Deducing cascading failures caused by cyberattacks based on attack gains and cost principle in cyber-physical power systems

Yufei WANG^{1,2}, Yanli LIU³, Jun'e LI¹

Abstract To warn the cascading failures caused by cyberattacks (CFCAs) in real time and reduce their damage on cyber-physical power systems (CPPSs), a novel early warning method based on attack gains and cost principle (AGCP) is proposed. Firstly, according to the CFCA characteristics, the leading role of attackers in the whole evolutionary process is discussed. The breaking out of a CFCA is deduced based on the AGCP from the view of attackers, and the priority order of all CFCAs is then provided. Then, the method to calculate the probability of CFCAs is proposed, and an early warning model for CFCA is designed. Finally, to verify the effectiveness of this method, a variety of CFCAs are simulated in a local CPPS model based on the IEEE 39-bus system. The experimental results demonstrate that this method can be used as a

reliable assistant analysis technology to facilitate early warning of CFCAs.

Keywords Cyber-physical power system, Cascading failure, Cyberattack, Early warning, Fault probability, Attack gains and cost principle, Attack route choice

1 Introduction

In power systems, cyberspace and physical space have become integrated deeply in recent years. A power system has become a typical cyber-physical system in which cascading failures caused by cyberattacks (CFCAs) may occur [1–6]. CFCAs originate from the cyberspace and eventually cause great damage to the power systems. For example, in February 2006, during the “Aurora” military maneuver conducted by the United States, cyberattacks led to multiple generators going out of operation and a large-scale blackout in the eastern area [7]. In September 2010, the Stuxnet virus attacked programmable logic controllers and Iran nuclear centrifuges broke down, resulting in serious damage to the infrastructure of Iran’s nuclear industry [8]. In December 2015, the malicious attackers conquered the computer systems of the Ukraine power grid through “0-day” vulnerabilities and SSH backdoor, and used “Black energy” software to attack the power grid causing widespread blackout [9–11]. Therefore, it is of great significance to establish an effective method for early warning of CFCAs.

In the early researches on CFCAs, some scholars explored the internal logical relations between cybersecurity and power system faults and evaluated the impact of cyberattacks existing in supervisory control and data acquisition (SCADA), energy management system (EMS)

CrossCheck date: 27 November 2018

Received: 31 December 2017 / Accepted: 27 November 2018 /

Published online: 20 February 2019

© The Author(s) 2019

✉ Yanli LIU
yanliliu@tju.edu.cn

Yufei WANG
wallyful@126.com

Jun'e LI
jeli@whu.edu.cn

¹ Key Laboratory of Aerospace Information Security and Trusted Computing, Ministry of Education, School of Cyber Science and Engineering, Wuhan University, Wuhan 430072, China

² Global Energy Interconnection Research Institute Co. Ltd, Beijing 102209, China

³ Key Laboratory of Smart Grid of Ministry of Education, Tianjin University, Tianjin 300072, China

and so on [12–16]. The propagation process of CFCA has been simulated in IEEE-39 bus, IEEE 118-bus, and some real power systems [17–20]. The consequence of CFCA was calculated based on Bayesian network, attack graph and Petri network [21–23] and was also discussed based on percolation theory [24]. In [25], all kinds of cascading failures across cyber and physical spaces were studied based on an improved attack graph. The quantitative method of evaluating the consequence of CFCA was also proposed. In [26], an algorithm to identify CFCA in smart grid was proposed. In [27], all behaviors of attackers and defenders in a finite number of scenarios were deduced by game theory, and the main protection measures were discussed. However, there is lack of research on the real-time detection and early warning technology of CFCA. Especially, the priority order and the occurrence probability of CFCA cannot be judged effectively because it is difficult to determine the attacker propensity choice for attack routes if the process of CFCA is not analyzed from the view of attackers.

In this paper, the evolutionary process of CFCA and the attacker propensity choice are accurately deduced based on attack gains and cost principle (AGCP), and a novel early warning model of CFCA is proposed from the view of attackers. First, the leading role of attackers in the whole evolutionary process of CFCA is analyzed, and the CFCA sorting problem is abstracted into an optimal route search problem and solved. Then, according to the actual situation of cyber-physical power system (CPPS), the calculation method of all AGCP parameters are defined, the method of calculating the probability of CFCA is proposed based on AGCP, and the CFCA early warning model is designed from the whole life cycle of CFCA. Finally, a variety of CFCA are simulated in a typical CPPS, and both the priority choice order and the probability of CFCA are calculated.

2 Attack gains and cost principle

The AGCP, a ratio which is a general evaluation for attack's effectiveness, is the comprehensive comparison between attack cost and attack gain after performing an attack [28, 29]. The attack cost usually includes the difficulties of attack, the software/hardware protection, knowledge/experience required, cost of time, etc. The attack gains refer to what the attackers obtain from the attacked target. The AGCP ratio is calculated as:

$$Q = \sum_{i=1}^k q_i = \sum_{i=1}^k \frac{f_C^i(C_1^i, C_2^i, \dots, C_n^i)}{f_G^i(G_1^i, G_2^i, \dots, G_n^i)} \quad (1)$$

where Q is the AGCP ratio; the whole attack process includes k attack substeps and q_i is the AGCP ratio of

substep i , which is calculated by the cost function f_C^i consisting of n cost factors $C_1^i, C_2^i, \dots, C_n^i$ and the gains function f_G^i consisting of n gain factors $G_1^i, G_2^i, \dots, G_n^i$.

The AGCP can be summarized as “during an attack, attackers expect to get the minimum ratio of cost to gains”. It means the maximum attack gains are expected by paying as little attack cost as possible. Of course, attackers could make extreme choices in exceptional situations. For example, attackers will ignore the cost of inducing the CFCA to inflict maximum damage to CPPS in cyberwarfare.

3 Deducing evolutionary process of CFCA based on AGCP

3.1 Leading role of attackers in CFCA

CFCA is different from the traditional cascading failures of the power system. The source of the CFCA comes from cyberspace and results in the final damage to the power system. Firstly, attackers induce the immediate visible faults or the delayed invisible faults of power secondary equipment by cyberattacks. Then, “ $N - 1$ ” fault and even the cascading failures, which is the attack target, may be caused. Therefore, attackers are the key leading factor of CFCA. Each substep of CFCA is decided by the intention and decision of the attacker analyzing the CFCA from the view of attackers can restore the evolutionary process of CFCA and calculate the probability of CFCA more realistically.

3.2 Sorting priority order of CFCA based on AGCP

As shown in Fig. 1, the attack graph of CFCA is built according to [25, 26, 30]. The attack graph of CFCA could be described as $G(V, A)$, where V is the set of vertices, and A is the set of directed edges. The attack graph of CFCA has multiple sources $\{V_1, V_2\}$ and multiple sinks $\{V_9, V_{10}, V_{11}, V_{12}, V_{13}, V_{14}\}$. Each of these directed edges, which represents an attack substep, is the driving process between two adjacent events in CFCA. Each directed attack route from the source to sink represents one class of CFCA. Attackers need to evaluate each attack route comprehensively to determine the priority order of attack routes and select an optimal attack route for themselves to endanger CPPS. The process of evaluating attack routes is as follows.

3.2.1 Basis of attack route decision

According to the attack graph, attackers need to make two decisions for each substep to fulfill CFCA: one is

Fig.1 Attack graph of CFCA

choosing which kind of power secondary failure as a phased attack target after the cyberattack is identified, and the other is choosing which power primary failure as the final target after the power secondary failure is identified. For the attack graph of CFCA, the weights of directed edges affect the choice on the attack route. How to define the weights of directed edges is the key to analyze the attacker behavior.

3.2.2 Measuring the attack effectiveness

The AGCP ratio, which represents the weight of directed edges, is used to measure the effectiveness of attack substeps.

There are 42 attack routes in the attack graph. Each route includes a directed edge $A_{\alpha,\beta}^1$ from the vertex of the L_1 layer to the vertex of the L_2 layer and a directed edge $A_{\beta,\gamma}^2$ from the vertex of the L_2 layer to the vertex of the L_3 layer. In this paper, the superscript "1" means the variables from L_1 to L_2 ; the superscript "2" means the variables from L_2 to L_3 . $\alpha \in \{1, 2\}$, $\beta \in \{3, 4, \dots, 8\}$, $\gamma \in \{9, 10, \dots, 14\}$.

As shown in (2), $Q_{\alpha,\beta,\gamma}$ of each attack route is the sum of the weight $q_{\alpha,\beta}^1$ of directed edge $A_{\alpha,\beta}^1$ and the weight $q_{\beta,\gamma}^2$ of directed edge $A_{\beta,\gamma}^2$. For example, $Q_{2,3,10}$ of the attack route $V_2 \rightarrow V_3 \rightarrow V_{10}$ is $q_{2,3}^1 + q_{3,10}^2$.

$$Q_{\alpha,\beta,\gamma} = q_{\alpha,\beta}^1 + q_{\beta,\gamma}^2 \quad (2)$$

1) Calculating $q_{\alpha,\beta}^1$

$q_{\alpha,\beta}^1$ represents the gain and cost of secondary power system failure caused by cyberattacks. The attack cost C^1 of $q_{\alpha,\beta}^1$ includes the following three factors:

a) The concealed factor C_C^1 of a cyberattack indicates the probability of the cyberattack being detected. The higher its value is, the easier the cyberattack will be detected and the higher the corresponding attack cost will be. As shown in (3), a_{total}^1 is the historical statistics data that all types of scanning occur, a_C is the historical statistics result that the cyberattack was successfully detected, and L_C^1 is the historical statistics result that the cyberattack occurred.

$$C_C^1 = \frac{a_C}{a_{total}^1} \quad (3)$$

b) The implementation factor C_I^1 of the cyberattack indicates the historical percentage of scanning the cyberattack. The lower the value is, the easier scanning is and the lower the cyberattack cost is. As shown in (4), a_i^1 is the historical statistics data that type i scanning occurs.

$$C_I^1 = \frac{a_{total}^1}{a_i^1} \bigg/ \sum_{i=1}^{k^1} \frac{a_{total}^1}{a_i^1} \quad (4)$$

c) The duration factor C_T^1 of the cyberattack indicates the sustained time to execute the cyberattack. The higher

the value is, the easier the cyberattack can be detected and the more cost it will take. As shown in (5), t is the attack duration time measured in seconds.

$$C_T^1 = e^{-(1/t)} \quad t \in [0, +\infty) \quad (5)$$

Similarly, the attack gain G^1 of $q_{\alpha,\beta}^1$ is defined as the harm factor G_F^1 of secondary faults.

d) The harm factor G_F^1 represents the functional failure degree of a power secondary fault after a cyberattack, $G_F^1 \in [0, 1]$. G_F^1 can be calculated according to actual situation as:

$$G_F^1 = 1 - \frac{g_{F'}^1}{g_F^1} \quad (6)$$

where $g_{F'}^1$ is the remaining functional degree of secondary failure after a cyberattack; g_F^1 is the original functional degree. For example, once a protective device fails to operate due to a cyberattack and loses its protection function, G_F^1 is 1; once the adjustable output range of the generator is only 30% of the normal value after a cyberattack, G_F^1 is 0.7.

Considering all the above factors, the equation for calculating $q_{\alpha,\beta}^1$ can be written as:

$$q_{\alpha,\beta}^1 = \frac{\lambda_C^1 (C_C^1)^{\eta_C} + \lambda_I^1 (C_I^1)^{\eta_I} + \lambda_T^1 (C_T^1)^{\eta_T}}{\lambda_F^1 G_F^1} \quad (7)$$

In (7), λ^1 and η^1 can be dynamically adjusted according to the expectation focus.

2) Calculating $q_{\beta,\gamma}^2$

$q_{\beta,\gamma}^2$ represents the gain and cost of the primary failure caused by the secondary power system failure. The attack cost C^2 of $q_{\beta,\gamma}^2$ includes the following three factors:

a) The concealed factor C_C^2 of secondary faults indicates whether the secondary failure would trigger the three defense lines of power systems. If not triggered, its value is 0, and otherwise the value is 1.

b) The detection factor C_D^2 of secondary faults is the detection probabilities of faults, which could be approximately expressed by the historical data.

c) The duration factor C_T^2 of secondary failure is given by (8). The higher the value is, the easier it will be detected and the more cost it will take.

$$C_T^2 = e^{-(1/t)} \quad t \in [0, +\infty) \quad (8)$$

Similarly, the attack gain G^2 of $q_{\beta,\gamma}^2$ is defined by the following two parts.

d) The triggering factor G_C^2 of the secondary failure causes the primary failure. If a secondary failure can

immediately cause primary failure, its value is 1, and otherwise it is 0.

c) The ratio of power loss G_P^2 caused by primary faults is shown in (9). $\sum P_{D_0}$ is the original total power, and $\sum P_{D'}^1$ is the total power after primary faults.

$$G_P^2 = \frac{|\sum P_{D_0} - \sum P_{D'}^1|}{\sum P_{D_0}} \quad (9)$$

Considering all the above factors, the equation for calculating $q_{\beta,\gamma}^2$ is shown in (10). λ^2 and η^2 are the importance weights of factors.

$$q_{\beta,\gamma}^2 = \frac{\lambda_C^2 (C_C^2)^{\eta_C} + \lambda_P^2 (C_P^2)^{\eta_P} + \lambda_T^2 (C_T^2)^{\eta_T}}{G_C^2 \lambda_P^2 G_P^2} \quad (10)$$

3.2.3 Solving priority order of attack routes

After defining the weights of all directed edges, the AGCP ratio of each attack route can be calculated. The following three principles should be considered when attackers search the optimal attack route.

1) The 1st principle: the minimum Q priority

For attackers, the optimal attack route search problem, which selects the CFCA with the minimum sum value of the AGCP ratio Q , can be equivalent to the shortest path search problem. Since the attack graph of CFCA has multiple sources (V_1 and V_2), it is necessary to iteratively search each source to obtain the priority order of attack routes, and select the attack route with minimum Q as the optimal one. If multiple attack routes have the same AGCP ratio Q , attackers can further select the attack route according to the 2nd or the 3rd principle.

2) The 2nd principle: success rate first

If there are some attack routes with the same Q , the attacker prefers the attack route with a smaller variance of all attack substeps with a small AGCP ratio. The variance is calculated using (11) and (12).

$$E(q_x) = \frac{1}{2} \sum_{l=1}^2 q_x^l \quad (11)$$

$$D(q_x) = \sum_{l=1}^2 [q_x^l - E(q_x)]^2 \quad (12)$$

where q_x^l is the AGCP ratio of the l layer directed edge in the attack route x . The value of q_x^l indicates the difficulty of attack substeps. The attack substeps with higher q_x^l values are not always successfully completed by attackers with different technical backgrounds; thus the failure of CFCA

should be avoided if a certain substep is too difficult to achieve.

3) The 3rd principle: the gains priority

If there are some attack routes with the same Q , the attacker prefers the attack route with the maximum sum of $G_x^1 + G_x^2$.

In summary, the priority order of principles is slightly different for attackers with different purposes: the order “1st principle > 2nd principle > 3rd principle” would be selected by attackers who pursue the success rate of CFCA; the order “1st principle > 3rd principle > 2nd principle” would be selected to pursue more gain of CFCA.

3.3 Calculating probability of CFCA based on priority order

After the priority order of attack routes is determined, attackers would choose the attack route with minimum Q from the ideal view. However, the attackers are not unconditionally blind to pursue the minimum Q . Once one attack substep is difficult to achieve (if the technique difficulties are beyond the attacker capabilities or the step can be easily detected), attackers are likely to abandon this attack route by risk avoidance consideration, and choose the second best attack route. Therefore, the suboptimal attack route in priority order still has a great probability of occurrence. To quantify the attacker choice of attack route, the priority order of attack routes is probabilistically calculated.

The principle of the calculation could be summarized as follows: calculate the probability according to 1st principle > 2nd principle > 3rd principle or 1st principle > 3rd principle > 2nd principle; if the probability of several attack routes is the same, the probability is revised according to the 2nd or 3rd principle. The detailed steps are given as follows.

Step 1 Determining the priority order of attack routes. The orders 1st principle > 2nd principle > 3rd principle or 1st principle > 3rd principle > 2nd principle could be selected, and the order 1st principle > 2nd principle > 3rd principle is assumed here.

Step 2 According to both the 1st principle and the Q of the attack route x , the initial probability $P_x^{(1)}$ of the attack route x is calculated by (13).

$$P_x^{(1)} = \frac{\frac{1}{Q_x}}{\sum \frac{1}{Q}} \times 100\% \quad (13)$$

Step 3 According to the 2nd principle, the revised probability of the attack route x is given. If G_x^2 of the attack route x is the same as others, $P_x^{(1)}$ is corrected as $P_x^{(2)}$ with the 2nd principle and their variances $D(x)$ by (14).

$$P_x^{(2)} = \begin{cases} P_x^{(1)} + \Delta x & \text{if } D(x) < E[D(x)] \\ P_x^{(1)} & \text{if } D(x) = E[D(x)] \\ P_x^{(1)} - \Delta x & \text{if } D(x) > E[D(x)] \end{cases} \quad (14)$$

where Δx is the corrected value of initial probability $P_x^{(1)}$ to reflect the impact of the 2nd principle on priority order. Under the case that many attack routes have the same Q , the probability of an attack route with a lower variance is slightly higher than others with larger variances. $D(x)$ is the variance of q_x , and $E[D(x)]$ is the mean value of $D(x)$.

Step 4 According to the 3rd principle, the final probability of an attack route P_x^* is given. If $P_x^{(2)}$ of the attack route x is not the same as any other route, then $P_x^{(2)}$ is its final probability P_x^* ; if $P_x^{(2)}$ of several attack routes are the same, then $P_x^{(2)}$ could be corrected to P_x^* with the 3rd principle and their damage Dam , as (15).

$$P_x^* = \begin{cases} P_x^{(2)} + \Delta y & \text{if } Dam(x) > E[Dam(x)] \\ P_x^{(2)} & \text{if } Dam(x) = E[Dam(x)] \\ P_x^{(2)} - \Delta y & \text{if } Dam(x) < E[Dam(x)] \end{cases} \quad (15)$$

where Δy is the corrected value of $P_x^{(2)}$ reflecting the impact of the 3rd principle on priority order. In the case when many attack routes have the same variance, the probability of an attack route with greater damage is slightly higher than others with smaller damage. $Dam(x)$ is the damage in the attack route x , and $E[Dam(x)]$ is the mean value of $Dam(x)$.

Step 5 According to the priority order, the inequalities are solved to obtain the feasible solution of Δx and Δy .

Step 6 Obtain the final probability P_x^* of the attack route x .

If the order 1st principle > 3rd principle > 2nd principle is selected, then switch the order of **Step 3** and **Step 4**.

Calculating the probability of CFCA based on the AGCP ratio has two main advantages. On the one hand, the purpose of attackers to pursue the minimum AGCP ratio could be directly reflected; on the other hand, this method of calculation reflects the actual situation as close as possible by considering the attack route selection as a tendentious probabilistic problem because attackers have incomplete knowledge and are trapped in various external conditions.

4 Early warning model of CFCA

4.1 Life cycle of CFCA

The life cycle of CFCA is analyzed according to its generation and propagation mechanism. If CFCA is considered as an event, it can be divided into three successive

stages as “before the event”, “during the event” and “after the event”. The “before the event” is a preparation period of CFCA, and the basic states of the target are detected by attacker technical means that include IP and ports scanning, topology discovery, vulnerability discovery, etc. The optimal or suboptimal attack route is selected according to the attack graph described in Section 3. The “during the event” is the formation stage of CFCA.

Attackers implement the cyberattack, sequentially resulting in power secondary and primary faults. The “after the event” is the spread stage of CFCA. The $N-1$ fault occurs in multiple vulnerability power nodes at the same time or in turn, leading to the instability of power systems and even large-scale blackout, as shown in Fig. 2.

4.2 Working principle of CFCA early warning

The existing security protection technologies and devices in CPPS are isolated from each other; therefore, it is difficult for them to cooperate. Traditional detection technologies, such as intrusion detection system (IDS), intrusion prevention system (IPS), and security operation center (SOC) and other traditional cybersecurity technologies focus on the security of cyberspace and cannot make judgments about the cyberthreats to power systems [31, 32]; besides, the three-defense-lines and fault diagnosis technologies in power systems focus on post-failure protection, making it difficult to trace the fault from the cyberspace and acquire early warning in advance.

To generate the CFCA early warning, a real-time detection technique of failure source is proposed. The preparation period of “before the event” or the cyberattack stage of “during the event” can be detected accurately in real time; then the type and probability of CFCA are predicted according to the detection results and the warning signal can be sent in time, facilitating protective measures such as fault blocking, changing system operation mode,

Fig.2 Life cycle of CFCA

and emergency response to realize the active defense for CFCA. The advantages of CFCA early warning technology include the following: ① It could be helpful to combine the cybersecurity detection with power systems protection to form a complete protection system of CPPS; ② It prevents the propagation of cyberattack in time; ③ In the case of irresistible cyberattacks (such as cyberwarfare), it can forecast the type of CFCA and make emergency response in advance.

4.3 CFCA early warning model design

The CFCA early warning model comprises seven parts, including data preprocessing and hybrid cyberattack detection, as shown in Fig. 3.

The hybrid cyberattack detection is the core part. It receives real-time information and network flow from the data preprocessing part and detects whether the cyberattacks can induce cascading failures across space. Then, it transmits the detection results to the diagnosis part, which determines the specific type of CFCA and sets the early warning. Finally, the final protection is taken based on the warning results from the emergency protection part. For hybrid cyberattack detection, cyberattack detection is abstracted to a multiple classification problem and solved by using a machine learning algorithm [31, 32]. The IDS based on the improved ball vector machine (IBVM) algorithm [31] has a higher detection accuracy and greater detection speed—a detection process can be finished within 10^{-6} s. The deployment of the

Fig.3 Framework of early warning model

CFCA early warning model is shown in Fig. 4. The model collects data in bypass mirror mode from both the communication and control networks.

5 Case studies

5.1 Test environment

To verify the method proposed in this paper, the local CPPS model is established based on a power plant simulation platform, smart substation simulation platform, and IEEE 39-bus system. The power plant simulation platform is used to simulate the 9# generator (G9); the smart substation platform is used to simulate Bus 29, and they are connected by the power dispatching data network. The early warning model is deployed in all platforms, as shown in Figs. 5 and 6.

In the local CPPS model, the cyberattack platform is used to simulate cyberattacks, and the early warning model is used to detect CFCA. Many cyberattack software programs are integrated into the cyberattack platform, such as the IP and port scan tool, remote malicious attack control tools, etc. The cyberattack platform launches cyberattacks for both the station layer nodes and network to induce CFCA. To facilitate real-time capture of all network messages, the network message capture tool is integrated into the early warning model.

5.2 CFCA priority sequence in local CPPS model

Based on the attack graph of CFCA, there are 27 directed edges and 28 attack routes in the local CPPS model. According to the AGCP calculation method and the principle order $1^{\text{st}} > 2^{\text{nd}} > 3^{\text{rd}}$, q of the directed edge, the attack route Q , the priority sequence, and the CFCA probability are calculated, as shown in Tables 1, 2 and 3. To simplify calculations, all λ and η in (7) and (10) are set to be 1. Suppose the initial state of the local CPPS model is

Fig. 4 Deployment of CFCA early warning model

Fig. 5 Structure of local CPPS model

a normal operation and there are three types of disturbances that could be selected, such as cutting-off generator, reducing generator output by half, and cutting of bus.

In Table 1, the concealed factor C_C^1 is obtained using the actual detection results of the improved ball vector machine (IBVM) IDS, and the implementation factor C_I^1 can be calculated via the actual historical data [31]. Denial of service (DoS) attacks need to attack the targets continuously to paralyze the serving function, and hence their duration factor C_T^1 approaches 1. While the duration time of exploited attacks, which control the targets and send exploited commands, are usually several minutes, the buffer overflow attack, which usually lasts approximately 2 min, is selected as the practical attack in this case. The DoS attacks could paralyze the power secondary functions; therefore, the harm factor G_F^1 of DoS attacks is 1. However, calculating the harm factor G_F^1 of exploited attacks needs to consider both the actual attack targets and ways. If power secondary device outage is the attack target, then the harm factor G_F^1 is 1; but if the generator output is reduced by half by cyberattacks, the harm factor G_F^1 is 0.5.

As seen from Table 2, the secondary power system hidden faults always exist until removed, and their duration factor C_T^2 approaches 1; however, the duration time of secondary power system overt faults is usually less than 1 s, and their C_T^2 is 0.3679. To simplify the calculation, all C_P^2 are set to 1. The factor G_P^2 is respectively calculated for different cases: in the case of cutting-off G9, the G_P^2 is 0.134; in the case of reducing G9 output by half, the G_P^2 is 0.067; in the case of cutting off Bus 29, the generator output is not affected due to Bus 29 change and the G_P^2 is 0. All priority probabilities of CFCA are listed in Table 3. However, probabilities of other CFCA, whose AGCP ratio

Fig. 6 Power plant with smart substation simulation platform

Table 1 The q of each directed edge from L_1 layer to L_2 layer

Sub-attack route	C_C^1	C_I^1	C_T^1	G_F^1	$q_{x,\beta}^1$
$V_1 \rightarrow V_4$	0.9780	0.9035	0.9999	1	2.8814
$V_1 \rightarrow V_5$	0.9780	0.9035	0.9999	1	2.8814
$V_1 \rightarrow V_8$	0.9780	0.9035	0.9999	1	2.8814
$V_2 \rightarrow V_3$	0.7794	0.0965	0.9917	0.5	3.7352
$V_2 \rightarrow V_4$	0.7794	0.0965	0.9917	0.5	3.7352
$V_2 \rightarrow V_5$	0.7794	0.0965	0.9917	1	1.8676
$V_2 \rightarrow V_6$	0.7794	0.0965	0.9917	0.5	3.7352
$V_2 \rightarrow V_7$	0.7794	0.0965	0.9917	0.5	3.7352
$V_2 \rightarrow V_8$	0.7794	0.0965	0.9917	1	1.8676

Q is close to infinity, are ignored in this experiment (such as the “ $V_2 \rightarrow V_5 \rightarrow V_{10}$ ” attack route), and their priority probabilities are 0 because their occurrence requires external conditions in which the operating state of the local CPPS model has changed.

5.3 Simulation and early warning CFCA

A typical CFCA “ $V_2 \rightarrow V_3 \rightarrow V_9$ ” has been simulated in the local CPPS model and is set as the normal state. Assume that there is no technical limitation for attackers on the cyberattack platform.

1) “Before the event” – cyberattack preparation phase. To explore the location of cyberattack target, the cyberattack platform uses the IP and port scanning tool to gather the network information related to the power plant simulation platform. The messages intercepted by the early

Table 2 The q of each directed edge from L_2 layer to L_3 layer

Sub-attack route	C_C^2	C_P^2	C_T^2	G_C^2	G_F^2	$q_{\beta,\gamma}^2$
$V_3 \rightarrow V_9$	1	1	0.3679	1	0.1340	17.6709
$V_3 \rightarrow V_{10}$	1	1	0.3679	1	0.0670	35.3418
$V_3 \rightarrow V_{11}$	1	1	0.3679	1	0	$+\infty$
$V_3 \rightarrow V_{12}$	1	1	0.3679	1	0	$+\infty$
$V_4 \rightarrow V_9$	1	1	0.9999	0	0.1340	$+\infty$
$V_4 \rightarrow V_{10}$	1	1	0.9999	0	0.0670	$+\infty$
$V_4 \rightarrow V_{11}$	1	1	0.9999	0	0	$+\infty$
$V_4 \rightarrow V_{12}$	1	1	0.9999	0	0	$+\infty$
$V_5 \rightarrow V_9$	0	1	0.9999	0	0.1340	$+\infty$
$V_5 \rightarrow V_{10}$	0	1	0.9999	0	0.0670	$+\infty$
$V_5 \rightarrow V_{11}$	0	1	0.9999	0	0	$+\infty$
$V_5 \rightarrow V_{12}$	0	1	0.9999	0	0	$+\infty$
$V_6 \rightarrow V_9$	1	1	0.3679	1	0.1340	17.6709
$V_6 \rightarrow V_{11}$	1	1	0.3679	1	0	0
$V_7 \rightarrow V_9$	0	1	0.9999	0	0.1340	$+\infty$
$V_7 \rightarrow V_{11}$	0	1	0.9999	0	0	$+\infty$
$V_8 \rightarrow V_9$	0	1	0.9999	0	0.1340	$+\infty$
$V_8 \rightarrow V_{11}$	0	1	0.9999	0	0	$+\infty$

warning model are shown in Appendix A Table A1. Since a substantial cyberattack did not form at this stage, the early warning model did not generate any alarm.

2) “During the event” – CFCA formation phase. After determining the network location of the operator station, the cyberattack platform performs a buffer overflow attack to obtain the operator station control right, to realize

Table 3 Priority order of attack routes in local CPPS model

Attack route (CFCA)	AGCP ratio Q	Variance q	Dam	“1 st -2 nd -3 rd ” principles	$P_x^{(1)}$ (%)	P_x^* (%)
$V_2 \rightarrow V_3 \rightarrow V_9$	21.4061	97.1019	0.1340	1 st	39.24	39.24
$V_2 \rightarrow V_3 \rightarrow V_{10}$	39.0770	499.4886	0.0670	2 nd	21.52	21.52
$V_2 \rightarrow V_6 \rightarrow V_9$	21.4061	97.1019	0.1340	1 st	39.24	39.24

remote control. Part of attack messages intercepted by the early warning model are shown in Appendix A Table A2. At this time, the remote malicious attack at the operation station has been detected by the early warning model. In addition, the early warning model determines which type of CFCA would occur based on a joint inference of Fig. 1 and the probability. There are two types of CFCA that may occur at the operation station. One is the CFCA “ $V_2 \rightarrow V_3 \rightarrow V_9$ ” with a 39.24% probability, and the other is the CFCA “ $V_2 \rightarrow V_3 \rightarrow V_{10}$ ” with a 21.52% probability. As a result, the early warning model gives an alarm of CFCA “ $V_2 \rightarrow V_3 \rightarrow V_9$ ” for a protective action. However, there no attack-blocking measures that have been taken to fully demonstrate the consequences of CFCA. Finally, to trigger an “ $N-1$ ” disturbance, the operator station sends a wrong instruction to cut off G9.

3) “After the event” – damage diffusion phase. After an “ $N-1$ ” disturbance is formed, power flow transfer occurs, as shown in Table 4, without line loss.

5.4 Experimental results

1) Attackers play the leading role in the CFCA process and could actively choose the most favorable CFCA. Cyberthreats endanger normal operation of a power system under attacker continuity driving.

2) The outbreak of CFCA is subject to many external conditions; therefore, many CFCAs with great harm may not happen. CFCA requires attackers own some certain knowledge and technical skill, while the attackers lack of technology can only select and implement limited types of CFCAs. Meanwhile, fewer types of CFCAs could directly occur without external conditions’ limitation. The CFCA needs the change of power systems’ state, such as “ $V_2 \rightarrow V_7 \rightarrow V_9$ ”.

Table 4 A part of power transfer before and after CFCA

Element	Power before CFCA (MW)	Power after CFCA (MW)
Bus 25-Bus 26	76.65	443.90
Bus 26-Bus 27	268.49	−196.35
Bus 26-Bus 28	−140.82	272.83
Bus 26-Bus 29	−190.18	222.50
Bus 28-Bus 29	−347.61	63.76
Bus 29-Bus 38	−824.77	0.00

3) The attacker deciding process could be clearly described based on AGCP. On the one hand, the priority order based on AGCP reflects the working principle that attackers reasonably select the optimal attack route; on the other hand, it makes the CFCA occurrence close to the actual situation and the probability of CFCA can be qualified based on AGCP.

4) During the “before the event” and “during the event” phase, the early warning model could timely detect cyberattacks that can deduce power system faults, and provide the type and probability of CFCA to help operators prevent serious damage in time.

6 Conclusion

To enhance CPPS’ security protection level, CFCA was comprehensively studied based on AGCP from the view of attackers. Firstly, the priority order of CFCA was discussed and calculated based on AGCP. Secondly, the calculation method of the probability of CFCA was proposed and how to choose the optimal attack route under different technical level is discussed. Thirdly, an effective CFCA early warning model was proposed. Finally, a typical CFCA was simulated in the local CPPS model and the test results verify the effectiveness of the proposed method. The optimal attack strategy formulation including the coordinated attack and protection technology considering the dynamic game theory between attackers and defenders will be our future work.

Acknowledgements This work was supported by the National Key Research and Development Program of China (No. 2017YFB0903000), National Natural Science Foundation of China (No. 61471328), and Natural Science Foundation of Tianjin City (No. 15JCQNJC07000).

Open Access This article is distributed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made.

Appendix A

The messages intercepted by the early warning model are shown in Table A1.

Table A1 Messages of IP and sort scanning

No.	Time (s)	Source	Destination	Protocol	Length (B)	Information
26	1.7983	LcfcHefe_03:b5:71	Broadcast	ARP	60	Who has 192.168.1.9? Tell 192.168.1.16
27	1.7983	LcfcHefe_03:b5:71	Broadcast	ARP	60	Who has 192.168.1.10? Tell 192.168.1.16
28	1.7983	LcfcHefe_03:b5:71	Broadcast	ARP	60	Who has 192.168.1.11? Tell 192.168.1.16
29	1.7986	LcfcHefe_03:b5:71	Broadcast	ARP	60	Who has 192.168.1.12? Tell 192.168.1.16
30	1.7986	LcfcHefe_03:b5:71	Broadcast	ARP	60	Who has 192.168.1.13? Tell 192.168.1.16
31	1.7987	192.168.1.16	192.168.1.14	ICMP	98	Echo (ping) request id=0x0200,seq=12032/47,ttl=63(reply in 34)
32	1.7987	192.168.1.16	192.168.1.14	ICMP	98	Echo (ping) request id=0x0200,seq=12288/48,ttl=63
33	1.7991	192.168.1.16	192.168.1.14	ICMP	98	Echo (ping) request id=0x0200,seq=12800/50,ttl=63(reply in 35)

Table A2 Messages of remote malicious control

No.	Time (s)	Source	Destination	Protocol	Length (B)	Information
2374	174.9902	192.168.1.1	192.168.1.17	PRES	130	DATA TRANSFER(DT) SPDU
2375	174.9948	192.168.1.17	192.168.1.1	COTP	1082	DT TPDU (0) [COTP fragment, 1021 bytes]
2376	174.9951	192.168.1.17	192.168.1.1	COTP	1082	DT TPDU (0) [COTP fragment, 1021 bytes]
2377	174.9951	192.168.1.1	192.168.1.17	TCP	60	32863 > iso-tsap [ACK] Seq=394 Ack=9842 Win=49640 Len=0
2378	174.9959	192.168.1.17	192.168.1.1	PRES	622	DATA TRANSFER(DT) SPDU
2379	175.0457	192.168.1.17	192.168.1.1	PRES	84	DATA TRANSFER(DT) SPDU
2380	175.0458	192.168.1.1	192.168.1.17	TCP	60	32863 > iso-tsap [ACK] Seq=394 Ack=10440 Win=49640 Len=0
2381	175.0480	192.168.1.17	192.168.1.1	PRES	188	DATA TRANSFER(DT) SPDU
2382	175.0506	192.168.1.1	192.168.1.17	PRES	133	DATA TRANSFER(DT) SPDU
2383	175.0935	192.168.1.17	192.168.1.1	TCP	60	32863 > iso-tsap [ACK] Seq=10574 Ack=473 Win=8113 Len=0

Part of attack messages intercepted by the early warning model are shown in Table A2.

References

- [1] Ilic MD, Xie L, Khan UA et al (2010) Modeling of future cyber-physical energy systems for distributed sensing and control. *IEEE Trans Syst Man Cybernet* 40(4):825–838
- [2] Adhikari U, Morris TH, Pan S (2014) A cyber-physical power system test bed for intrusion detection systems. In: *Proceedings of IEEE PES general meeting, Harbor, USA, 27–31 July 2014*, 5 pp
- [3] Bogdan P, Marculescu R (2011) Cyberphysical systems: workload modeling and design optimization. *IEEE Des Test Comput* 28(4):78–87
- [4] Zhao JH, Wen FS, Xue YS et al (2010) Cyber physical power systems: architecture, implementation techniques and challenges. *Autom Electr Power Syst* 34(16):1–7
- [5] Liu D, Sheng WX, Wang Y et al (2015) Key technologies and trends of cyber physical system for power grid. *Proc CSEE* 35(14):3522–3531
- [6] Kim KD, Kumar PR (2012) Cyber-physical systems: a perspective at the centennial. *Proc IEEE* 100:1287–1380
- [7] Zeller M (2011) Myth or reality—does the Aurora vulnerability pose a risk to my generator? In: *Proceedings of 64th annual conference for protective relay engineers, Texas, USA, 11–14 April 2011*, 7 pp
- [8] Langner R (2011) Stuxnet: dissecting a cyberwarfare weapon. *IEEE Secur Priv* 9(3):49–51
- [9] Guo QL, Xin SJ, Wang JH et al (2016) Comprehensive security assessment for a cyber physical energy system: a lesson from Ukraine's blackout. *Autom Electr Power Syst* 40(5):145–147
- [10] Zhao JH, Liang GQ, Wen FS et al (2016) Lessons learnt from Ukrainian blackout: protecting power grids against false data injection attacks. *Autom Electr Power Syst* 40(7):149–151
- [11] Liu N, Yu XH, Zhang JH (2016) Coordinated cyber-attack: inference and thinking of incident on Ukrainian power grid. *Autom Electr Power Syst* 40(6):144–147
- [12] Xue YS (2003) The way from a simple contingency to system-wide disaster—lessons from the eastern interconnection blackout in 2003. *Autom Electr Power Syst* 27(18):1–5
- [13] Mei SW, Wang YY, Chen LJ (2011) Overviews and prospects of the cyber security of smart grid from the view of complex network theory. *High Volt Eng* 37(3):672–679
- [14] Cao YJ, Zhang YD, Bao ZJ et al (2013) Analysis of cascading failures under interactions between power grid and communication network. *Electr Power Autom Equip* 33(1):7–11
- [15] Wang YF, Yan Z, Wang J (2015) The cross space transmission of cyber risks in electric cyber-physical systems. In:

- Proceedings of 11th international conference on natural computing, Zhangjiajie, China, 15–17 August 2015, 5 pp
- [16] Su S, Wu CJ, Ma J et al (2014) Attacker's perspective based analysis on cyber attack mode to cyber-physical system. *Power Syst Technol* 38(11):3115–3120
  - [17] Liu S, Chen B, Takis Z et al (2014) A coordinated multi-switch attack for cascading failures in smart grid. *IEEE Trans Smart Grid* 5(3):1183–1195
  - [18] Chen B, Butler K, Kundur D (2013) Impact analysis of transient stability due to cyber attack on FACTS devices. *N Am Power Symp* 1:1–6
  - [19] Law Y, Alpcan T, Palaniswami M (2015) Security games for risk minimization in automatic generation control. *IEEE Trans Power Syst* 30(1):223–232
  - [20] Zhang YC, Wang LF, Xiang YM et al (2015) Power system reliability evaluation with SCADA cybersecurity considerations. *IEEE Trans Smart Grid* 6(4):1–15
  - [21] Vellaithurai C, Srivastava A, Zonouz S et al (2015) CPIndex: cyber-physical vulnerability assessment for power-grid infrastructures. *IEEE Trans Smart Grid* 6(2):566–575
  - [22] Srivastava A, Morris T, Ernster T et al (2013) Modeling cyber-physical vulnerability of the smart grid with incomplete information. *IEEE Trans Smart Grid* 4(1):235–244
  - [23] Chen T, Sanchez-Aarnoutse J, Buford J (2011) Petri net modeling of cyber-physical attacks on smart grid. *IEEE Trans Smart Grid* 2(4):741–749
  - [24] Han YQ, Guo CX, Zhu BQ et al (2016) Model cascading failures in cyber physical power system based on improved percolation theory. *Autom Electr Power Syst* 40(17):30–37
  - [25] Wang YF, Qiu J, Zhao T (2016) Evaluating the harmfulness of cascading failures across space in electric cyber-physical systems. *J Comput Theor Nanosci* 13(11):8844–8853
  - [26] Li WG, Deng SG, Li JS et al (2013) Defense strategy of cascading failures between information network and physical power grid. *High Volt Eng* 39(11):2714–2720
  - [27] Shi LB, Jian Z (2016) Vulnerability assessment of cyber physical power system based on dynamic attack-defense game model. *Autom Electr Power Syst* 40(17):99–105
  - [28] Ouyang M (2012) The research on the assessment of the attack resistances based on the attack cost and attack effect. Dissertation, Beijing University of Posts and Telecommunications
  - [29] Evans S, Waller J (2015) Risk-based security engineering through the eyes of the adversary. In: *Proceedings of 6th annual IEEE systems, man and cybernetics information assurance workshop*, New York, USA, 15–17 June 2005, 8 pp
  - [30] Xue YS, Ni M, Yu WJ et al (2016) Power grid blackout defense system including communication/information security early warning and decision support. *Autom Electr Power Syst* 40(17):3–12
  - [31] Wang YF, Zhao T, Li SY et al (2013) An intrusion detection method for electric power information network based on improved minimum enclosing ball vector machine. *Power Syst Technol* 37(9):2675–2680
  - [32] Gao KL, Liu JM, Xu RZ et al (2011) A hybrid security situation prediction model for information network based on support vector machine and particle swarm optimization. *Power Syst Technol* 35(4):176–182

Yufei WANG obtained his master degree from the North China Electric Power University in 2012. He is now a Ph.D. student at Wuhan University and an engineer of Global Energy Interconnection Research Institute. His research interests include cyber-physical power systems, cybersecurity, and machine learning.

Yanli LIU obtained her Ph.D. degree from Tianjin University in 2014. She is now an associate professor with Tianjin University. Her research interests include power system stability and security, cyber-physical systems, and renewable energy.

Jun'e LI obtained her Ph.D. degree from Wuhan University in 2004. She is now a professor of Computer Science & Technology at Wuhan University. Her research interests include computer network architecture, cybersecurity, and cyber-physical systems.