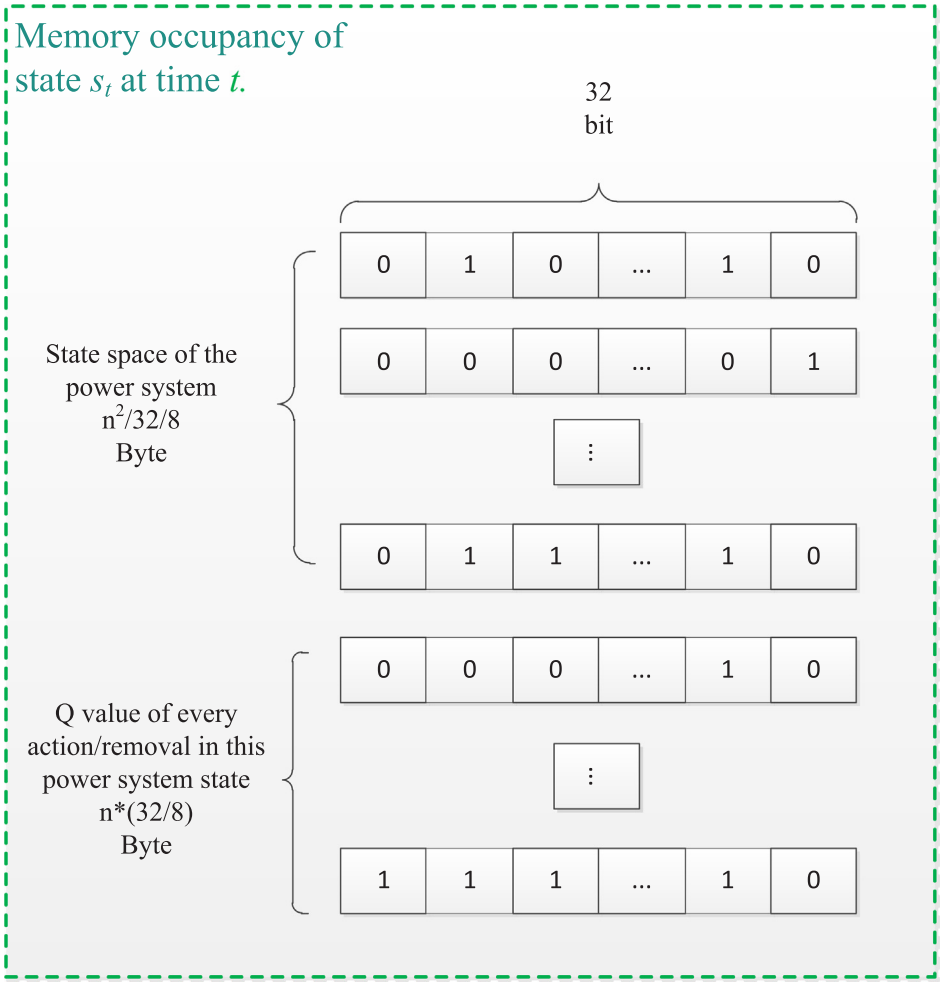
We define the number of electrical devices in the power system is n and the number of sequential fault devices is k. Then the dimension of state space S is n^2 and that of action space A is n. If exhaustive method is used, the time complexity of finding the maximum lost loads caused by k devices fault is $O(C_n^k)$. The search space of $Q_{*}(s, \sigma)$ is n^3. If the method of using a Q table that consists of the state-action pair\;(s, σ) is applied to store and update Q value for large-scale data center power systems, the computational complexity and memory occupancy are unacceptable. Generally, the value function $Q(s, \sigma)$ is a big table stored in the computer memory, a typical storage form is illustrated in Fig. 11.

This Q table is dived into two segments. The first half represents the working state of the power system, and each bit represents the working situation of two corresponding electrical devices. 1 represents the power supply relationship between the two corresponding nodes, and 0 represents the connectionless relationship. The second half stores the Q value of each action/tripping under this state s_t, and each Q value is stored by 32-bit memory. Assuming that the number of states corresponding to s_t stored in memory after $\mathcal{N}$ iterations is $\mathcal{K}$ ($\mathcal{K} \leqslant 2^{n^2}$) bit, the memory occupied by this Q table is $\mathcal{K}^2/32/8 + \mathcal{K}*(32/8)$ Byte. The simulation environment in this paper has 594 nodes. Assume that Q value is stored by this table. $\mathcal{K}$ is assumed to be 10^4 bit after $2 * 10^4$ iterations, which is much smaller than 2^{594^2} bit. Thus, the memory occupancy of this table is 35.8G Byte. Obviously, the memory occupied by this Q table is unacceptable, and the searching time for the best action in this table is also unacceptable.

Therefore, we apply the generalized method to approximate the state-action value function $Q(s, \sigma)$, and update the value function by gradient descent method. We define the Q value of t step in the linear representation as follows:

$$Q_t(s, \sigma; \theta) = \vec{\theta}_t^{\,T} \vec{\varnothing}_s \tag{4.4}$$

where $\vec{\varnothing}_s$ is the eigenvector of working state s of the power system, and the parameters $\vec{\theta}_t^{\,T}$ has the same number of components as $\vec{\varnothing}_s$. Because the dimension of the power system state s is very large, it is difficult to construct the eigenvector by ordinary linear coding method. So, we use GRBF to construct the eigenvector. The function is as follows:



$$\Psi(s-u) = e^{-\frac{||s-u||^2}{2\rho^2}} \tag{4.5}$$

There are two hyper parameters in GRBF. One is the center u, which is the mean value of Gaussian function, and the other is the width ρ. As the state of the power system is very large, in order to cover as more features of the state s as possible but limit the complexity, we introduce GA GRBFs and of which all the centers are set to be 0 of n dimensions. $GA = n/100$, where n is the dimension of the state s and GA is derived by rounding down. The last hyper parameter is the width ρ, which is important in calculating the eigenvector of working state s. And the innovation of this part is that we design a method to compute the width $\rho_g (g \in [0, 1, ..., GA-1])$.

From the Fig. 12 of a simple example of one-dimensional GRBF, we can see that proper width of GRBF should cover the largest state s whose elements are 1 except diagonal ones. Otherwise, the generalized value function Q_t cannot represent the states correctly. For example, if the largest state s locates at the dash line, the GRBFs whose widths are 1 and 0.5 cannot capture the features of the state s. We introduce the method of calculating the width ρ_g as follows:

$$\rho_g = \frac{GA}{2^g} * \frac{||s_{max} - u||_2}{\sqrt{2n}} = \frac{GA}{2^g} * \frac{\sqrt{n-1}}{\sqrt{2n}}, \quad g \in [0, 1, ..., GA-1] \tag{4.6}$$

where we can see that the nominator is related to the distance between the largest state and the center u, the denominator is related to the dimension of the states. On the left side of the fraction is a geometric series, which is related to the amount of GRBFs. The left side of the fraction is used to balance the distribution of eigenvectors.

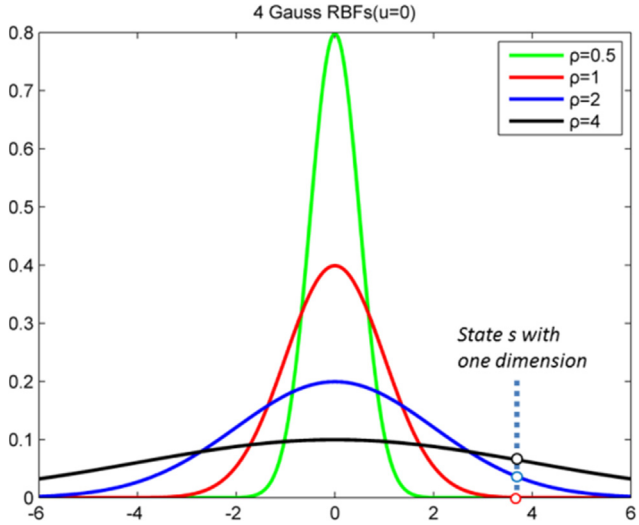


Fig. 12. A simple example of one-dimensional GRBF. The dash line indicates the position of state s with 1 dimension.

We define the process of obtaining all the eigenvectors of the state s as building process, which involves three steps. First calculate the center u_g and width ρ_g of each GRBF, second disassemble each GRBF into multiple eigenvectors by Taylor series [60], in the end combine all the features of every GRBF. Details are as follows:

(1) Set the center u_g of each GRBF to be 0 with n dimensions. The width ρ_g can be calculated by Eq. (4.6).
(2) Mapping the current state s to eigenvectors by each GRBF. In order to reduce the computational complexity, we take the first $w = 100$ eigenvectors. The decomposition process is as follows:

$$\begin{aligned}&\Psi_g(||s-u_g||)\\&=\exp(-\frac{||s-u_g||^2}{2\rho_g^2})\\&\approx\sum_{j=0}^{w}\frac{(s^Tu)^j}{j!\rho_g^{2j}}\exp\left(-\frac{1}{2\rho_g^2}||s||_2^2\right)\exp\left(-\frac{1}{2\rho_g^2}||u||_2^2\right)\\&=\sum_{j=0}^{w}\varnothing_g(j)\end{aligned}\tag{4.7}$$

(3) Combine all the eigenvectors $\varnothing_g$ one by one.

$$\varnothing_s=[\varnothing_g(j)]\ ;for\ all\ g\in GA, j\in[0,1,...,w]\tag{4.8}$$

Where, the eigenvector $\varnothing_s$ capture the features of the state s and $\varnothing_g(j)$ are the elements of the eigenvector $\varnothing_s$.

The weight vector of eigenvector in Eq. (4.4) is updated by gradient descent method. The parameter α is the learning rate.

$$\overrightarrow{\theta}_{t+1}^T=\overrightarrow{\theta}_t^T+\alpha[r_t+\gamma Q_{t+1}(s_{t+1},\sigma_{t+1})-Q_t(s_t,\sigma_t)]\nabla_{\overrightarrow{\theta}_t}Q_t(s_t,\sigma_t)\tag{4.9}$$

4.2. Action policy design

In order to converge as soon as possible and avoid falling into endless exploration, the selection policy π adopts the softmax method [59]:

$$\pi_t(s,\sigma)=\frac{e^{\mathbb{P}(s,\sigma)}}{\sum_b e^{\mathbb{P}(s,b)}}\tag{4.10}$$

Where the probability $\mathbb{P}(s,\sigma)$ of selecting an action $a(\sigma)$ (only one electrical device is selected in each action iteration) under the state s also adopts the generalized method. Its state eigenvector is the same as that of $Q_t(s,\sigma)$, which is $\overrightarrow{\varnothing}_s$. The updating method of the corresponding weight vector is the same as Eq. (4.9), which is shown in Eq. (4.12).

$$\mathbb{P}(s,\sigma;\vartheta)=\vartheta_t^T\overrightarrow{(\sigma)}\,\overrightarrow{\varnothing}_s\tag{4.11}$$

$$\vartheta_{t+1}^T\overrightarrow{(\sigma)}=\vartheta_t^T\overrightarrow{(\sigma)}+\alpha[r_t+\gamma Q_{t+1}(s_{t+1},\sigma_{t+1})-Q_t(s_t,\sigma_t)]\nabla_{\vartheta_t^T\overrightarrow{(\sigma)}}Q_t(s_t,\sigma_t)\tag{4.12}$$

4.3. Reward design

Unlike the previous methods, which get +1 reward when blackouts happen in the power system (most of the time, the reward is 0), this paper uses the quantitative representation of vulnerability when some faults occur as a reward. The proposed method can obtain positive reward immediately after each node is tripped, which can avoid no updating the parameters of the algorithm for a long time. Thus, the proposed method can accelerate the search speed of the optimal solution. This paper proposes the following reward function:

$$r_t(s_t,\sigma_t)=Vul(tr)\tag{4.13}$$

s.t. $tr=[\sigma_0,\ \sigma_1,\ ...,\sigma_t]$

Where Vul is given by Eq. (1.2).

4.4. Details of the whole AIVDCN algorithm

The framework of AIVDCN is illustrated in Fig. 13:

The detail of AIVDCN is as follows:

Step1. Model the IDC power system by weighted digraph $G=(V,E)$.
Step2. The operation state T of the IDC power system is represented by the adjacency matrix s of the modeled graph G in step 1, and the eigenvector of state s is calculated according to Eq. (4.8).
Step3. All the initiated values of parameter θ of the value function Q, parameter ϑ of policy π, number of starting fault devices x, number of starting iteration *episode*, and vulnerable nodes' vector *VUL* are set to be zero. The dimension of the vector *VUL* is set to be 10 in this work which is long enough.
Step4. Initialize the initial normal working state of the IDC power system to be s, whose situation is that no equipment or power load fails.
Step5. Select an electrical device (only one electrical device) to make it trip in all the alternative devices under the current state s. The selection method is as follows: in all the value functions $Q(s,\sigma;\theta)$ of state s, the policy $\pi(s,\sigma;\theta)$ is used to select action σ that will be tripped next and its corresponding Q value.
Step6. Execute the above action σ, i.e., transfer current IDC power system topology and the selected action σ to the above PFEM algorithm in this paper.
Step7. By observing the topological structure of the temporary stable power network at this time, the next working state T' and the corresponding adjacency matrix s' of the power network are obtained.
Step8. Based on depth-first search (DFS), the reward r under s' is calculated easily.
Step9. Select another electrical device σ' under the current state s', the selection method is the same as step5.
Step10. Update the parameters of the value function Q and the policy π by Eq. (4.10) and Eq. (4.12).
Step11. Add one to the number of devices that have been tripped, that is $x=x+1$. If $x<10$, execute step 12, else judge *episode*. If *episode* is smaller than the maximum number N, add one to it, and then go to step 4. Else if *episode* is equal to N, go to step 13.
Step12. Set s' to be s, and return to step 6.
Step13. Output the vulnerable nodes' sequence: Execute *episode* once again from step5, but the selecting policy of action σ is set to be $argmaxQ(s,\sigma;\theta)$ in each step x, and put it in the x-position of *VUL*.
Step14. For any k elements in *VUL* that is the set of vulnerable nodes, there are C_{10}^k combinations. All the sequential combinations are put into the PFEM algorithm independently, and then the combination which makes the largest quantitative representation of vulnerability is the most vulnerable k devices in the IDC power system.

The flow chart of this algorithm is shown in Fig. 14:

5. Experiments and discussion

In this paper, Networkx [61] which is a tool for complex network is applied to model and simulate a real IDC power network. This IDC power network consists of 719 edges, 594 nodes and 205 power loads. The modeled graph G of this IDC power network is shown in Fig. 15.

The probability of each type of fault events $p_{i,j}$ (in Eq. (1.2)) is determined by the situation of the data center. For example the probability of human errors is higher in a new data center, the probability of equipment aging is higher in a data center that has operated for more than 5 years, the probability of lightning strikes is higher in a data center that is located in the tropics, the probability of cyber-attack is higher in a data center that utilize the public wireless network for data transmission and downloading control instructions. The corresponding weights are determined by the data center infrastructure maintenance staff according to the possibility of each type of events, which can be

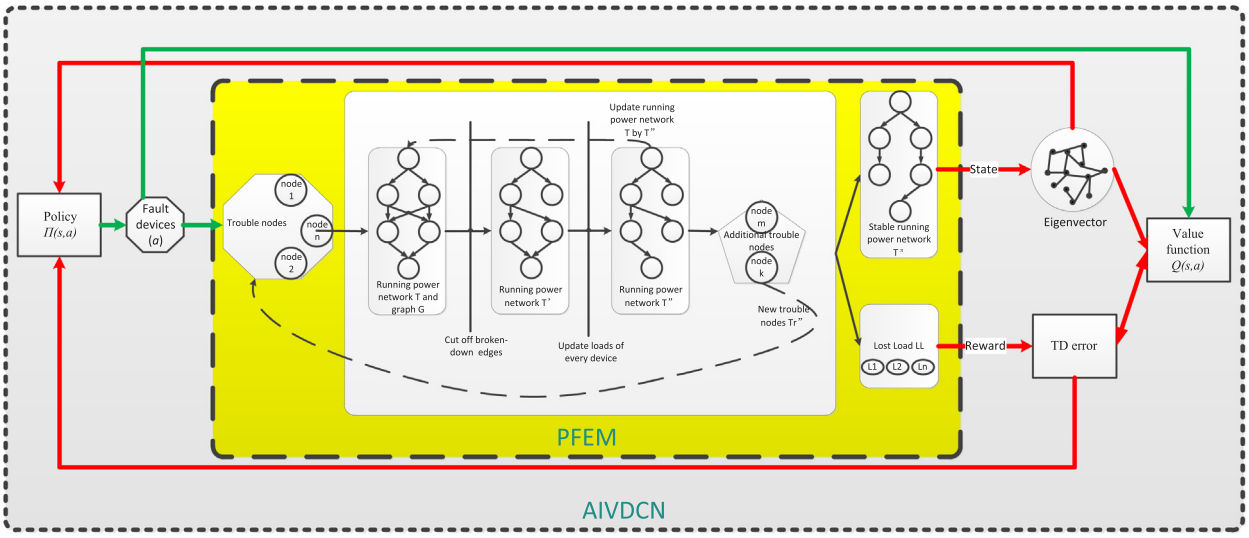


Fig. 13. The framework of AIVDCN.

determined by fuzzy theory, experience or other methods. The experimental case in this paper is located in Beijing, China, where the climate is relatively stable, natural disasters are rare, and power grid is relatively stable. At the same time, the data center has been put into operation for 5 years, and the condition of electrical equipment is relatively stable. So, the probability and weight of equipment failure caused by natural disasters, human errors, etc. are lower. However, due to the use of a large number of intelligent devices with network communication, the probability of cyber-attacks is higher, but the maintenance staff attaches great importance to network security, so the weight of this fault is low. Because of the good condition of electrical equipment, the probability of failure caused by equipment aging is low, but because of the large quantities, it is more likely to occur than other types of failure, so the corresponding weight is larger. According to experience,

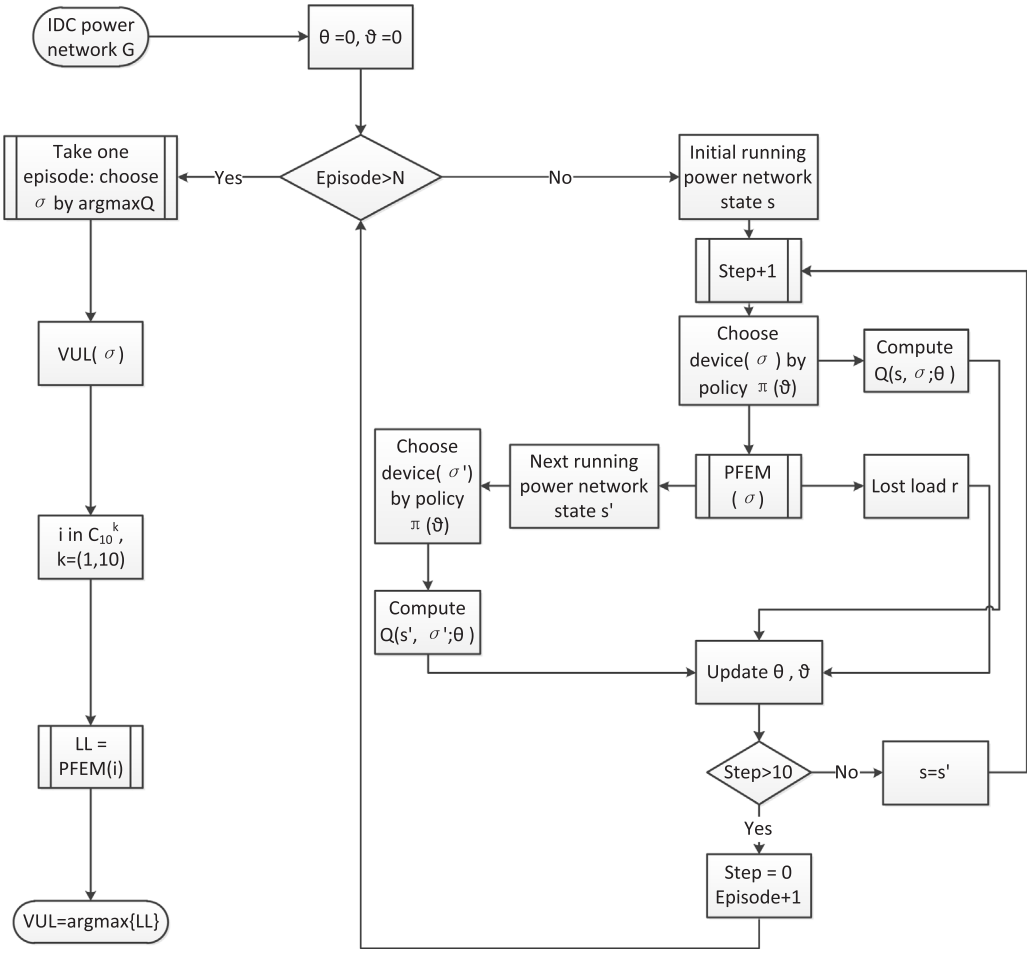


Fig. 14. Flow chart of AIVDCN algorithm.

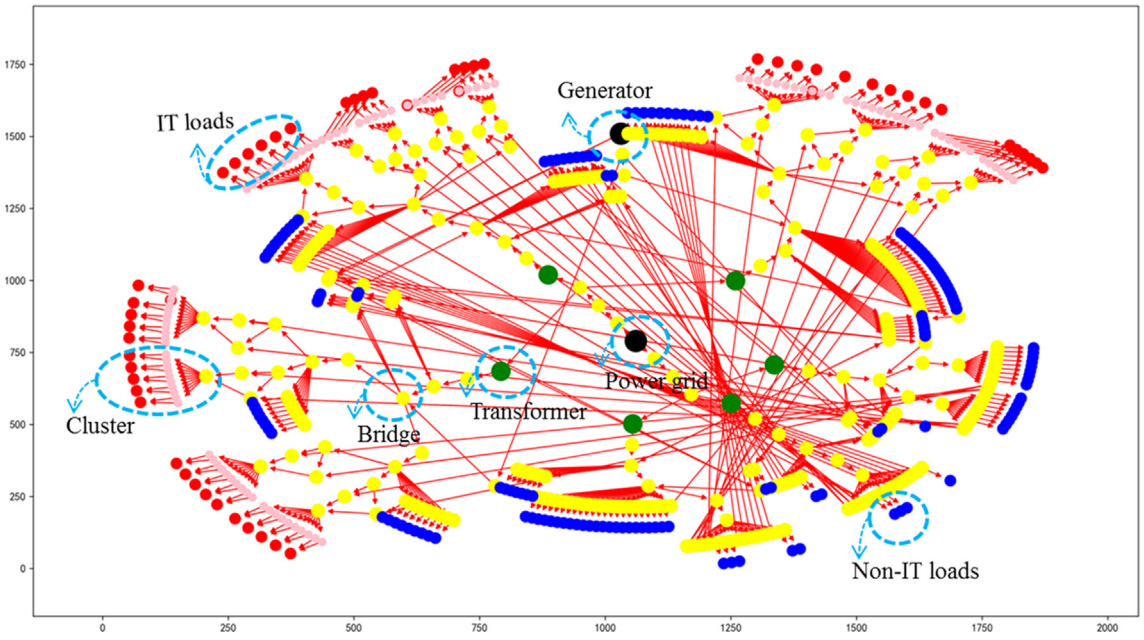


Fig. 15. The modeled graph G of a real data center power network. This graph has the following characteristics: (1) it is a directed graph pointing from the power supply node to the power receiving node; (2) a few nodes connect a large number of other nodes; (3) some nodes act as bridges for energy flow although they are less connected with other nodes; (4) the same load has multiple power supply routes; (5) some nodes are clustered together, which connect with other nodes through some key nodes. In this figure, the green nodes are transformers, the yellow nodes are switchgears, the blue nodes are non-information loads, and the red nodes are IT loads. (For interpretation of the references to colour in this figure legend, the reader is referred to the web version of this article.)

Table 2
Fault probability and the corresponding weight of various types of electrical equipment.

Electrical Equipment	Disaster		Cyber-attack		Human Error		Aging		reliability
	Weight	Probability	Weight	Probability	Weight	Probability	Weight	Probability	ΣWeight*(1- Probability)
Power grid	0.1	0.0000001	0.2	0.0000262	0.1	0.0000001	0.6	0.0002968	0.99981666
Diesel generator	0.15	0.0000001	0.01	0.0000500	0.3	0.0005000	0.54	0.0000716	0.9998108
Transformer	0.1	0.0000001	0.2	0.0000002	0.1	0.0000002	0.6	0.0000274	0.999983492
ATS	0.1	0.0000001	0.15	0.0000800	0.3	0.0008000	0.45	0.0000562	0.999722691
STS	0.1	0.0000001	0.15	0.0000800	0.3	0.0008000	0.45	0.0000262	0.9997362
UPS	0.1	0.0000001	0.15	0.0000900	0.3	0.0009000	0.45	0.0000572	0.99969077
High voltage circuit breaker	0.1	0.0000001	0.2	0.0000800	0.3	0.0000600	0.4	0.0000001	0.999965948
Low Voltage Circuit Breaker	0.1	0.0000001	0.15	0.0000002	0.4	0.0009000	0.35	0.0000001	0.99963991
Switchgear	0.1	0.0000001	0.15	0.0000020	0.3	0.0009000	0.45	0.0000220	0.99971979

this data center's maintenance staff determines the fault probability and the corresponding weight of various types of electrical equipment as Table 2.

In this paper, we simulated the power system of this real data center by applying the proposed parallel fault evolution model PFEM and vulnerable nodes' identification algorithm AIVDCN. Fig. 16 below shows the average ratio of lost power loads of each round of 20,000 episodes. We can find that the average ratio of lost power loads gradually converges to 40%-78% after 15,000 episodes. That is to say the proposed algorithm can identify the devices which will cause at least 40% power loss when they fail through evaluating 15,000 states of the power system at most, and the complexity of AIVDCN algorithm is much smaller than $O(C_n^k)$. Fig. 17 shows the number of times each device has been tripped. The more the device has been tripped, the more likely it will cause huge load lost after its failure. It can be seen that the electrical devices that has been tripped more often are double power automatic transfer switches, which plays the role of bridge in the power system.

In this paper, after convergence of the proposed AIVDCN algorithm, the lost loads caused by vulnerable devices obtained by five other algorithms are compared. The six algorithms are: AIVDCN, node degree [62] centrality, random algorithm, node eigenvector centrality, node betweenness centrality [11] and node closeness centrality [11]. The comparative experiment has three steps. The first step gets the vulnerable nodes' vector *VUL* of the six algorithms respectively. And then sequentially tripping any k electrical devices in *VUL* of every algorithm, the load loss is derived correspondingly. In the end, the load loss of any k electrical devices of each algorithm is sorted from large to small.

Fig. 18 shows the relationship between the percentage of lost loads (Eq. (1.1)) and the number of initial fault nodes. Fig. 19 shows the relationship between the quantitative representation of vulnerability parameter (Eq. (1.2)) and the number of initial fault nodes. From the results we can find that:

(1) Deliberate tripping of electrical devices can significantly affect the power supply of the IDC power system. There would be more than 15% power loads loss when one (0.17%) electrical device has been tripped, which make clear that there are vulnerable spots in the IDC power network.
(2) AIVDCN algorithm can find more vulnerable nodes: after more than two initial equipment fail, the loss of load is at least 5% higher than that of other algorithms.
(3) Tripping seven (1.18%) electrical devices of the IDC power system with the proposed AIVDCN algorithm will lead to crash of all loads.

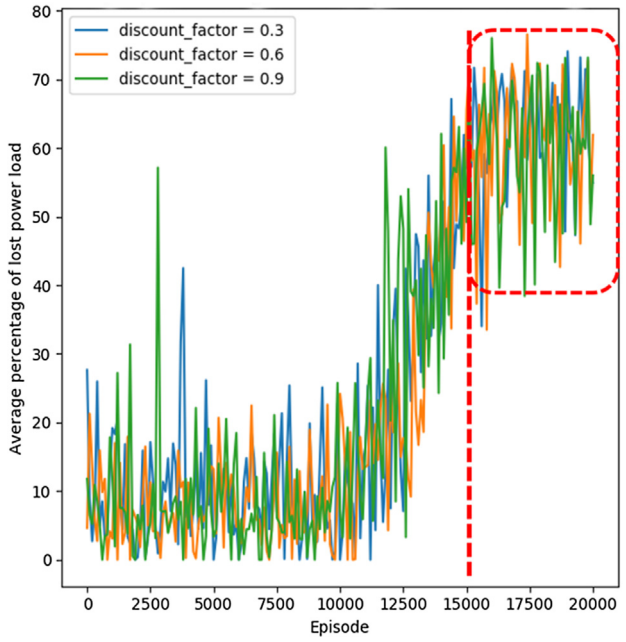


Fig. 16. Average percentage of lost power loads in a real IDC power system.

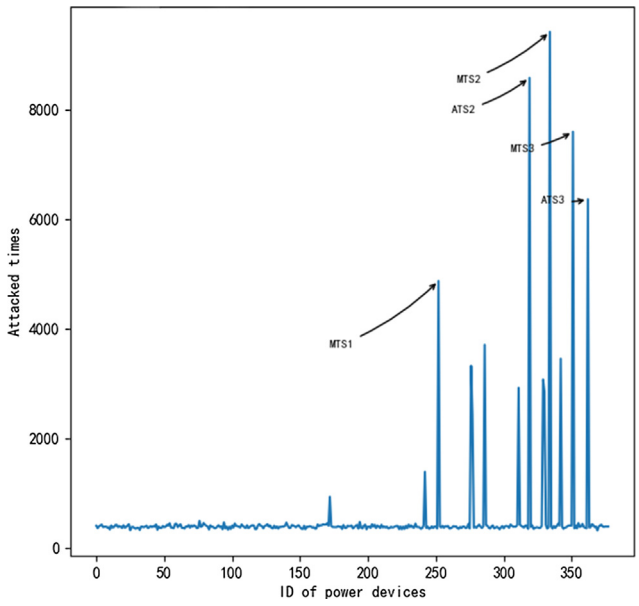


Fig. 17. Times of being tripped for each electrical device.

But other algorithms can't do it. That is to say AIVDCN has advantages of finding the vulnerability of the IDC power system.

(4) Our novel AIVDCN algorithm is better than other vulnerable spots' identifying algorithms in terms of both lost loads and quantitative representation of vulnerability.

6. Conclusions

The power system in the data centers is very important. The failure of some electrical devices may lead to large-scale power outage, which will affect the operation of information systems directly. Therefore, it is necessary to identify such devices in advance. In this paper, the fault evolution model of the power system is parallelized, and the AIVDCN algorithm is proposed to identify the vulnerable spots of the power system. The proposed PFEM model make full utilize the characteristics of the IDC power system, which has parallel acceleration advantage.

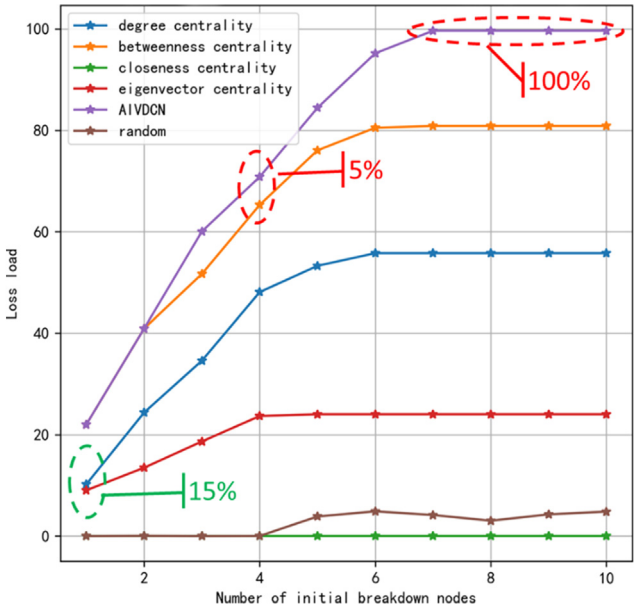


Fig. 18. Relationship between lost loads and the number of initial fault nodes.

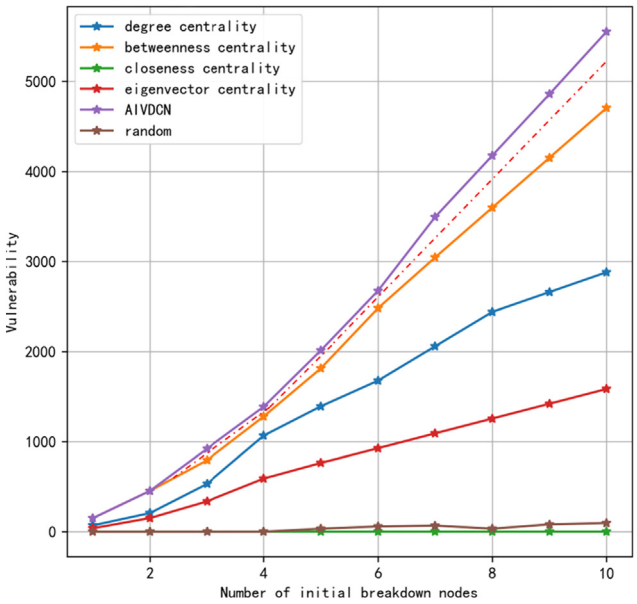


Fig. 19. Relationship between the quantitative representation of vulnerability and the number of initial fault nodes.

The proposed model can simulate the power fault evolution process, such as the transfer of power (from one path to another following topological changes) and electrical device tripping. Through this model, the fault nodes can be selected arbitrarily and the corresponding lost loads can be observed. The proposed AIVDCN algorithm can find more vulnerable spots whose failure may cause loss of loads at least 5% higher than that of other algorithms.

As it applies a generalized representation of the power system's states, AIVDCN algorithm can be applied to various IDC power network topologies especially large-scale ones. Furthermore, as the proposed model PFEM is specifically tailored for data center power systems, so it is not applicable to power transmission systems. But the proposed AIVDCN algorithm is not limited to the IDC power system, so it is also applicable to power transmission systems. The only thing that needs to be done is redefining the state space and action space when applying this algorithm to power transmission systems.

CRediT authorship contribution statement

Chunjian Kang: Conceptualization, Methodology, Software, Validation, Formal analysis, Investigation, Resources, Data curation, Writing - original draft, Writing - review & editing, Supervision. **Jianwen Huang:** Funding acquisition. **Zhang Zhang:** Project administration. **Qiang Liu:** Writing - original draft. **Wenping Xiang:** Writing - original draft. **Zhiguo Zhao:** Visualization. **Xinpei Liu:** Writing - review & editing. **Liwen Chong:** Data curation.

Declaration of Competing Interest

We declare that we have no financial and personal relationships with other people or organizations that can inappropriately influence our work, there is no professional or other personal interest of any nature or kind in any product, service and/or company that could be construed as influencing the position presented in, or the review of, the manuscript entitled “An Automatic Algorithm of Identifying Vulnerable spots of Internet Data Center Power Systems Based on Reinforcement Learning”.

Acknowledgements

This work was supported by CNCERT/CC Foundation for Young Scholars.

Appendix A. Supplementary material

Supplementary data to this article can be found online at https://doi.org/10.1016/j.ijepes.2020.106145.

References

[1] Cao Fang, Wang Yajing, Zhu Feng, Cao Yujie, Ding Zhaohao. UPS node based workload management for data centers considering flexible service requirements. In: 2019 IEEE/IAS 55th Industrial and Commercial Power Systems Technical Conference. I&CPS2019, Calgary, Canada; 2019, pp. 1–9.
[2] Tian Bing, Mao Chengxiong, Lu Jiming, Wang Dan, He Yu, Duan Yuping, Qiu Jun. 400 V/1000 kVA Hybrid Automatic Transfer Switch IEEE Transactions on Industrial Electronics, 60 (2013), pp. 5422–5435.
[3] Yao Jia, Abramovitz Alexander, Wang Yu, Weng Hongjie, Zhao Jianfeng. Safe-triggering-region control scheme for suppressing cross current in static transfer switch. Electric Pow Syst Res 2015;125:245–253.
[4] Sărăcin Cristina Gabriela, Sărăcin Marin, Zdrenţu Daniel. Experimental study platform of the automatic transfer switch used to power supplies back-up. In: 2013 - 8th International Symposium on Advanced Topics in Electrical Engineering. ATEE2013, Bucharest; 2013. p. 1–6.
[5] Zhongguancun online enterprise station China. Fire attacks of the data center; 2012. [Online]. Available: http://server.zol.com.cn/337/3371759_all.html; [accessed 20 August 2019].
[6] Liang Gaoqi, Weller Steven R, Zhao Junhua, Luo Fengji, Yang Dong Zhao. The 2015 ukraine blackout: Implications for false data injection attacks IEEE. Trans Power Syst 2017;32:3317–3318.
[7] Cuadra Lucas, Salcedo-Sanz Sancho, Ser Javier Del, Jiménez-Fernández Silvia, Woo Geem Zong. A Critical Review of Robustness in Power Grids Using Complex Networks Concepts. Energies 2015; 8:211–9265.
[8] Abedi Amin, Gaudard Ludovic. Franco Romerio Review of major approaches to analyze vulnerability in power system. Reliab Eng Syst Saf 2019;183:153–72.
[9] Chunjian Kang, Xinpei Liu, Su Chen, Junbiao Xu. Study on identifying the vulnerability of the data center power network. In: 2018 International Seminar on Computer Science and Engineering Technology. SCSET 2018, Shanghai, China; 2019.
[10] Grondman Ivo, Busoniu Lucian, Lopes Gabriel AD, Babuska Robert. A Survey of Actor-Critic Reinforcement Learning: Standard and Natural Policy Gradients. IEEE Trans Syst Man Cybernet C (Appl Rev) 2012; 42:1291–1307.
[11] Francisco Gutierrez E, Barocio F, Uribe P Zuniga. Vulnerability analysis of power grids using modified centrality measures. Discrete Dynamics in Nature and Society 2013.
[12] Zio Enrico. Challenges in the vulnerability and risk analysis of critical infrastructures. Reliab Eng Syst Saf 2016;152:137–150.
[13] Bompard Ettore, Huang Tao, Wu Yingjun, Cremenescu Mihai. Classification and trend analysis of threats origins to the security of power systems. Int J Electr Pow Energy Syst 2013;50:50–64.
[14] Liu Chen-Ching, Jung Juhwan, Heydt GT, Vittal V, Phadke AG. The strategic power infrastructure defense (SPID) system - A conceptual design. IEEE Control Syst Mag 2000;20:40–52.
[15] Min Ouyang. Comparisons of purely topological model, betweenness based model and direct current power flow model to analyze power grid vulnerability. Chaos 2013;23:293–6.
[16] Cuffe Paul. A comparison of malicious interdiction strategies against electrical networks. IEEE J Emerg Select Top Circuits Syst 2017;7:205–217.
[17] Miller Colin R. Electromagnetic pulse threats in 2010. Electromagnetic Pulse Threats 2005;16:903–904.
[18] Cun-Lai Pu, Wei Cui. Vulnerability of complex networks under path-based attacks. Physica A: Statist Mech Appl 2015;419:622–629.
[19] Ten Chee-Wooi, Ginter Andrew. Rashiduzzaman bulbul cyber-based contingency analysis. IEEE Trans Power Syst 2016;31:3040–50.
[20] Bompard E, Napoli R, Xue F. Assessment of information impacts in power system security against malicious attacks in a general framework. Reliab Eng Syst Saf 2009;94:1087–1094.
[21] Kalech Meir. Cyber-attack detection in SCADA systems using temporal pattern recognition techniques. Comput Secur 2019;84:225–38.
[22] Koç Yakup, Warnier Martijn, Kooij Robert E, Brazier Frances MT. An entropy-based metric to quantify the robustness of power grids against cascading failures. Saf Sci 2013;59:126–34.
[23] Donde Vaibhav, Lopez Vanessa, Lesieutre Bernard, Pinar Ali, Yang Chao, Meza Juan. Severe Multiple Contingency Screening in Electric Power Systems. IEEE Trans Power Syst 2008; 23:406–417.
[24] Pinar Ali, Meza Juan, Donde Vaibhav, Lesieutre Bernard. Optimization Strategies for the Vulnerability Analysis of the Electric Power Grid. SIAM J Optim 2010;20:1786–1810.
[25] Vaiman M, Bell K, Chen Y, Chowdhury B, Dobson I, Hines P, et al. Risk assessment of cascading outages: methodologies and challenges. IEEE Trans Power Syst 2012;27:631–41.
[26] Guo Hengdao, Zheng Ciyan, Ho-Ching Iu Herbert, Fernando Tyrone. A critical review of cascading failure analysis and modeling of power system. Renew Sustain Energy Rev 2017;80:9–22.
[27] Junjian Qi, Shengwei Mei. Blackout model considering slow process and SOC analysis. In: 2012 IEEE Power and Energy Society General Meeting. PES2012, San Diego, USA; 2012, pp. 1–6.
[28] Eppstein MJ, Hines PDH. A ‘random chemistry’ algorithm for identifying collections of multiple contingencies that initiate cascading failure. IEEE Trans Power Syst 2012;27:1698–705.
[29] Yan Jun, Tang Yufei, He Haibo, Sun Yan. Cascading failure analysis with DC power flow model and transient stability. IEEE Trans Power Syst 2015;30:285–97.
[30] Song Jiajia, Cotilla-Sanchez Eduardo, Ghanavati Goodarz, Hines Paul DH. Dynamic modeling of cascading failure in power systems. IEEE Trans Power Syst 2016;31:2085–95.
[31] Demarco CL, Qverbye TJ. An energy based security measure for assessing vulnerability to voltage collapse. IEEE Trans Power Syst 1990;5:419–27.
[32] Amja Nima, Esmaili Masoud. Improving voltage security assessment and ranking vulnerable buses with consideration of power system limits. Int J Electr Power Energy Syst 2003;25:705–715.
[33] Singh C, Patton AD. Protection system reliability modeling: unreadiness probability and Mean duration of undetected faults. IEEE Trans Reliab 1980;29:339–40.
[34] Sheng Su, Li KK, Chan WL, Xiangjun Zeng, Xianzhong Duan. Monte Carlo based maintenance resource allocation considering vulnerability. In: 2005 IEEE/PES Transmission & Distribution Conference & Exposition: Asia and Pacific. 2005, Dalian, China; 2005, pp. 1–5.
[35] Delgadillo Andrés, Manuel Arroyo José, Alguacil Natalia. Analysis of electric grid interdiction with line Switching. IEEE Trans Power Syst 2010; 25:633–641.
[36] López-Lezamaa Jesús M, JuanCortina-Gómezb, Muñoz-Galeano Nicolás. Assessment of the electric grid interdiction problem using a nonlinear modeling approach. Electric Power Syst Res 2017;144:243–254.
[37] Stubna MD, Fowler J. An application of the highly optimized tolerance model to electrical blackouts. Int J Bifurcation Chaos 2003;13:237–42.
[38] Baea Koeunyi, Thorpb James S. A stochastic study of hidden failures in power system protection. Decis Support Syst 1999;24:259–68.
[39] JieChen James S, Thorp IanDobson. Study on cascading dynamics in power transmission systems via a DC hidden failure model. Int J Electr Power Energy Syst 2005;27:318–26.
[40] Dobson I, Chen J, Thorp JS, Carreras BA, Newman DE. Examining criticality of blackouts in power system models with cascading events. In: Proceedings of the 35th Hawaii International Conference on System Sciences. HICSS2002, Big Island, HI, USA; 2002, pp. 10.
[41] Dobson I, Carreras B, Lynch V, Newman D. An initial model for complex dynamics in electric power system blackouts. In: Proceedings of the 34th Hawaii International Conference on System Sciences. HICSS2001, Maui, HI, USA; 2001. p. 51.
[42] Zhongwei Meng, Zongxiang Lu, Jingyan Song. Comparison analysis of the small-world topological model of Chinese and American power grids. Automation Electric Power Syst 2004;28:21–24.
[43] Ming Ding, Pingping Han. Small-world topological model based vulnerability assessment to large-scale power grid. Proc CSEE 2005; 25:118–122.
[44] Åke J. Holmgren Using graph models to analyze the vulnerability of electric power networks Risk Anal, 2006;26:955–969.
[45] Bompard Ettore, Luo Lingen, Pons Enrico. A perspective overview of topological approaches for vulnerability analysis of power transmission grids. Int J Crit Infrastruct 2015;11:15–26.
[46] Paolo Crucitti, Vito Latora, Massimo Marchiori. A topological analysis of the Italian electric power grid. Physica A: Statist. Mech. its Appl. 2004;338:92–97.
[47] Pepyne David L. Topology and cascading line outages in power grids. J Syst Sci Syst

Eng 2007; 16:202–221.
[48] Guohua Zhang, Ce Wang, Jianhua Zhang, Jingyan Yang, Yin Zhang, Manyin Duan. Vulnerability assessment of bulk power grid based on complex network theory. In: 2008 Third International Conference on Electric Utility Deregulation and Restructuring and Power Technologies. DRPT 2008, Nanjing, China; 2008, pp. 1554–1558.
[49] Ni Zhen, Paul Shuva, Zhong Xiangnan, Wei Qinglai. A reinforcement learning approach for sequential decision-making process of attacks in smart grid. In: 2017 IEEE Symposium Series on Computational Intelligence. SSCI2017, Honolulu, USA; 2017, pp. 1–8.
[50] Yan Jun, He Haibo, Zhong Xiangnan, Tang Yufei. Q-learning-based vulnerability analysis of smart grid against sequential topology attacks. IEEE Trans Inform Forensics Security 2017;12:200–210.
[51] Simon Haykin Neural networks and learning machines Pearson Prentice Hall, NJ, USA; 2008.
[52] Abdulrasheed Babalola Adeniyi, Belkacemi Rabie, Zarrabian Sina, Craven Robert. Adaptive Immune System reinforcement Learning-Based algorithm for realtime Cascading Failures prevention. Eng. Appl. Artif. Intell. 2017; 57:118–133.
[53] Sina Zarrabian, Rabie Belkacemi, Adeniyi Babalola. A Reinforcement learning approach for congestion management and cascading failure prevention with experimental application. Electric Power Syst. Res. 2016;141:179–190.
[54] Chopade Pravin, Bikdash Marwan. New centrality measures for assessing smart grid vulnerabilities and predicting brownouts and blackouts. Int. J. Crit. Infrastruct. Protect 2016;12:29–45.
[55] Bompard Ettore, Estebsari Abouzar, Huang Tao, Fulli Gianluca. A framework for analyzing cascading failure in large interconnected power systems: a post-contingency evolution simulator. Int J Electr Power Energy Syst 2016;81:12–21.
[56] Nilsson James W. Introductory circuits of electrical and computer engineering. Pearson, New York, USA; 2001.
[57] Sutton Richard S, Barto Andrew G. Reinforcement Learning: An Introduction. MIT Press, MA, USA; 1998.
[58] M.J.D. Powell, Radial basis functions for multivariable interpolation: A review. J.C. Mason, M.G. Cox (Eds.), Algorithms for Approximation, Clarendon Press, Oxford (1987), pp. 143–167.
[59] Vamplew Peter, Dazeley Richard, Foale Cameron. Softmax exploration strategies for multiobjective reinforcement learning. Neurocomputing 2017; 263:74–86.
[60] Arfken George B, Weber Hans J, Harris Frank E. Math Method Physic Academic Press, MA, USA, 2012.
[61] Networkx. Software for complex networks; 2002. [Online]. Available: http://networkx.github.io/; [accessed 20 August 2019].
[62] Wang Shuai, Liu Jing. Robustness of single and interdependent scale-free interaction networks with various parameters. Phys A 2016;460:139–51.