
Article:
Du, M. orcid.org/0009-0009-9806-841X, Zhang, X. orcid.org/0000-0002-6063-959X, Zhang, J. orcid.org/0000-0002-6188-4108 et al. (1 more author) (2025) Malicious attacks for maximising island numbers in cyber-physical power system: a graph-theoretic approach. IEEE Internet of Things Journal. ISSN: 2327-4662

https://doi.org/10.1109/jiot.2025.3619395

Malicious Attacks for Maximising Island Numbers in Cyber-Physical Power System: A Graph-Theoretic Approach

Min Du, *Member, IEEE*, Xin Zhang, *Senior Member, IEEE*, Jinning Zhang, *Member, IEEE*, Rui Zhang

***Abstract*—This letter proposes an island-maximising attack mechanism to maximise the number of power islands in cyber-physical power systems (CPPS) by disrupting lines. Specifically, a single-level mixed-integer programming (MIP) model is developed with a graph-theoretic approach, which is able to divide CPPS into power islands, while intra-island line overloads are induced in a high-stealth manner with increasing load shedding and economic loss. Case studies conducted on modified IEEE 14-bus and practical 36-zone Great Britain systems validate the effectiveness of our proposed island-maximising approach.**

***Index Terms*—Graph theory, cyber-physical power system, power island, malicious attacks.**

I. INTRODUCTION

MODERN power system is evolving into cyber-physical power system (CPPS), which is a critical part of industrial cyber-physical systems [1]. While this evolution enhances the monitoring and the control of physical power system with advanced information technologies, it renders CPPS more susceptible to malicious attacks including both cyber and physical attacks [2]. A well-documented example is the cyberattack on Ukraine in December 2015, where adversaries infiltrated Supervisory Control and Data Acquisition (SCADA) networks and remotely tripped substations, causing outages that affected approximately 225,000 customers [3]. Another case is the Metcalf substation physical attack in California in April 2013, where a physical attack by snipers disabled 17 transformers, resulting in significant economic loss [4]. Thus, analysing potential malicious attack strategies against CPPS is crucial to improving the system resilience.

At present, extensive research has been conducted on various attack strategies to reveal the potential CPPS vulnerability to malicious attacks, which can help the system operator design defence strategies against such attacks [5]. In this context, Liu *et al*. proposed a bi-level model to maximise the operational cost and load shedding by launching cyberattacks in economic dispatch [6]. The authors in [7] revealed that cyber attackers can overload multiple targeted lines by corrupting the least-load nodes [8]. Recently, the authors in [9] analysed the vulnerability of power systems and associated economic performance under multiple line contingencies due to physical attacks. However, most existing studies focus on operational aspects such as load shedding, economic loss or line overloads in CPPS. Thus, graph theoretic approaches are adopted to specifically design the malicious attacks from the network perspective, where the system is divided into several isolated power islands, leading to greater network disruption and power system isolation with more severe cyber-physical impacts. Biswas *et al*. in [10] employed a graph-theoretic approach to identify vulnerable components such as transmission lines under extreme events. Here, the identified vulnerable lines represent the weak points in the network along which power islanding is most likely to occur. Then, the authors in [11] proposed a graph-theoretic approach based on the Fiedler vector to isolate power systems into islands by malicious attacks, while the power imbalance was minimised in the system. However, this approach was limited to dividing a power system into two islands in CPPS. Such network isolation-based attacks are particularly attractive to attackers because the power islands can amplify system instability and damage network integrity, leading to more severe disruptions compared with the load shedding, economic loss and line overloads caused by malicious attacks.

Motivated by this, Table I summarises the mainstream malicious attack strategies, and highlights the advantages of our proposed island-maximising approach in addressing the following two key questions: ***Can attackers divide a power system into several isolated power islands by disrupting lines through malicious attacks and maximise the number of islands in the system? Can attackers stealthily induce line overloads in certain isolated power islands while causing load shedding and economic loss in a power system?***

TABLE I
COMPARISON BETWEEN PROPOSED AND EXISTING ATTACK STRATEGIES

Attack Strategy	Ref [6]	Ref [7]	Ref [9]	Ref [10]	Ref [11]	This paper
Power island	×	×	×	✓	✓	✓
Graph-theoretic	×	×	×	✓	✓	✓
Line overload	×	✓	×	×	×	✓
Economic loss	✓	×	✓	×	×	✓
Island number	×	×	×	×	×	✓
High stealth	×	×	×	×	×	✓

† "Island number" indicates that the maximum number of power islands under malicious attacks.

To address the above questions, this letter proposes a novel island-maximising attack mechanism based on a graph-theoretic approach, which can maximise the number of power islands in CPPS by disrupting lines. Also, Kirchhoff's Current Law (KCL) is enforced within each island to improve the stealthiness of such attacks, while leading to effective load shedding and economic loss. The study assumes that when system operators become aware of the event, they are not able to immediately respond to the islanding situations, and incorrect decisions may be made under the false assumption that the entire system still satisfies Kirchhoff's Voltage Law (KVL). Thus, these incorrect decisions can cause power flow imbalances within islands, leading to further line overloads in certain isolated power islands.

This work was supported by the U.K. Research and Innovation Future Leaders Fellowship "Digitalisation of Electrical Power and Energy Systems Operation" under Grant MR/W011360/2. (*Corresponding author:* Xin Zhang.)

M. Du and X. Zhang are with the School of Electrical and Electronic Engineering, University of Sheffield, Sheffield, S10 2TN United Kingdom (e-mail: m.du@sheffield.ac.uk; xin.zhang1@sheffield.ac.uk).

J. Zhang is with the School of Engineering, University of Leicester, Leicester, LE1 7RH United Kingdom (e-mail: jz388@leicester.ac.uk).

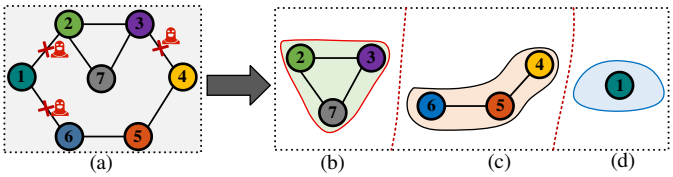
R. Zhang is with the System Operations, National Energy System Operator, Wokingham, RG41 5BN, United Kingdom (email: rui.zhang@nationalenergyso.com).

II. Proposed Single Level MIP Attack Model

A. Graph-Theoretic Based Island-Maximising Attack

Power network can typically be modelled as an undirected graph $\boldsymbol{G} = (\boldsymbol{B}, \boldsymbol{L})$, where $\boldsymbol{B}$ is the set of buses (vertices) and $\boldsymbol{L}$ is the set of lines (edges), i.e., $(i,j)|i,j \in \{1,2,\dots,N\}$. For a subset of lines $\boldsymbol{A}$, i.e.,$\boldsymbol{A} \subseteq \boldsymbol{L}$, removing these lines yields the remaining graph (i.e., $\boldsymbol{G} \setminus \boldsymbol{A}$) and its connected components in this graph are referred to as islands. Essentially, a malicious attack that interrupts lines in $\boldsymbol{A}$ induces an edge cut, dividing $\boldsymbol{G}$ into multiple mutually disconnected subgraphs.

Thus, the power system islanding in CPPS can be described as a graph cut problem, which aims to decompose a graph into multiple internally connected but mutually disconnected subgraphs by disrupting lines. When the graph $\boldsymbol{G}$ is divided into several subgraphs, as shown in Fig. 1, the five graph islanding criteria are satisfied*: **1) Any two subgraphs are mutually disconnected; 2) All components in each subgraph are internally connected; 3) Each bus is assigned to only one subgraph; 4) The sum of buses in all subgraphs equals the entire bus set B; 5) Each subgraph contains at least one bus.***



Note that the three divided subgraphs follow the graph islanding criteria.

Fig. 1. (a) Original undirected graph $\boldsymbol{G}$ as "island a"; (b) Induced subgraph as "island b"; (c) Connected subgraph; (d) Trivial subgraph as "island d".

Unlike traditional malicious attack methods, the islanding-maximising attack mechanism is designed to maximise the number of power islands subject to an attack-budget constraint, while intra-island power balance (KCL) is maintained to improve the attack stealthiness, with the entire system still satisfying the KVL constraint. This novel attack mechanism integrates the graph-theoretic island division and physical law-based power system operation. This differentiates our approach from purely structural graph partitioning, where a feasible islanding attack must satisfy both graph connectivity conditions and system operation constraints.

B. Mathematical Formulation of Proposed Model

A graph-theoretic based mixed-integer programming (MIP) model is proposed for malicious attacks to maximise the number of islands in CPPS.. The objective of this model is to intentionally disrupt a subset of lines such that the resulting power system is divided into multiple isolated power islands, satisfying the five graph islanding criteria and the physical laws of power system operation (i.e., KCL and KVL). Thus, the mathematical formulation of this problem can be presented as follows:

$$\max_{y_k} \ \sum_{k=1}^{N} y_k \tag{1}$$

where the objective function (1) aims to maximise the number of islands in the power system. Here, y_k is a binary variable that equals 1 if candidate island k exists, and 0 otherwise. k denotes the index of candidate islands. N is the total number of buses. This problem is subject to the following constraints:

$$\left|\text{Island}_i - \text{Island}_j\right| \le M \cdot u_l \quad \forall l = (i,j) \in \boldsymbol{L} \tag{2}$$

where l is the index of lines, and $\boldsymbol{L}$ denotes the set of lines. u_l is a binary variable that equals 1 if line l is attacked, and 0 otherwise. Island_i is an integer variable that represents the index of the island to which bus i belongs. M is a sufficiently large positive constant. Constraint (2) ensures that two buses connected by an intact line must belong to the same island, essentially satisfying criterion 2, and preventing unintended connections between islands through uninterrupted lines, thus also satisfying criterion 1.

$$\sum_{k=1}^{N} z_{i,k} = 1 \qquad \forall i \in \boldsymbol{B} \tag{3}$$

$$|\text{Island}_i - k| \le M \cdot (1 - z_{i,k}) \ \forall l = (i,j) \in \boldsymbol{L} \tag{4}$$

where $z_{i,k}$ is a binary assignment variable that equals 1 if bus i is assigned to island k, and 0 otherwise. Constraint (3) enforces that each bus must be exclusively assigned to exactly one island, thereby satisfying criterion 3. Note that this constraint also satisfies criterion 4 since it guarantees that all buses are assigned to islands. Constraint (4) serves as an auxiliary condition to constraint (3), ensuring consistency between the integer variable Island_i and the binary variable $z_{i,k}$.

$$y_k \le \sum_{i=1}^{N} z_{i,k} \qquad \forall k \le N \tag{5}$$

where constraint (5) denotes that an island should be assigned at least one bus, otherwise this island does not exist. That is, this constraint satisfies criterion 5.

$$\sum_{l=1}^{NL} u_l \le AL_{\text{attack}}^{\max} \tag{6}$$

where NL represents the total number of lines; $AL_{\text{attack}}^{\max}$ indicates the attack budget. Constraint (6) enforces that the total number of attacked lines does not exceed the attack budget.

$$\sum_{g \in \mathcal{G}} P_g \cdot z_{g,k} = \sum_{d \in \mathcal{D}} (D_d - J_d) \cdot z_{d,k} \quad \forall k \le N \tag{7}$$

where g is the index of generators. d is the index of loads. P_g is the power output of generator g. J_d is the shedding of load d. To improve the stealthiness of island-maximising attacks, isolated power islands can maintain independent operation after line disruptions, i.e., by ensuring power balance. Constraint (7) ensures power balance within each island (i.e., each island satisfies KCL). This is because such attacks divide the system into islands, which may be detectable if the power balance within each island is not satisfied. Thus, ensuring power balance within each island is essential for improving the stealthiness of island-maximising attacks.

$$(1 - u_l) \cdot \mathbf{SF}_l \cdot [\mathbf{KP} \cdot \boldsymbol{P} - \mathbf{KD} \cdot (\boldsymbol{D} - \boldsymbol{J})] = PL_l \ \forall l \in \boldsymbol{L} \tag{8}$$

$$-PL_l^{\max} \le PL_l \le PL_l^{\max} \qquad \forall l \in \boldsymbol{L} \tag{9}$$

where **KP** and **KD** are bus-unit and bus-load incidence matrices, respectively. $\mathbf{SF}_l$ indicates the l^{th} row of the shift factor (**SF**) matrix. $\boldsymbol{P}$ is the power output vector of generators; $\boldsymbol{D}$ is the load demand vector; $\boldsymbol{J}$ is the load shedding vector. $PL_l^{\max}$ indicates the maximum power flow of line l. Constraint (8) calculates the power flow of line l (i.e., PL_l) with additional attack decision variable u_l based on the overall system, which implicitly satisfies KVL using shift factor coefficients. This is because the system operator cannot immediately switch to power system islanding operation, and power flow analysis is still conducted under the assumption of an intact system operation with continuous line overloads. Constraint (9) limits the power flow of line l.

$$0 \le P_g \le P_g^{\max} \qquad \forall g \in \mathcal{G} \tag{10}$$

$$0 \le J_d \le D_d \qquad \forall d \in \mathcal{D} \qquad (11)$$

where $P_g^{\max}$ is the maximum power output of generator g. D_d is the demand of load d. $\mathcal{G}$ and $\mathcal{D}$ are the sets of generators and loads, respectively. Constraints (10)-(11) limit the power output of generator g and the load shedding of load d, respectively.

Note that the absolute value terms involved in constraints (2) and (4) can be linearised using the method proposed in [12], while the bilinear terms in constraints (7)-(8) are linearised using the big-*M* method [13]. Finally, our proposed MIP model can be efficiently solved using commercial solvers.

III. Case Studies

In this section, we use modified IEEE 14-bus and practical Great Britain 36-zone systems to demonstrate the effectiveness of our proposed model. The model is implemented on M3 Max-based MacBook Pro with 36 GB, using MATLAB 2021b.

A. Vulnerability Analysis

We first study the impact of our proposed island-maximising attacks on the modified IEEE 14-bus system from the perspective of power islands and line overloads. Tables II-III and Fig. 2 show the simulation results when the attack budget is set to 3 lines.

1) Power islands Analysis: We can observe that our approach can effectively divide the system into three power islands (i.e., one induced island and two trivial islands, as classified in Fig. 1) after disrupting targeted lines 11, 14, and 18 (as shown in Fig. 2), while both methods in [7, 9] are unable to achieve islanding. Since the trivial "Island d"-1 in Fig. 2 only contains load bus 11, this bus is completely separated from the main structure of the system, which leads to complete load shedding in this island. Similarly, the trivial "Island d"-3 is only composed of generator bus 8, indicating the presence of isolated and interrupted power supply. Note that only the related total cost is shown in Table II due to space limitations. We can observe that the total cost in our approach is higher than that in [7, 9], which validates the effectiveness of our approach in designing a high-impact island-maximising mechanism and revealing the vulnerability of CPPS under malicious attacks. While the total cost in [11] is higher than that in our proposed approach, only two power islands are formed without further line overloads, whereas three islands are formed in our method, two of which are trivial islands. The comparative analysis validates that our approach can divide the system into the maximum number of isolated power islands, bringing significant vulnerability and potential security risks to CPPS.

2) Line Overload Analysis: As shown in Table III, our approach is able to successfully overload three lines in the induced "Island b"-2, and their locations are shown in Fig. 2, with the power flow of line 4-5 reaching up to 125% of its rated capacity. This is because the system operator is assumed to not immediately respond the occurrence of power islands in the system after the disruption of targeted lines, who may continuously operate the islanded power system under the assumption that power support from other areas remains feasible, i.e., cross-island power dispatch. In fact, once power islands are formed, cross-island power dispatch becomes physically impossible. This causes incorrect cyber dispatch and control actions resulting from this incorrect assumption,

TABLE II
Power Islands Under Different Approaches

$AL_{\text{attack}}^{\max}$ =3	Index of targeted lines	Type of islands	Bus set of each island	Total number of islands
This letter	11, 14, 18	"Island d"-1	{11}	3
		"Island b"-2	{1, 2, 3, 4, 5, 6, 7, 9, 10, 12, 13, 14}	
		"Island d"-3	{8}	
Ref. [7]	7, 10, 19	"Island a"	{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14}	"1"
Ref. [9]	11, 14, 20	"Island a"	{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14}	"1"
Ref. [11]	10, 16, 17	"Island b"-1	{1, 2, 3, 4, 5, 7, 8, 9}	2
		"Island b"-2	{6, 10, 11, 12, 13, 14}	

† "Island a" indicates that the power system remains structurally intact after malicious attacks, where this island is an original undirected graph, as shown in Fig.1. "Island b" indicates that this island is an induced subgraph, as shown in Fig.1. "Island d" indicates that this island is a trivial subgraph. The intact system is still regarded as an original undirected island, and the number of islands is described as "1".

potentially inducing intra-island line overloads. Though the method in [7] can induce line overloads, these overloaded lines do not severely impact the system vulnerability due to their low overload ratios. What's worse, these approaches in [9, 11] cannot cause any line overload. This implies that our approach can induce more severe line overloads compared to existing approaches. As suggested by the NERC Standard PRC-023-1 R1.2 in [8], power line will trip once its power flow exceeds 115% of its rated capacity. To sum up, our approach can additionally induce intra-island line overloads after islanding formation, leading to further failure stages and even cascading events.

TABLE III
Overloaded Lines Under Different Approaches

$AL_{\text{attack}}^{\max}$ =3	Overload lines	Overloading ratio (p.u.)	Load shedding (MW)	Total cost ($)
This letter	2-3	1.04	136.09	23621.67
	2-4	1.02		
	4-5	1.25		
Ref. [7]	4-5	1.04	104.54	19458.54
	5-6	1.03		
	12-13	1.02		
Ref. [9]	\	\	136.42	23607.88
Ref. [11]	\	\	153.93	26867.04

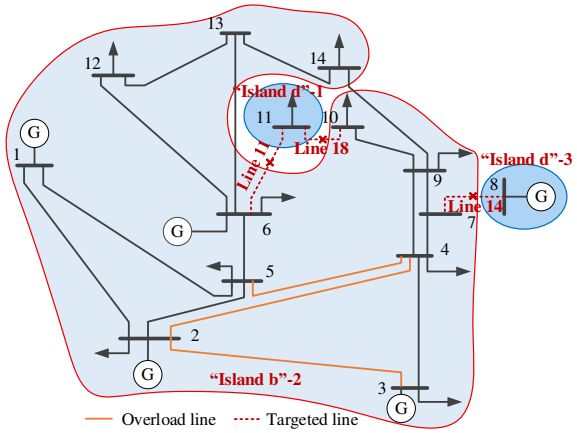


Fig. 2. Distributions of overloaded and targeted lines. ("Island d"-1 and "Island d"-3 are labeled, the remaining part of the system is represented by "Island b"-2).

B. Analysis of Load Shedding and Economic Loss

We further analyse the impacts of our designed island-maximising attacks in terms of load shedding and economic loss. As shown in Table IV, load shedding and economic loss increase with the increase in the attack budget. For example, when the attack budget $AL_{\text{attack}}^{\max} = 3$, load shedding and

economic loss are 136.09 MW and \$4,163.1, respectively, while these impact values rise to 180.95 MW and \$9,572.42 when $AL_{\text{attack}}^{\max} = 4$. This is because our approach can effectively divide the power system into more islands as the attack budget increases, which also reveals the system vulnerability to malicious attacks. Although ref. [6] explicitly maximises the total cost under malicious attacks, its resulting economic loss (\$5,506.17) is still lower than that caused by our method when the attack budget ranges from 4 to 6 lines. This is because ref. [6] does not consider island-maximising mechanism and thus underestimates the operational consequence of multi-line disruptions. Similarly, ref. [11] can only divide the system into two islands, leading to 153.92 MW of load shedding and \$7,408.50 in economic loss, which are also below the results obtained by our approach. These comparisons confirm that our approach reveals more severe and realistic attack consequences. Also, across all attack budgets, the top three targeted lines are 11, 14, and 18. Thus, the system operator is advised to prioritise the defence strategy for lines {11, 14, 18}. In summary, this comparative analysis demonstrates both the effectiveness of our approach and its practical value for resilience-oriented defence decisions.

TABLE IV
SIMULATION RESULTS UNDER DIFFERENT ATTACK BUDGETS

This letter		Index of targeted lines	Load shedding (MW)	Economic loss (\$)	Total number of islands
$AL_{\text{attack}}^{\max}$	3	11, 14, 18	136.09	4163.13	3
	4	11, 14, 16, 18	180.95	9572.42	4
	5	12, 13, 14, 19, 20	185.75	10191.14	4
	6	3, 6, 11, 14, 16, 18	186.50	10309.00	5
Ref. [6]	\	\	149.95	5506.17	"1"
Ref.[11]	\	10, 16, 17	153.92	7408.50	2

† Economic loss is defined as the incremental operation cost of power system caused by island-maximising attacks compared to normal conditions.

C. Practical 36-zone Great Britain System

To further validate the practicality of our proposed approach, additional case studies are conducted on a practical 36-zone Great Britain system with a total load level of 40,000 MW, where these power system zones are connected to each other using 69 lines at the 400 kV transmission level. More detailed data can be referred to [14], which are publicly available. Note that the attack budget is set to 3 lines, and Table V shows the corresponding simulation results.

TABLE V
SIMULATION RESULTS ON THE PRACTICAL 36-ZONE GREAT BRITAIN SYSTEM

Models	Index of targeted lines	Load shedding (MW)	Total cost (\$)	Economic loss (\$)	Number of islands
This letter	46, 48, 50	23140.18	4075283.89	2154721.36	3
	"Island b"-1:{1-24, 34} "Island b"-2:{25-33, 36} "Island d"-3:{35}				
Ref. [6]	\	6359.12	1907624.14	404601.99	"1"
Ref. [7]	16, 24, 31	3589.41	1547850.08	44827.93	"1"
Ref. [9]	1, 2, 10	4457.91	1663092.78	160070.63	"1"
Ref. [11]	42, 43, 48	8850.51	2572448.31	561171.00	2
	"Island b"-1:{1-20, 23, 24, 34} "Island b"-2:{21, 22, 25-33, 35, 36}				

It is evident that our approach can divide the practical system into three isolated power islands by targeting lines 46, 48, and 50, one of which is a trivial island. By contrast, the method in [11] only divides the system into two islands, while these methods in [6, 7, 9] are unable to create any system structural division, where the system remains structurally intact after malicious attacks. Thus, our approach induces 23,140.18 MW of load shedding and a total cost of \$4,075,283.89, both substantially exceeding those obtained in [6, 7, 9, 11]. These results mean that our approach can lead to more significant impacts on the system compared to existing methods, providing a useful tool for vulnerability assessment and strategic defence decisions in power systems. In addition, the computation time of 497.34 seconds confirms the tractability and scalability of our approach, further demonstrating its practicality for CPPS vulnerability analysis.

IV. CONCLUSION

In this letter, we propose a single level mixed-integer programming (MIP) model, based on a graph-theoretic approach, to design island-maximising attacks in cyber-physical power system (CPPS). Such attacks can effectively disrupt lines to divide a power system into the maximum number of power islands. Moreover, such island-maximising attacks can further induce intra-island line overloads while resulting in load shedding and economic loss in the system. Our approach reveals and analyses the new vulnerability of CPPS under the novel island-maximising attacks, providing insightful guidance for the system operator to develop resilience-oriented defence strategies. In the future, we will study the mitigation of island-maximising attacks to improve the resilience of CPPS.

REFERENCES

[1] W. Hao, P. Yao, T. Yang, and Q. Yang, "Industrial Cyber–Physical System Defense Resource Allocation Using Distributed Anomaly Detection," *IEEE Internet of Things Journal,* vol. 9, no. 22, pp. 22304-22314, 2022.

[2] Z. Lian, P. Shi, and M. Chen, "A Survey on Cyber-Attacks for Cyber-Physical Systems: Modeling, Defense, and Design," *IEEE Internet of Things Journal,* vol. 12, no. 2, pp. 1471-1483, 2025.

[3] SANS ICS, "Analysis of the cyber attack on the Ukrainian power grid," Electricity Inf. Sharing Center (E-ISAC), Washington, DC, USA, Rep. 2, Mar. 2016, vol. 388.

[4] P. W. Parfomak, "Physical security of the US power grid: high-voltage transformer substations," ed: Congressional Research Service Washington, DC, 2014.

[5] Y. Luo *et al.*, "External Vulnerability Assessment of Power System under Attack Based on Attack-Defense Game," *IEEE Transactions on Power Systems,* pp. 1-11, 2025.

[6] X. Liu, Z. Li, Z. Shuai, and Y. Wen, "Cyber Attacks Against the Economic Operation of Power Systems: A Fast Solution," *IEEE Transactions on Smart Grid,* vol. 8, no. 2, pp. 1023-1025, 2017.

[7] Y. Tan, Y. Li, Y. Cao, and M. Shahidehpour, "Cyber-Attack on Overloading Multiple Lines: A Bilevel Mixed-Integer Linear Programming Model," *IEEE Transactions on Smart Grid,* vol. 9, no. 2, pp. 1534-1536, 2018.

[8] M. Zhou, C. Liu, A. A. Jahromi, D. Kundur, J. Wu, and C. Long, "Revealing Vulnerability of N-1 Secure Power Systems to Coordinated Cyber-Physical Attacks," *IEEE Transactions on Power Systems,* vol. 38, no. 2, pp. 1044-1057, 2023.

[9] J. M. J. I. g. Arroyo, transmission and distribution, "Bilevel programming applied to power system vulnerability analysis under multiple contingencies," vol. 4, no. 2, pp. 178-190, 2010.

[10] R. S. Biswas, A. Pal, T. Werho, and V. Vittal, "A Graph Theoretic Approach to Power System Vulnerability Identification," *IEEE Transactions on Power Systems,* vol. 36, no. 2, pp. 923-935, 2021.

[11] B. Pradhan, S. S. Paik, D. S. Roy, and D. K. Mohanta, "A sustainable protection scheme for the Indian power system using grid computing: A graph-theoretic approach," in *2011 Annual IEEE India Conference*, 2011, pp. 1-6.

[12] S. Gao, J. Lei, X. Wei, Y. Liu, and T. Wang, "A Novel Bilevel False Data Injection Attack Model Based on Pre- and Post- Dispatch," *IEEE Transactions on Smart Grid,* vol. 13, no. 3, pp. 2487-2490, 2022.

[13] M. Du, X. Liu, Q. Zhou, and Z. Li, "Hybrid Robust Tri-Level Defense Model Against Multiperiod Uncertain Attacks," *IEEE Transactions on Smart Grid,* vol. 13, no. 4, pp. 3255-3265, 2022.

[14] National Energy System Operator, "GB 36-bus electricity transmission network model," 2024. [Online]. Available: https://www.neso.energy/publications/gb-36-bus-electricity transmission -network-model.