Two Attacking Strategies of Coordinated Cyber-Physical Attacks for Cascading Failure Analysis in Smart Grid

WenJie Kang[1,2,3,4(✉)]

[1] Information Technology (Internet Supervision) Department, Hunan Police Academy, Changsha, China
kangwenjiebishen@126.com

[2] School of Electronic Information and Electrical Engineering, Changsha University, Changsha, China

[3] College of Systems Engineering, National University of Defense Technology, Changsha, China

[4] Key Laboratory of Hunan Province for New Retail Virtual Reality Technology, Hunan University of Technology and Business, Changsha, China

Abstract. As a classic Cyber-Physical System (CPS), smart grids often suffer from various types of attacks, one of which the most threatening attacks is Coordinated Cyber-Physical Attack (CCPA). In order to improve the robustness of the smart grid under CCPA, two attack strategies are proposed to analyze the cascading failure of smart grids. Firstly, we define attack goals (AGs) function to identify important cyber and physical nodes as possible targets. Secondly, based on these targets, the algorithm of optimal attack and saturation attack strategy is designed and applied to CCPA for analyzing the effect of those attack strategies on smart grids. Finally, node loss is used as an evaluation index to compare the attack effect of CCPA, Cyber Attack (CA) and Physical Attack (PA). The experimental results show that when the same proportion of nodes are removed, the CCPA has more node losses than the CA and PA, regardless of based on the optimal attack strategy or the saturation attack strategy.

Keywords: Smart grids · Attack goals (AGs) · Coordinated Cyber-Physical Attack · Attacking strategy

Supported by National Natural Science Foundation of China under Grant Nos. 61501482, 61572514, 61903049 and 61702539, Scientific Research Fund of Hunan Provincial Education Department (19C0160 and 20B057), Open Fund of Key Laboratory of Hunan Province (2017TP1026), Hunan Key Laboratory Open Research Fund Project 2017TP1026, Hunan Provincial Natural Science Foundation of China under Grant No. 2018JJ3611, Changsha Science and Technology Program (Grant K1705007) and NUDT Research Project under Grant No. ZK-18-03-47.

X. Wang et al. (Eds.): 6GN 2020, LNICST 337, pp. 384–396, 2020.
https://doi.org/10.1007/978-3-030-63941-9_29

1 Introduction

The fifth-generation (5G) contributions to meet the requirements of data transmission and real-time state perception of industrial control network. Moreover, the next-generation (B5G/6G) will address the major opportunities and face new challenges, not only to create more new technologies, protocols and applications, but also to bring more security risks, such as coordinated cyber-physical attacks, cross-layer attacks etc. On the one hand, attackers can use acquired knowledge of target network to carry out cross-layer attacks on the Cyber-Physical Systems from the information domain to the physical domain; On the other hand, attackers can cooperate with each other and use their own resources to launch multi-directional and multi-target cyber-physical attacks; The study of cross-layer attack has completed in [1]. This paper will analyze the impact of CCPA combined with different attack strategies on the cascading failures of smart grid.

An incident in 2015 involving Ukrainian power systems was seen as a coordinated cyber-attack (CCA), where attackers injected malicious commands into the cyber domain, causing a breakdown in the physical domain for several hours [2]. Continuous attacks on Venezuelan power grid on March 7 and 8, 2019 resulted in power supply interruptions in 18 states across the country, which has once again caught the attention of scientists. As a major threat to the ICT infrastructure of power systems [3], CCAs are described as an organized cyber disruption, in which the attackers may have a well-organized plan to launch multiple cyber-attacks intended to compromise the same target [2].

With the increasing prevalence of terrorism and sabotage activities, the power grid is becoming more vulnerable to various kinds of cyber and physical attacks [4]. In the future, the attackers may launch cyber and physical attacks at the same time and collaborate to finish the task by sharing the same (multiple) targets and attacking them simultaneously. Coordinated cyber-physical attacks (CCPAs) on smart grids could lead to undetectable line outages, leading to a need for topology preservation and load-redistribution attacks that trigger cascading failures [5]. An exploration of potential attack goals (AGs) will contribute to clarifying the target, rather than blindly anticipating attack strategies. A coordinated cyber-physical attack following these AGs will maximize the destruction.

Liu et al. [6] proposed a framework that models a class of cyber-physical switching attack in smart grid systems to demonstrate how attack construction on a linearized version of the system still executes on nonlinear and realistic models of the system. Deng et al. [7] proposed CCPAs in smart grid by utilizing cyber attacks to mask physical attacks which can lead to power outages and potentially cause cascading failures. CCPAs used a false data injection attack vector based on phasor measurement unit (PMU) to avoid physical attacks being detected. The mathematical model of locally coordinated cyber-physical attacks is proposed to use incomplete network information in order to cause undetectable transmission line outages [8]. Liu et al. [9] developed coordinated cyber-physical attack based on variable structure systems theory to enable large-scale power system disturbances. Since CCPAs on its critical infrastructure can cause disastrous human and economic losses, a stochastic game-theoretic approach is proposed to generate the optimal strategies that defenders can adopt to pro-

tect the smart grid against CCPAs [10]. Tian et al. [11] investigated Multilevel Programming-Based CCPAs and the countermeasure with one leader and multiple followers in smart grid. Lakshminarayana et al. [12] proposed a moving target defense (MTD) strategy to detect coordinated cyber-physical attacks (CCPAs) that consists of a physical attack and followed by a coordinated cyber attack.

The rest of the paper is organized as follows. Section 1 introduces the model of coordinated cyber-physical attacks that contains identification evaluation of cyber and physical attack goal, CCPA based on optimal attack strategy and CCPA based on saturation attack strategy. Section 2 shows the experimental results and analyzes the reasons for the results. Finally, Sect. 3 draws relevant conclusions and presents future work.

1.1 Identification of Cyber and Physical Attack Goals (AGs) [13]

In order to generate an attack sequence of CCPA, the first thing to do is to identify the cyber AGs and physical AGs. As a characteristic of the power grid, power flow can cause the redistribution of voltage and frequency following the breakdown or failure of a substation. Therefore, physical AGs not only rely on the power flow, but also depends on the characteristic of network structure. Due to the coupling relationship, cyber AGs are mainly related to its coupled physical AGs, degree and dependency.

When analyzing the power-flow process, we ignore the internal complex changes in the power system and directly analyze the results by using active power P and reactive power Q as the load of the substations. When the load $L_i = \sqrt{P_i^2 + Q_i^2}$ of a substation i is over a certain threshold range $[(1-\alpha)*L_i, (1+\alpha)*L_i]$, it will fail due to overload. However, the threshold value relies on the capacity of the network and reflects the robustness of the network itself. This means that an overloaded or underloaded substation will malfunction, triggering the load redistribution again. By simulating attacker behavior, it is possible to reveal which substations are likely to cause more substation failure; in this way, these substations can easily be highlighted as AGs. The malfunction condition of a substation occurs when the substation's load exceeds the network's capacity.

The impact of nodes is used to describe the importance of each substation. A larger impact represents a failed node can cause more node failures. Therefore, Failure Node Set (FNS) is defined as a collection of failed nodes caused by the failure of a substation k, which is used to evaluate the impact of the failed substation k. Differences in parameter α may result in a different FNS. We use Formula 1 to assess the impact of the substations and adopt the average of IM under all tolerance parameters in order to evaluate physical AGs.

$$IM_i^{\alpha_j} = \begin{cases} n(FNS_i^{\alpha_j}), FNS_i^{\alpha_j} = FNS_{Max}^{\alpha_j} \\ n(FNS_i^{\alpha_j}) - n(FNS_{Max}^{\alpha_j} \bigcap FNS_i^{\alpha_j}), otherwise \end{cases} \tag{1}$$

where $n(FNS_i^{\alpha_j})$ represents the size of FNS of substation i under tolerance parameter α_j. $FNS_{Max}^{\alpha_j} \bigcap FNS_i^{\alpha_j}$ is the intersection of $FNS_{Max}^{\alpha_j}$ and $FNS_i^{\alpha_j}$. If FNS of substation i is contained by a maximum FNS, it is insignificant and will

not be used as an attack goal. It means that a substation with a larger $n(FNS_i)$ and a smaller $n(FNS_{Max} \bigcap FNS_i)$ has a bigger probability of node i being attacked. Hence, the probability of nodes being physical AGs is described as:

$$Prob_i^P = \mu * \frac{ID_i^+}{ID_i^-} * \frac{1}{M} \sum_{j=1}^{M} Im_i^{\alpha_j} \tag{2}$$

where $Prob_i^P$ denotes the probability that substation i will be selected as an AG for the power grid, and ID_i^+ and ID_i^- represent dependence out-degree and dependence in-degree of node i, respectively. α_j denotes a tolerance parameter j that reflects the capacity of the network to deal with overload. M denotes the number of tolerance parameters.

The ultimate goal of the attackers is to destroy physical devices, and they may select cyber AGs in order to control the failure of these physical AGs. Because the coupling relationship is the same, we will use Formula 1 as the function of AGs in the communication network.

Due to the coupling relationship, cyber nodes that control key substations become more important. The large-degree nodes are usually transfer stations for information collection and data transmission via the communication network and are of great significance to network security. As such, these factors should be taken into account when calculating the probability of nodes being cyber AGs in a communication network:

$$Prob_i^C = \mu * \frac{ID_i^+}{ID_i^-} * \frac{D_i}{D_{Max}} * \sum_{CR_{ij}=1} Prob_j^P \tag{3}$$

where $Prob_i^C$ represents the probability that cyber node i will be an AG in a communication network. D_i denotes the degree of node i, while D_{Max} is the maximum value of the degree of all nodes. $CR_{ij} = 1$ represents a coupling link from cyber node i to physical node j.

Based on the probability of nodes being AGs, the attacker may choose the cyber and physical nodes with higher probability as the target of CCPA. By simulating the CCPA scenarios in real situations, we design two attack strategies: optimization attack strategy (OAS) and saturation attack strategy (SAS). The OAS is to select the least AGs to maximize the attack effect when attacking the same number of AGs. The SAS is to cover every cyber and physical AGs without redundant attack, and select the least number of AGs to make the attack achieve the effect of attacking all AGs. Cyber attack (CA) refers to the invasion, attack and destruction of important nodes in information system by means of information technology. However, Physical attack (PA) refers to the use of violent means, special tools or weapons to destroy important power stations in the power network one by one.

1.2 CCPA Based on Optimal Attack Strategy

The optimal attack strategy for coordinated cyber physical attacks is to find the optimal attack sequence and achieve the effect of exceeding cyber attacks

or physical attacks. The CCPA based on optimal attack strategy algorithm is designed to generate attack sequences by searching for cyber or physical AGs. From the perspective of the attack effect, the number of nodes in attack sequence is less than that of cyber attack or physical attack, and its attack effect is better than that of cyber attack and physical attacks.

We design the objective function $Max\{*\}$ of the OAS to satisfy the conditions of formulas (5)–(9). The purpose of formula (4) is to find the attack sequence with the best attack effect when attacking the same number of AGs. Formula (5) represents the same number of cyber and physical nodes being attacked, which is a constant.

$$Max(OA(t^P + t^C)) = Max(f^P + f^C) \tag{4}$$

s.t.

$$num(t^P + t^C) = m \tag{5}$$

$$0 < num(t^P) \leq N \tag{6}$$

$$0 < num(t^C) \leq N \tag{7}$$

$$OA(t^P + t^C) \geq PA(t_1^P), num(t_1^P) = m \tag{8}$$

$$OA(t^P + t^C) \geq CA(t_1^C), num(t_1^C) = m \tag{9}$$

Where f^P and f^C represent the number of failed physical nodes and failed cyber nodes, respectively. t^P and t^C denote the set of the physical and cyber AGs, respectively. m is the number of cyber and physical AGs. $num(*)$ denotes the number of $*$. $OA(*)$, $CA(*)$ and $PA(*)$ represent the attack effect of CCPA Based on optimal attack strategy, cyber attack and physical attack of $*$, respectively. t_1^* represents a set of $*$ different from t^*.

The main steps of Algorithm 1 are as follows:

Step 1: Initialization. The first N cyber AGs are taken as the cyber candidate sequence CyberAGs in order of degree. The first L physical AGs are taken as the physical candidate sequence PhysicalAGs, and the coupling relationship matrix CR_{ij} is obtained.

Step 2: Traverse all nodes of the physical candidate sequence. If there are cyber nodes coupled with it that belong to the information candidate sequence CyberAGs, then remove these nodes from the CyberAGs, named as delete-CyberAGs( ).

Step 3: Traversing the cyber candidate sequence CyberAGs, if the CyberAGs contains nodes AG_i^P and meets the condition of $CR_{AG_i^C AG_j^P} = 1$, and then removing them from the physical candidate sequence PhysicalAGs.

Step 4: Cyber physical attack sequence: attacksequence is equal to Cyber-AGs+PhysicalAG

Algorithm 1: The CCPA based on optimal attack strategy is used to identify the attack sequence of cyber and physical AGs.

Input: $AG^P = (p_1, p_2, ..., p_m)$,$D^C$,$CR_{ij}$,$L$
Output: attacksequence
deletecyberAGs ← null
deletephysicalAGs ← null
cyberAGs ← null
physicalAGs ← null
attacksequence ← null
for $i = 1;i < N;i++$ **do**
  cyberAGs.add(D_i^C)
  physicalAGs.add(AG_i^P)
end
for $i = 1;i < N;i++$ **do**
  for $i = 1;i < L;i++$ **do**
    if $CR_{ij} == 1$ **then**
      deletecyberAGs.add(AG_j^C)
    end
  end
end
cyberAGs.removeAll(deletecyberAGs)
for $i = 0;i < N;i++$ **do**
  for $j = 0;j < L;j++$ **do**
    if *cyberAGs.contain*(AG_j^C) && $CR_{ji} == 1$ **then**
      deletephysicalAGs.add(AG_i^P)
    end
  end
end
physicalAGs.removeAll(deletephysicalAGs)
attacksequence ← cyberAGs + physicalAGs

1.3 CCPA Based on Saturation Attack Strategy

A saturation attack strategy of CCPA involves an attack sequence of cyber and physical AGs. Saturation attacks strategy cover the whole range of AGs, excluding repeated attacks. Such an attack sequence does not contain redundant attacks where the same AG is repeatedly attacked or where two AGs are attacked to produce the same attack effect.

We design the objective function $Min\{*\}$ of the SAS to satisfy the conditions of formulas (11)–(15). The purpose of formula (10) is to find the attack sequence of the least number of AGs to make the attack achieve the effect of attacking all AGs without redundant attack.

$$Min(num(t^P + t^C)) \tag{10}$$

s.t.

$$SA(t^P + t^C) = PA(t_2^P) + CA(t_2^C) \tag{11}$$

$$0 < t^P \leq N \tag{12}$$

$$0 < t^C \leq N \tag{13}$$

$$num(t_2^P) = m \tag{14}$$

$$num(t_2^C) = m \tag{15}$$

Where f^P and f^C represent the number of failed physical nodes and failed cyber nodes, respectively. t^P and t^C denote the set of the physical and cyber AGs, respectively. m is the number of cyber and physical AGs. $num(*)$ denotes the number of $*$. $SA(*)$, $CA(*)$ and $PA(*)$ represent the attack effect of CCPA Based on saturation attack strategy, cyber attack and physical attack of $*$, respectively. t_2^* represents a set of $*$ different from t^*.

CCPA based on saturation attack strategy is an attack mode that covers all attack goals, and it eliminates redundant attacks and repeated attacks. A redundant attack means that two different attack targets produce the same attack effect, and a repeated attack means that one target is attacked multiple times. Algorithm 2 describes the attack sequence generation process for a saturated attack. The steps are as follows:

Step 1. Initialization n cyber AGs, cyber candidate sequence CyberAGs=null, the first n physical AGs, physical candidate sequence PhysicalAGs=null, the coupling relationship matrix CR_{ij} is obtained.
Step 2. Traversing all the nodes of the cyber candidate sequence CyberAGs, traversing all the nodes of the physical candidate sequence PhysicalAGs, if the condition meets $CR_{AG_i^C AG_j^P} = 1$, removing the physical node j from the deleteAGs and removing failure node set getFNS(AG_j^P) that contains physical node j from the node set deleteAGs.
Step 3. Traverse all the remaining nodes of the physical candidate sequence PhysicalAGs. If the deleteAGs does not contain nodes AG_j^C, the physical candidate sequence PhysicalAGs will be added.
Step 4. Cyber physical attack sequence: attacksequence is equal to $CyberAGs + PhysicalAGs$.

2 Experiments and Analysis

In order to verify the effectiveness of CCPA based on different attack strategies, we used a fraction of the practical smart grid as experimental data. The smart grid consists of power grid and communication network, in which cyber nodes are coupled with physical nodes by two-way coupling link with one-to-one corresponding. Figure 1(a) shows that the power grids is composed of 154 substations and 192 transmission lines. Here, square nodes represent generators and circular nodes represent substations. The communication network is constructed by 154 cyber nodes and 153 communication lines in Fig. 1(b), in which the control centers are represented by square nodes and monitoring/controlling nodes are represented by circular nodes.

Algorithm 2: The CCPA based on saturation attack strategy is used to identify the attack sequence of cyber and physical AGs.

Input: $AG^P = (p_1, p_2, ..., p_m)$,$AG^C = (c_1, c_2, ..., c_n)$, CR_{ij}
Output: attacksequence
deletephysicalAGs ← null
cyberAGs ← null
physicalAGs ← null
attacksequence ← null
for $i = 1;i < AG^C.length;i++$ **do**
  cyberAGs.add(D_i^C)
  for $j = 0;j < AG^P.length;j++$ **do**
    if $CR_{ij} == 1$ **then**
      deletephysicalAGs.add(AG_j^P)
      deletephysicalAGs.addAll(getFNS(AG_j^P))
    end
  end
end
for $j = 0;j < AG^P.length;j++$ **do**
  if *!deletephysicalAGs.contain(*AG_j^P*)* **then**
    physicalAGs.add(AG_j^P)
  end
end
attacksequence ← cyberAGs + physicalAGs

No matter what attack strategy or method is adopted, the first thing an attacker has to do is to identify the attack goals. In order to achieve the desired attack effect, the appropriate attack goals should be chosen based on different attack strategies. According to the formula (2), we can get the probability of substations being physical AGs in Fig. 2(a). The greater the probability of the node, the easier it is to be selected as the target of attack. Similarly, the probability of cyber nodes being AGs can be computed by the formula (3) in Fig. 2(b). In the case of limited attack resources, an attacker may select a certain proportion of nodes as attack goals according to his own situation.

The optimal attack strategy is to find an optimal attack sequence when the same proportion of nodes are attacked, so that the attack effect of CCPA is better than other attacks under the same conditions. Figure 3(a) shows that the network layers and distribution of physical and cyber AGs. Labels "C" and "P" represent cyber and physical AGs, respectively. The x-axis represents the distribution of cyber or physical AGs between nodes 1 and 154. We assume that 10% of nodes are selected as targets in the case of limited resources, so 15 cyber AGs and 15 physical AGs can be found by Algorithm 1. The attack sequence consists of cyber AGs and Physical AGs. When the same proportion of nodes are attacked, the CCPA based on OAS has a significantly better attack effect than PA and CA, as shown in Fig. 3(b).

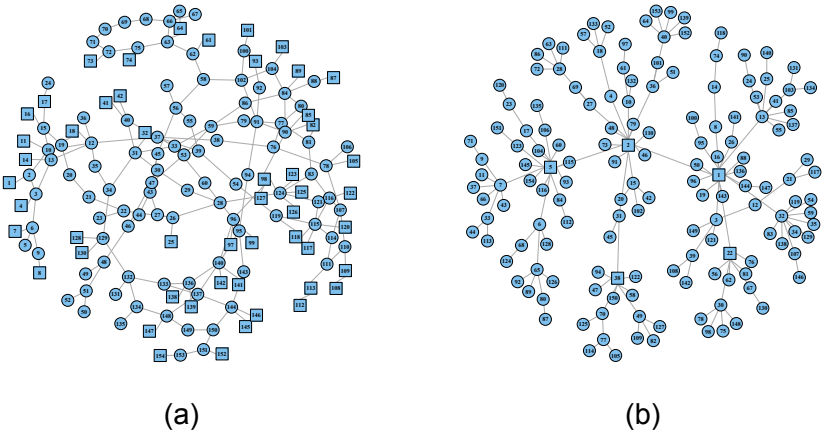

Fig. 1. The network structure diagram of smart grid. (a) Power grid. (b) Communication network.

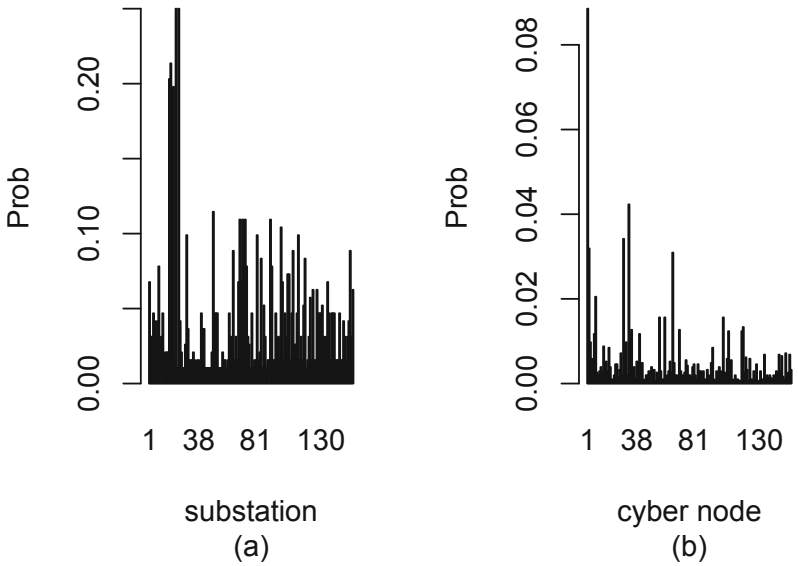

Fig. 2. (a) The probability of substations being physical AGs. (b) The probability of nodes being cyber AGs.

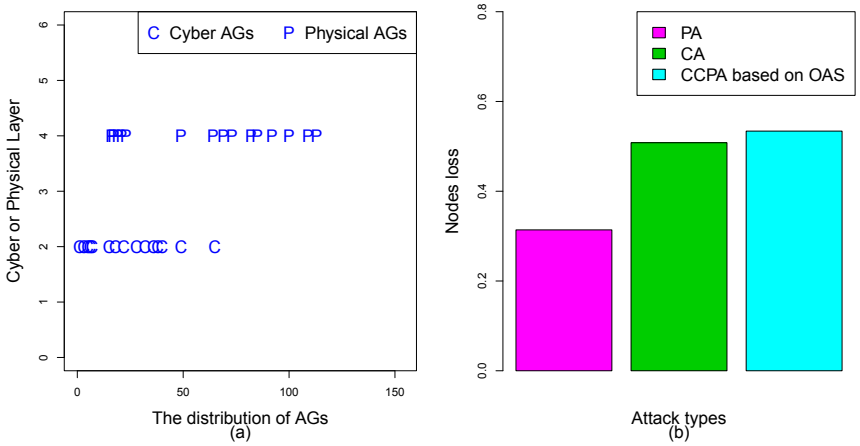

Fig. 3. The CCPA based optimal attack strategy. (a) The network layers and distribution of AGs. (b) Comparison of attack effects of cyber-attack (CA), physical attack (PA) and CCPA based on OAS.

The saturation attack strategy is to cover each node as much as possible without considering resource consumption or having sufficient resources, while avoiding redundant attacks. According to Algorithm 2, 30 cyber AGs and 9 physical AGs can be identified in Fig. 4(a), which has the same attack effect with 30 cyber AGs and 30 physical AGs. The tolerance α has a greater impact on the robustness of smart grid, so we calculate node loss of CCPA based on SAS to compare with PA and CA. It is clear that CCPA based on SAS has better attack effect than CA and PA regardless of $\alpha = 0.3$,$\alpha = 0.4$ and $\alpha = 0.5$ in Fig. 4(b).

In order to better show the node loss under different attack types, we show the curve of the cascading failure process by attacking the nodes one by one in Fig. 5. The black curve, red curve and blue curve represent the process of node loss under CCPA based on SAS, CA and PA, respectively. It is easy to see from Fig. 5(a), (b) and (c) that the ranking of node loss is CCPA based on SAS $>$ CA $>$ PA regardless of $\alpha = 0.3$, $\alpha = 0.4$ and $\alpha = 0.5$. This means that CCPA may become an attack mode that attackers are willing to choose, because it is difficult to defend and has higher attack effects.

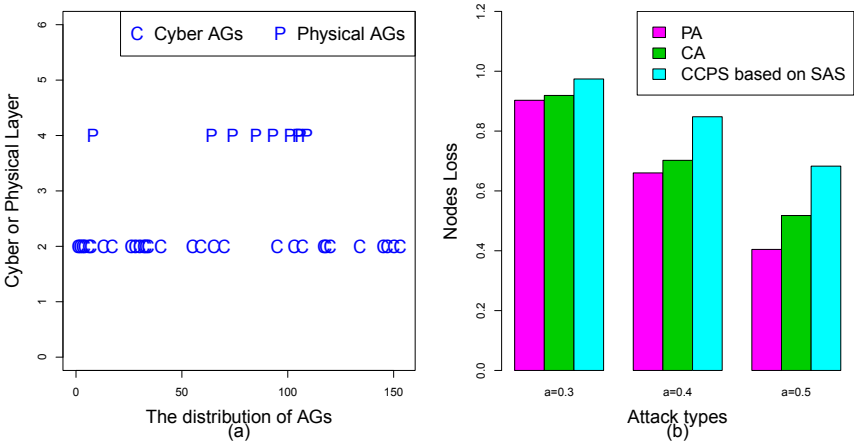

Fig. 4. The CCPA based saturation attack strategy (a) The network layers and distribution of AGs. (b) Comparison of attack effects of cyber-attack (CA), physical attack (PA) and CCPA based on SAS under different tolerances α.

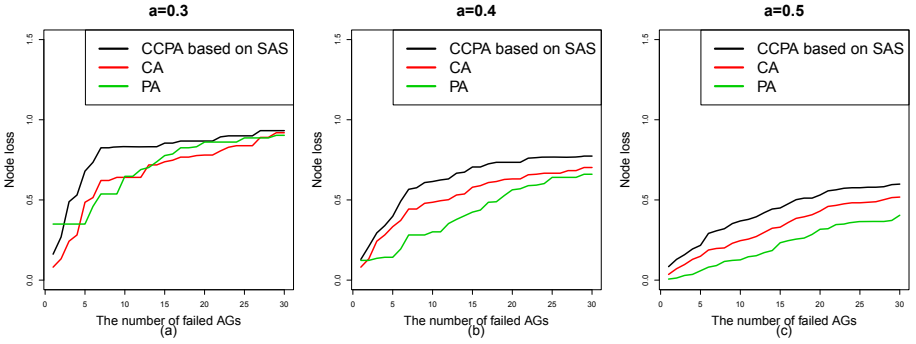

Fig. 5. The comparison of node loss of CA, PA and CCPA based on SAS. (a) $\alpha = 0.3$. (b) $\alpha = 0.4$. (c) $\alpha = 0.5$

3 Conclusion

In this paper, the optimal attack strategy and saturation attack strategy are proposed and applied to CCPA. Through experiments, we can draw the following conclusions: 1)When the same number of nodes are attacked, a set of attack sequence can always be identified by OAS to achieve a higher attack effect; 2) In order to achieve the same attack effect, the saturated attack strategy can find the attack sequence of fewer nodes regardless of $\alpha = 0.3$, $\alpha = 0.4$ and $\alpha = 0.5$; 3) whether based on OAS or SAS, the CCPA has a better attack effect than CA and PA.

In fact, Coordinated Cyber-Physical Attacks not only include the coordination of different attack strategies and means, but also the coordination of the

multi-directional and multi-targets. This require us to find an effective integrated defense mechanism or strategy to deal with CCPAs. At the same time, we also found an unconventional phenomenon from the experimental results, that is, different attack sequences composed of the same cyber and physical nodes have different attack effects on the cascading failure of smart grid.

In the future, there are a few points worthy of our in-depth study as follows:1) Research on analyzing the effect of different attack sequences on cyber-physical systems; 2) Research and identification of multiple types of attack strategies; 3) Research on cooperative defense model against CCPA.

References

1. Kang, W.J., Zhu, P.D., Hu, G., Hang, Z., Liu, X.: Cross-layer attack path exploration for smart grid based on knowledge of target network. In: Liu, W., Giunchiglia, F., Yang, B. (eds.) KSEM 2018. LNCS (LNAI), vol. 11061, pp. 433–441. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-99365-2_38
2. Smith, R.: Assault on California power station raises alarm on potential for terrorism. Wall Street J. http://online.wsj.com/news/articles/SB10001424052702304851104579359141941621778
3. Yang, Q., Yang, J., Yu, W., An, D., Zhang, N., Zhao, W.: On false data-injection attacks against power system state estimation: modeling and countermeasures. IEEE Trans. Parallel Distrib. Syst. **25**(3), 717–729 (2014)
4. Xiang, Y., Wang, L., Yu, D., Liu, N.: Coordinated attacks against power grids: load redistribution attack coordinating with generator and line attacks. In: IEEE Power Energy Society General Meeting, pp. 1–5 (2015)
5. Li, Z., Shahidehpour, M., Alabdulwahab, A., Abusorrah, A.: Bilevel model for analyzing coordinated cyber-physical attacks on power systems. IEEE Trans. Smart Grid **7**(5), 2260–2272 (2016)
6. Liu, S., Mashayekh, S., Kundur, D.: A framework for modeling cyber-physical switching attacks in smart grid. IEEE Trans. Emerg. Top. Comput. **1**(2), 273–285 (2013)
7. Deng, R., Zhuang, P., Liang, H.: CCPA: coordinated cyber-physical attacks and countermeasures in smart grid. IEEE Trans. Smart Grid **8**(5), 2420–2430 (2017)
8. Li, Z., Shahidehpour, M., Abdulwhab, A., et al.: Analyzing locally coordinated cyber-physical attacks for undetectable line outages. IEEE Trans. Smart Grid **9**(1), 35–47 (2017)
9. Liu, S., Feng, X., Kundur, D., et al.: Switched system models for coordinated cyber-physical attack construction and simulation. In: 2011 IEEE First International Workshop on Smart Grid Modeling and Simulation (SGMS), pp. 49-54. IEEE (2011)
10. Wei, L., Sarwat, A., Saad, W., et al.: Stochastic games for power grid protection against coordinated cyber-physical attacks. IEEE Trans. Smart Grid **9**(99), 684–694 (2016)
11. Tian, M., Cui, M., Dong, Z., et al.: Multilevel programming-based coordinated cyber physical attacks and countermeasures in smart grid. IEEE Access **7**, 9836–9847 (2019)

12. Lakshminarayana, S., Belmega, E.V., Poor, H.V.: Moving-target defense for detecting coordinated cyber-physical attacks in power grids. IEEE Access **7**, 9836–9847 (2019)
13. Kang, W., Zhu, P., Liu, X.: Integrated defense mechanism based on attack goals against three attack strategies in smart grid. In: IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Toronto, ON, Canada, pp. 1027–1032 (2020)