Optimal Defense Resource Allocation and Geographically Feasible Hexagonal Topology Construction for Power Grid Security

Yifa Liu[1,2] and Long Cheng[1,2](✉)

[1] Institute of Automation, Chinese Academy of Sciences, Beijing 100190, China
long.cheng@ia.ac.cn
[2] School of Artificial Intelligence, University of Chinese Academy of Sciences, Beijing 100049, China

Abstract. Power system faces thousands of physical and cyber attacks which seriously threaten its security. It is noted that most defense methods are only suitable for specific cyber attacks and are not applicable to physical attacks. This paper provides a generic method regardless of different attack types through topological efforts to reduce potential loss of the power grid. In this paper, a proportional loss model is proposed depending on the different attack-defense resource allocations. The optimal allocation strategy can be converted into the solution to a $\min \max$ problem. In order to further improve the security of the power grid, by taking the geographical feasibility into consideration, a hexagonal construction method is proposed to provide a cost-affordable and geographically-feasible solution for new power grid construction.

1 Introduction

With the fast development of technology and the advancement of infrastructure processes, demands for electricity quality and quantity have increased significantly. Adopting modern sensing, control, measurement technologies, the modern smart power grid has been proposed to satisfy the huge requirement of electrical power [1]. As network complexity increases [2], there are numerous elements in the power system to be protected [3,4]. From the perspective of the attack method, the power system is susceptible to a variety of physical [5] and cyber attacks, such as denial-of-service (DoS) attack [6,7] and false data injection (FDI) attack [8].

There are also plenty of specific defense methods for certain attack in the literature. A data verification method against FDI was introduced in [9]. Countermeasure for the case where the attacker has limited knowledge was also proposed in [10]. A two-layer game theoretical model for FDI attacks against power systems was given in [11]. A list of defense mechanisms against FDI attacks focused on certain devices [12–15]. Analysis of defense against price attacks using game

K. Li et al. (Eds.): LSMS 2021/ICSEE 2021, CCIS 1468, pp. 452–462, 2021.
https://doi.org/10.1007/978-981-16-7210-1_43

theory was given in [16]. An attack-resilient controller and an attack detection mechanism for price attacks were proposed in [17]. Stochastic games were used for fighting against coordinated cyber-physical attacks on power grids [18]. By adding wireless communication, an efficient way of optimizing topology of a wired networked system was proposed in [19]. There are also other methods of reducing damage, for example, a load redistribution way was proposed to reduce the impact on the load after attacks in [20]. It is noted that most papers regarding power grid security focus on cyber attacks and the defense methods can only handle a specific attack. Therefore, a natural question is whether we can find a generic defense way to protect the power grid, or at least reduce the impact of attacks.

In this paper, the power grid is modeled by a graph topology, and each section is treated as a node. The value of each node is equivalent to the total value of users affected by the crash of this node. Then a proportional model is proposed to analyze the probability of a node being crashed depending on different attack-defense resource allocations. For lack of information about the time and location of potential attacks, the defender should adopt a conservative strategy. Then this optimal resource allocation can be converted into a $\min\max$ problem. It can be found that the total loss function is dependent not only on the resource allocation, but also on the topology of the power grid.

In order to further improve the security of the power grid, the function of topology is taken into account. Adding redundant connections can reduce the harm when some nodes are crashed, which does not conflict with many specific defense methods and can be used with them simultaneously. Moreover, considering the construction feasibility of power grids in reality, a geography-based based hexagonal city planning topology construction method is proposed to provide a novel power grid construction solution.

2 Optimal Resource Allocation Strategies

2.1 Structure of Power Grid

The structure of power grid includes power plants, substations with different capacities, regional dispatching systems at different levels and power transmission lines to users as shown in Fig. 1. Then the power grid can be described by a graph topology, where each vulnerable section is treated as a node. This paper assumes that the direction to the end-users is positive and considers a power grid topology consisting of Q nodes.

2.2 Risk Function

Assumption 1. *The attack resources are quite few compared to the defense resources.*

The attack resources can include personnel or hackers hired to launch the attack, some technological resources such as advanced tools or malwares for

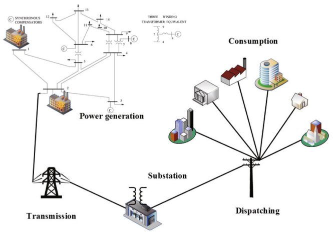


Fig. 1. Typical structure of one power grid.

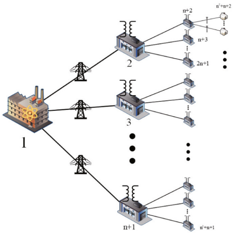


Fig. 2. Smart grid with a n-ary tree topology

malicious actions, and other economic resources. Similarly, the defense resources can include personnel to reinforce and repair the grid, technological resources such as efficient and effective suites of security tools or softwares to maintain the normal operation of the grid, and other economic resources. If more attack resources are allocated to the node, this node is more likely to be crashed, that is, the node can no longer perform normal work, and vice versa.

Although there have been many serious blackouts to alert humans to the importance of power grid security, and many of them have caused incalculable loss. However, it should still be known that accidents are rare, and most of the power grids are working properly, even if they often face various attacks.

Due to the law of diminishing marginal utility, with the more defense resources already allocated, adding extra defense resources produces fewer effects. By Assumption 1, the attack resources allocated to a single node are small that to add more attack resources does not reduce the value of unit resources, hence, the attack effect can be regarded as a linear function of quantity. Then the probability of node i being crashed is modeled by

$$p_i = \frac{a_i}{d_i}. \tag{1}$$

where p_i denotes the probability of node i being crashed, $0 \leq a_i \leq A$ and $A < d_i < D$ denote the attack and defense resource allocated to node i, $d_i \geq a_i$. $A = \sum_{k=1}^{N} a_k$ and $D = \sum_{k=1}^{N} d_k$, $D \gg A$ denote the total attack and defense resource, respectively.

Remark 1. The attacks discussed in this paper are primarily those that target a single node. This analysis is not applicable to large-scale chain reactions, such as infectious viruses. Unless it can be quickly blocked so that it affects only the area where it occurred.

Assumption 2. *Nodes are independent of each other.*

As long as nodes are crashed, loss is caused. If damaged nodes are independent of each other, then the expectation of total loss of power grid can be expressed by

$$E(L) = \sum_{k=1}^{Q} p_k v_k = \sum_{k=1}^{Q} \frac{a_k}{d_k} v_k. \tag{2}$$

Assumption 3. *The defender would take conservative strategies since it has no information from the attack side.*

Denote $s_a = [a_1\ a_2\ \cdots\ a_N]^T$ and $s_d = [d_1\ d_2\ \cdots\ d_N]^T$ as the strategies of the attacker and defender respectively.

The goal of the attacker is to maximize the total loss by choosing the optimal attack strategy s_a^*, while the task of the defender is to adopt the optimal defense strategy s_d^* and minimize the total loss. Many studies simulated offense-defense scenarios by using game theory [11,13,16], differential game models [12] or multi-agent system [21]. However, neither the attacker nor the defender has global information, which means that the classic 2-player game where both players have perfect information of the payoff matrix and system states is not applicable.

Under Assumption 3, the defender should take the following conservative strategy to avoid the risk of disastrous loss,

$$s_d^* = \underset{s_d}{\operatorname{argmin}} \max_{s_a} E(L(s_a, s_d)) = \underset{s_d}{\operatorname{argmin}} \max_{s_a} \sum_{i=1}^{Q} \frac{a_i}{d_i} v_i, \tag{3}$$

$$s_a^* = \underset{s_a}{\operatorname{argmax}}\, E(L(s_a, s_d^*)). \tag{4}$$

Then the total loss under the optimal attack-defense resource allocation is

$$E(L(s_a^*, s_d^*)) = \min_{s_d} \max_{s_a} \sum_{i=1}^{Q} \frac{a_i}{d_i} v_i = \sum_{i=1}^{Q} \frac{a_i^*}{d_i^*} v_i. \tag{5}$$

2.3 Optimal Resource Allocation Strategy

Considering the aciculate variation $\Delta_{ij} = \delta(\mathbf{e}_i - \mathbf{e}_j)$. Then the difference of any two strategies can be expressed by a linear combination of aciculate variations.

First relax restrictions of $0 \le a_i \le A$ and $A < d_i < D$ to be $a_i \in \mathbb{R}$ and $d_i \in \mathbb{R}$. For any $i, j, i \ne j$, $E(L(s_a^* + \Delta_{ij}, s_d^*)) \le E(L(s_a^*, s_d^*))$, conversely $E(L(s_a^* - \Delta_{ij}, s_d^*)) \le E(L(s_a^*, s_d^*))$. Then it can be obtained that

$$\frac{\delta}{d_i^*} v_i - \frac{\delta}{d_j^*} v_j \le 0, \quad -\frac{\delta}{d_i^*} v_i + \frac{\delta}{d_j^*} v_j \le 0. \tag{6}$$

Therefore, $\delta v_i / d_i^* - \delta v_j / d_j^*$ must be 0.

It can be verified that this conclusion also holds under restrictions $0 \le a_i \le A$ and $A < d_i < D$. Then the optimal defense strategy should satisfy the following condition

$$\frac{d_i^*}{d_j^*} = \frac{v_i}{v_j}, \quad d_i^* = \frac{v_i}{\sum_{k=1}^{Q} v_k} D > 0. \tag{7}$$

It can be found that the amount of defense resources allocated to each node should be proportional to the value of that node. Furthermore, the loss function under the optimal strategies of both sides is shown as follows

$$E(L(s_a^*, s_d^*)) = \frac{A}{D} \sum_{k=1}^{Q} v_k. \tag{8}$$

It is obvious that s_a^* can be any feasible solution, which means s_d^* is sufficiently robust to deal with all attack strategies.

Equation (8) reveals the fact that the loss suffered by the power grid is positively correlated with the attack intensity and the power grid value, and negatively correlated with the amount of defense. However, that value v_i has not yet been assessed.

In reality, Electricity was transmitted from the plant to the users: residents, factories and etc. The power grid distributes electricity to users in a large area. High-voltage transmission (HVT) technology and three-phase transmission technology are adopted to reduce loss in power transmission. Therefore, there are many transformers with different capacities at intermediate levels. This observation makes the tree topology reasonable, where the plant is the root and the users are leaves. Since the completion of the power supply need requires a series of different devices, and the damage of any node can block the process. When a node is crashed, the power supplies of some end-users are affected. From this point of view, v_i is equal to the total value of leaf nodes affected.

Consider a n-ary tree with $M,\ M > 1$ levels, $Q = (n^M - 1)/(n-1)$. Label each node as shown in Fig. 2. Denote v_{user} as the value of a user, namely the loss caused when a user cannot get power. The loss caused by a crashed leaf node at the M-th level is $v_{\frac{n^{M-1}-1}{n-1}+j} = v_{\text{user}},\ j = 1, \cdots, n^{M-1}$. There are n^{M-i} leaf nodes in the descendant set of a node on the i-th $(i = 1, 2, \cdots, M-1)$ level, and those sets do not intersect. Hence all nodes on the i-th level have the same value $v_{\frac{n^{i-1}-1}{n-1}+j} = n^{M-i} v_{\text{user}},\ j = 1, \cdots, n^{i-1}$, and the defense resources allocated to them are equal.

Since there are n^{i-1} nodes at the i-th level, the total value of the i-th level is $n^{M-1} v_{\text{user}}$. Then all levels have the same value, which requires that defense resources should be distributed to each level evenly,

$$d^*_{\frac{n^{i-1}-1}{n-1}+j} = \frac{D}{Mn^{i-1}},\ i = 1, 2, \cdots, M,\ j = 1, 2, \cdots, n^{i-1}. \tag{9}$$

And the expectation of the total loss can be obtained that

$$E(L(s_a^*, s_d^*)) = Mn^{M-1} \frac{A}{D} v_{\text{user}}. \tag{10}$$

3 Improved Loss Function and Allocation Strategies

Assumption 4. *Nodes are relevant to each other.*

Based on Assumption 2, the loss function (2) works only when damaged nodes are irrelevant to each other. However, when any two nodes are at the "high" risk, the relationship between them should be taken into consideration.

When the parent node has been crashed, there is no need to attack any downstream node of this node, and vice versa. Only in the case that all its upstream nodes are intact, the value of the crashed node can be added to the total loss function. Due to the physical isolation, the probabilities of any two nodes being crashed are independent of each other. Therefore, under Assumption 4, the loss function can be improved as

$$E(L) = \sum_{k=1}^{Q} [p_k v_k \prod_{j \in \mathcal{U}_k} (1 - p_j)] = \sum_{k=1}^{Q} [\frac{a_k}{d_k} v_k \prod_{j \in \mathcal{U}_k} (1 - \frac{a_j}{d_j})], \tag{11}$$

where $\mathcal{U}_i$ is the set of upstream nodes of node i.

This improved loss function reflects one fact that the more attack resources allocated to the upstream node, the less necessity to take downstream nodes into account.

It is noted that loss function (11) is always no greater than (2) under the same strategies of both sides. If any attacked node is not an upstream (downstream) node of other attack targets, loss function (11) degenerates into (2). Therefore, the attacker should try to avoid the path between targets.

In the n-ary tree topology, the optimal attack can be achieved as long as the existence of path between the attacked nodes is avoided, while the defender should distribute defense resources evenly to all levels.

Assume the defender adopts the defense strategy defined by (9). Denote L as the maximal loss under any attack resource allocation. Let $L^* = Mn^{M-1}Av_{\text{user}}/D$, which is equal to the loss in (10), then $L \leq L^*$. Some different attack target selections are shown in Fig. 3. From this figure, it is obvious that the attacker can always avoid the existence of path to get the maximal loss L^* in a tree topology. And nodes at all levels are threaten as the one in Subsect. 2.3.

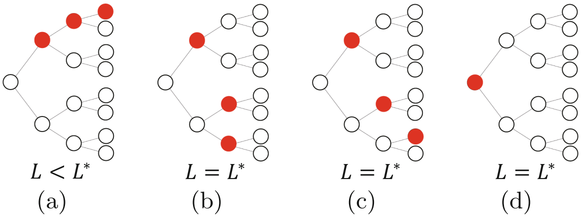


Fig. 3. Loss under different attack target selections in a tree topology.

If the defender does not take the defense strategy defined by (9), there exists a node such that the defense resource allocated to this node is less than that in (10). If the attacker centralizes all attack resources to this node, the loss becomes greater than that of (10). Hence the defense strategy defined by (9) is optimal.

To summarize, under the improved loss function defined by (11), the optimal defense strategy is the same as (9). And the optimal attack strategy can be any feasible strategy as long as there is no path between all attacked nodes. Then the expectation of the total loss can be calculated as

$$E(L(s_a^*, s_d^*)) = \frac{A}{D} M n^{M-1} v_{\text{user}}. \tag{12}$$

In the tree topology, every non-root node has only one parent, which means that there is only one path from the root to the leaf. If any node on the path is crashed, the leaf fails and the loss occurs. If there are backup paths, a node can get the service from an alternative superior in case of an emergency as shown in Fig. 4. Then whatever intermediate node is attacked, the power can still be transmitted from the plant to end-users.

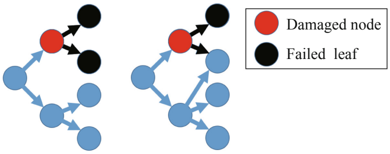


Fig. 4. Node failure situations with and without redundant connections.

It can be revealed that the total loss function is dependent on not only the resource allocation of both sides but also the topology of the power grid. If the connection structure is modified properly, the robustness of the power grid with respect to the attack can be improved.

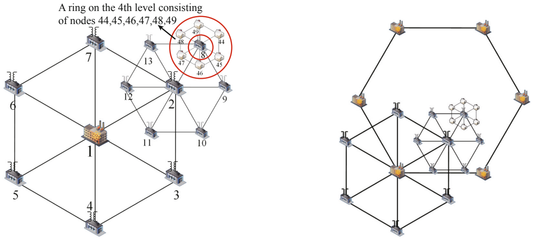
4 Geographical Knowledge Based Grid Construction

Section 3 tells how different topologies affect the total loss, however, only topology information cannot guide the construction of power grids. By taking the geographical distribution, capacity, and function of facilities into consideration, this section aims at providing a geographically feasible construction solution for power grids.

4.1 Hexagonal City Group

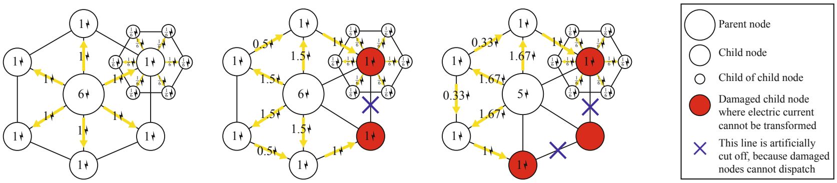
Based on geographical distribution, a feasible topology construction method is developed for the power grid, which is shown in Fig. 5(a). This topology is similar to a 6-ary tree except that six child nodes of one node are connected together to form a ring structure (one child node is linked to its two adjacent siblings).

Within this structure, the capacity of each facility (including the power line) is set to be twice its basic demand. Then even if up to two nodes are damaged, sibling nodes can take the responsibility of damaged nodes and maintain the healthy operation of the entire grid, which is demonstrated in Fig. 6.


A ring on the 4th level consisting
of nodes 44,45,46,47,48,49
1
2
3
4
5
6
7
8
9
10
11
12
13
44
45
46
47
48
49

(a) Hexagonal city groups (b) Combination of six hexagonal city groups

Fig. 5. A feasible power grid construction method with the hexagonal city group structure.


1
6
$\frac{1}{6}$
0.5
1.5
0.33
1.67
5
Parent node
Child node
Child of child node
Damaged child node where electric current cannot be transformed
This line is artificially cut off, because damaged nodes cannot dispatch

(a) Normal operation (b) Two nodes damaged (c) Three adjacent nodes damaged

Fig. 6. Operation conditions of power transmission under different scenarios: (a) the normal case; (b) although two nodes are damaged, the responsibility of these two nodes can be taken by their sibling nodes and the child nodes of damaged nodes are not affected; and (c) when three adjacent nodes are damaged, the middle damaged node and its descendants are affected, and the loss occurs.

Assume the power grid with the hexagonal structure has M levels, $Q = (6^M - 1)/5$. The total value of all leaf nodes is $6^{M-1} v_{\text{user}}$. According to Fig. 6, to make one node stop working, the attacker must crash this node and its two adjacent nodes to ensure the power cannot pass through this node. Therefore, the probability of any node other than the root stopping working is approximately equal to the probability that the point and its two neighbors are destroyed.

Due to space constraints, the detailed proof is not provided here. By using the same method in Sect. 2, the final optimal defense resource allocation strategy and the corresponding total loss are

$$d_1^* \approx D,\ d^*_{\frac{(6^{i-1}-1)}{5}+l} \approx 6^{-\frac{i+1}{3}} A^{\frac{2}{3}} D^{\frac{1}{3}},\ i = 2, \cdots, M,\ l = 1, \cdots, 6^{i-1}; \tag{13}$$

$$E((s_a^*, s_d^*)) \approx \frac{A}{D} 6^{M-1} v_{\text{user}}. \tag{14}$$

The total loss is reduced to (1/M) compared to that of the original tree structure.

4.2 Groups of Hexagonal City Groups

The most fragile section is the power generation process (root node) because it has no substitute, which results in a large number of defense resources being placed on the root. If there are multiple power plants, then they can be strung into a ring as shown in Fig. 5(b) and the loss can be further reduced.

Consider a combination of 6 city groups. The total amounts of the attack-defense resources are $6A$ and $6D$, respectively. By accumulating the loss on each level, then the optimal defense strategy and corresponding loss can then be calculated as follows

$$\begin{aligned} d_1^* = d_2^* = \cdots = d_6^* &= \frac{6^{\frac{2}{3}} - 1}{6^{\frac{2M}{3}} - 1} D, \\ d^*_{\frac{(6^{i-1}-6)}{5}+r} &= \frac{6^{-\frac{i-3}{3}} - 6^{-\frac{i-1}{3}}}{6^{\frac{2M}{3}} - 1} D, \ i = 2, \cdots, M, \ r = 1, \cdots, 6^i. \end{aligned} \tag{15}$$

$$E(L(s_a^*, s_d^*)) = (\frac{6^{\frac{3M-7}{3}} - 6^{\frac{M-7}{3}}}{6^{\frac{2}{3}} - 1})^3 (\frac{A}{D})^3 v_{\text{user}}. \tag{16}$$

In a word, the hexagonal city planning proposed in this paper can effectively reduce loss, without requiring too many additional connections. It can improve not only the security of the power system but also the efficiency of the infrastructure investment in the power grid.

5 Conclusion

The operation of the power system requires the coordination of a series of different facilities. As long as any section or any facility fails, the power supply can be cut off. Therefore, concentrating attack resources can produce a better destructive effect. Conversely, the defender should guarantee the reliability of every facility. Redundant connections can make sure that there are other facilities to maintain the operation of the grid after some facilities damaged.

When adding redundant connections, cost, feasibility, and the facility's capacity need to be taken into account. To achieve this goal, based on the city element's real physical location, this paper recommends using the hexagonal city planning method where any facility has the "backup" facilities for replacement in case of damage. Under this method, the expected loss of the entire grid has a cubic-level decay, while the grid construction of the proposed method has high geographic feasibility.

Acknowledgment. This work was supported in part by the National Natural Science Foundation of China (Grants 61633016 61873268 62025307 U1913209) and the Beijing Natural Science Foundation (Grant JQ19020)

References

1. Lu, G., De, D., Song, W.: SmartGridLab a laboratory-based smart grid testbed. In: Proceedings of the First IEEE International Conference on Smart Grid Communications. Gaithersburg, USA, pp. 143–148 (2010)
2. Bella, A.L., Cominesi, S.R., Sandroni, C., Scattolini, R.: Hierarchical predictive control of microgrids in islanded operation. IEEE Trans. Automation Sci. Eng. **14**(2), 536–546 (2017)
3. Bompard, E., Wu, D., Xue, F.: Structural vulnerability of power systems: a topological approach. Electric Power Syst. Res. **81**(7), 1334–1340 (2011)
4. Sridhar, S., Hahn, A., Govindarasu, M.: Cyber-physical system security for the electric power grid. Proc. IEEE **100**(1), 210–224 (2012)
5. Jeler, G.E., Roman, D.: The graphite bomb: an overvies of its basic military applications. Rev. Air Force Acad. **1**(31), 13–18 (2016)
6. Zhang, H., Cheng, P., Shi, L., Chen, J.: Optimal denial-of-service attack scheduling with energy constraint. IEEE Trans. Automatic Control. **60**(11), 3023–3028 (2015)
7. Zhang, H., Cheng, P., Shi, L., Chen, J.: Optimal DoS attack scheduling in wireless networked control system. IEEE Trans. Control Syst. Technol. **24**(3), 843–852 (2016)
8. Kosut, O., Jia, L., Thomas, R.J., Tong, L.: Malicious data attacks on the smart grid. IEEE Trans. Smart Grid **2**(4), 645–658 (2011)
9. Yang, X., Lin, J., Yu, W., Moulema, P., Fu, X., Zhao, W.: A novel en-route filtering scheme against false data injection attacks in cyber-physical networked systems. IEEE Trans. Comput. **61**(1), 4–18 (2015)
10. Deng, R., Liang, H.: False data injection attacks with limited susceptance information and new countermeasures in smart grid. IEEE Trans. Ind. Inf. **15**(3), 1619–1628 (2019)
11. Wang, Q., Tai, W., Tang, Y., Ni, M., You, S.: A two-layer game theoretical attack-defense model for a false data injection attack against power systems. Int. J. Electrical Power Energy Syst. **104**, 169–177 (2019)
12. Srikantha, P., Kundur, D.: A DER attack-mitigation differential game for smart grid security analysis. IEEE Trans. Smart Grid **7**(3), 1476–1485 (2016)
13. Farraj, A., Hammad, E., Daoud, A.A., Kundur, D.: A game-theoretic analysis of cyber switching attacks and mitigation in smart grid systems. IEEE Trans. Smart Grid **7**(4), 1846–1855 (2016)
14. Sridhar, S., Manimaran, G.: Data integrity attack and its impacts on voltage control loop in power grid. In: Proceedings of IEEE Power & Energy Society General Meeting. San Diego, USA, pp. 1–6 (2011)
15. 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 Distributed Syst. **25**(3), 717–729 (2014)
16. Esmalifalak, M., Shi, G., Han, Z., Song, L.: Bad data injection attack and defense in electricity market using game theory study. IEEE Trans. Smart Grid **4**(1), 160–169 (2013)
17. Giraldo, J., Crdenas, A., Quijano, N.: Integrity attacks on real-time pricing in smart grids: impact and countermeasures. IEEE Trans. Smart Grid **8**(5), 2249–2257 (2017)
18. Wei, L., Sarwat, A.I., Saad, W., Biswas, S.: Stochastic games for power grid protection against coordinated cyber-physical attacks. IEEE Trans. Smart Grid **9**(2), 684–694 (2018)

19. Wang, H., Zhao, Q., Jia, Q., Guan, X.: Efficient topology optimization for a wired networked system by adding wireless communication. In: Proceedings of 2012 American Control Conference. Montreal, Canada, pp. 448–453 (2012)
20. Wang, J.W., Rong, L.L.: Cascade-based attack vulnerability on the US power grid. Saf. Sci. **47**(10), 1332–1336 (2009)
21. Liu, Y., Cheng, L.: Sampled-data based mean square bipartite consensus of double-integrator multi-agent systems with measurement noises. In: Proceedings of 2018 Chinese Intelligent Systems Conference, pp. 339–349 (2019)