Coordinated Cyber-Physical Attack on Power Grids based on Malicious Power Dispatch

Xiaoliang Wang[a], Fei Xue[b,*], Shaofeng Lu[c], Lin Jiang[d], Ettore Bompard[e], Marcelo Masera[e], Qigang Wu[f]

[a] *School of Electronic and Information Engineering, Suzhou University of Science and Technology, Suzhou, China*
[b] *School of Advanced Technology, Xi'an Jiaotong-Liverpool University, Suzhou, China*
[c] *Shien-Ming Wu School of Intelligent Engineering, Guangzhou International Campus, South China University of Technology, Guangzhou, China*
[d] *Department of Electrical Engineering and Electronics, The University of Liverpool, Liverpool, UK*
[e] *Department of Energy, Politecnico di Torino, Turin, Italy*
[f] *School of Electrical and Automation, Changshu Institute of Technology, Suzhou, China*

***Abstract*— This paper proposes a new mode of cyber-physical attack based on injecting false commands, which poses an increasing risk to modern power systems as a typical example of Cyber-Physical Systems (CPS). Such attacks can trigger physical attacks by driving the system into vulnerable states. To address the critical issues arising from this new mode, we define an inverse-community (IC) in power flow distribution and evaluate it using inverse-modularity. To identify the most vulnerable state of the IC that represents the inherent vulnerability of the system, we employ a full malicious power dispatch problem. We also analyze an example of the proposed mode, where a partial malicious power dispatch that maximizes inverse-modularity is combined with physical attacks aimed at disconnecting vulnerable IC boundary lines, making cascading failures highly likely. To demonstrate the potential impact of this coordinated cyber-physical attack, we use the IEEE-118 and IEEE-300 bus systems for simulation. The results show the effectiveness of this attack strategy and provide a new perspective to analyze cyber-physical security issues in modern power systems.**

***Index Terms*— Coordinated cyber-physical attacks, cascading failure, complex network, false command injection.**

I. Introduction

The security of power grids in contemporary society is an unequivocal necessity. Advancements in communication and information technology mean that power systems have evolved from mere physical systems to complex Cyber-Physical Power Systems (CPPS) coupling with communication networks [1], [2]. The backbone of power system operations comprises diverse intelligent cyber infrastructures, like the energy management system and the supervisory control and data acquisition [3]. Nevertheless, these very infrastructures are vulnerable to malicious cyber-attacks [4]. To make matters worse, coordinated cyber-physical attacks aimed at the cyber and physical layers of CPPS can intervene with its operations more effectively than mere cyber attacks [5].

Malicious attacks on power systems can lead to initially undetectable faults that, if not addressed promptly, can eventually lead to failures [6]. The destructive effects of such attacks were evidenced by the 2010 cyber worm named 'Stuxnet', which targeted the Iranian nuclear fuel enrichment plant and tampered with the frequency of electrical current powering the centrifuges through manipulation of the SCADA system [7]. The severe repercussions of these attacks can bring about significant economic losses and result in catastrophic consequences.

Against this backdrop, in recent years, researchers have conducted extensive studies on cyber-physical attacks in power grids. In [8], a framework for a cyber switching attack is explored which has the potential to destabilize a target power system component by manipulating the switching of circuit breakers. Ref [9] has researched on an unobservable state-and-topology cyber-physical attacks strategy that can mask a physical attack by altering both state and topology data of a sub-network within the grid. Their attack model employs a two-step process aimed at increasing power flow on a target line while adhering to constraints on the sub-graph size and the limit on load shifts. Additionally, Ref [10] proposes a local cyber-physical attacks method that disconnects a transmission line and leads to a cascade failure within the system. This method conceals the actual outage event by modifying power flow measurements to misguide the control center into verifying an alternate fake outage line.

False data injection (FDI) attacks have become a highly significant research area in power grid cyber attacks. Ref [11] is among the first to introduce a category of FDI attacks that allowed the attacker to manipulate the data measured by meters after obtaining the network and topology data. FDI attacks are designed to deceive state estimation and evade bad data detection techniques. Ref [12] proposes a specific variant of FDI attack called load redistribution (LR) attacks, which target the security-constrained

* Corresponding author.
E-mail address: xiaoliang.wang@usts.edu.cn (X. Wang), fei.xue@xjtlu.edu.cn (F. Xue), lushaofeng@scut.edu.cn (S. Shao), l.jiang@liverpool.ac.uk (L, Jiang), ettore.bompard@polito.it (E. Bompard), marcelo.masera@polito.it (M. Masera), qigangw@cslg.edu.cn (Q. Wu).

economic dispatch (SCED) to impact power grid operations. These attacks manipulate state estimation to falsify the SCED outcome, thus leading to the possibility of physical attacks. Fu *et al*. [13] describe a strategy involving an initial physical attack causing cascading failure, which is then followed by LR attacks that mislead the re-dispatching through maximum line overloading. Furthermore, some researchers have concentrated on economic attacks through FDI to disrupt the functioning of deregulated electricity markets [14]. In Ref [15], the authors explore how attackers can manipulate electric load data through a reformulated OPF to cause system congestions and negatively impact the security and economy of the system. Naderi *et al* [16]. propose a deep learning framework to identify remedial action schemes against false data injection cyberattacks targeting smart power systems. This innovative approach utilizes long short-term memory cells integrated into a deep recurrent neural network to effectively process data and identify proper reaction mechanisms.

TABLE I SUMMARY OF A RECENT REVIEW ON CYBER-PHYSICAL ATTACKS APPROACHES [7], [17],[18].

Attack type	Objective	Consequence
FDI attack	Incorrect estimated state	Functional failure
LR attack	Incorrect estimated state	Functional failure
Topology attack	Incorrect Topology estimation Manipulating	Incorrect topology state
Aurora attack	Cause damage to generators, motors, and transformers	Electromagnetic torque and current fluctuations
Pricing attack	Mismatch between the generated and the consumed power	System emergencies

Table I summarizes some existing works on the cyber-physical attacks approaches. The aforementioned cyber-physical attacks methodologies utilized different mechanisms during the cyber-physical attacks. However, **the strategy of those different methods of cyber-physical attacks has as its primary objective to mask failures of the power networks by using false data.** Furthermore, the proposed approach in this paper differs from existing data-specific FDI methods in that it is tailored specifically for control commands. This paper investigates a new coordinated cyber-physical attacking mode resulting in malicious power dispatch. A novel metric based on the inverse-community structure is put forward to assess the vulnerability of power networks under cascading failures. Then, by studying the inverse-community structure of a power flow distribution grid as the target of the malicious power dispatch attack, this paper examines a cyber-physical attack strategy that combines a false command injection attack and a physical line disconnection attack, with the possibility of triggering a large-scale cascading failure.

The contributions of this study are summarized as follows:

1. Analysis of a coordinated cyber-physical attacking mode where a false command injection is used to drive the system into a vulnerable state, enabling physical attacks and triggering cascading failures.
2. Introduction of a novel metric, based on inverse-community structure, that assesses the inherent vulnerability of power systems to cascading failures caused by a full malicious power dispatch.
3. Demonstration of a coordinated cyber-physical attack strategy that maximizes the inverse-community modularity in a power flow distribution grid, by partially dispatching malicious power and disconnecting boundary lines to trigger cascading failures.

The paper is structured as follows: Section II reviews previous studies on coordinated cyber-physical attacks, while also presenting a novel coordinated cyber-physical attack mode. Section III introduces the inverse-community (IC) structure, along with a vulnerability assessment index for power systems. Section IV details a vulnerability assessment based on a full-scale malicious power dispatch attack, followed by Section V which provides an examination of a coordinated attack strategy involving partial malicious power dispatch and line disconnection. In Section VI, case studies and simulation results are presented. Finally, Section VII concludes the paper and provides closing remarks.

II. A NEW COORDINATED CYBER-PHYSICAL ATTACKING MODE

Previous studies about Coordinated Cyber-Physical Attacks (CCPA) could be summarized as:

- Cyber attacks with the purpose of masking physical attacks so that the impacts of consequence could be amplified – this is the approach of most previous studies [19-23],
- Cyber attacks are implemented as FDI, mostly after physical attacks [19-23].
- Cyber attacks aim to create obstacles to defense mechanisms by tampering with relevant parameters or blocking measurements [24] [25]. The effects could be quite uncertain due to lack of accurate defense decision models.
- Cyber attacks aiming at load redistribution, misguiding the system defense when facing following physical attacks [26]. The coordination relation between cyber and physical attacks is not clearly described.

As discussed above, compared with FDI attacks, False Command Injection (FCI) attacks have seldom been considered in coordination with cyber-physical attacks. However, the possibility of FCI and the corresponding impacts have been acknowledged [27]. Most previous studies about FCI mainly focused on device-level attacks, such as those affecting switching breakers [28-31], transformer taps [32] and phase shifters [33]. But none of them considered system-level FCI attacks.

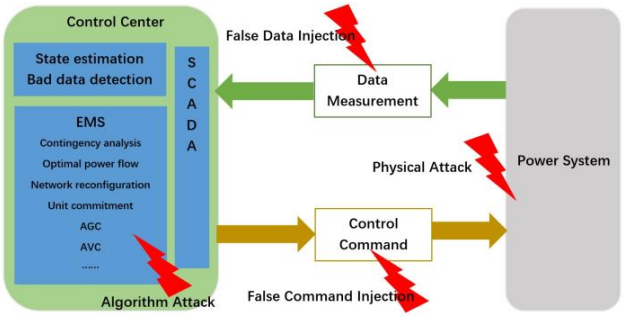

Fig. 1. False Data Injection and False Command Injection.

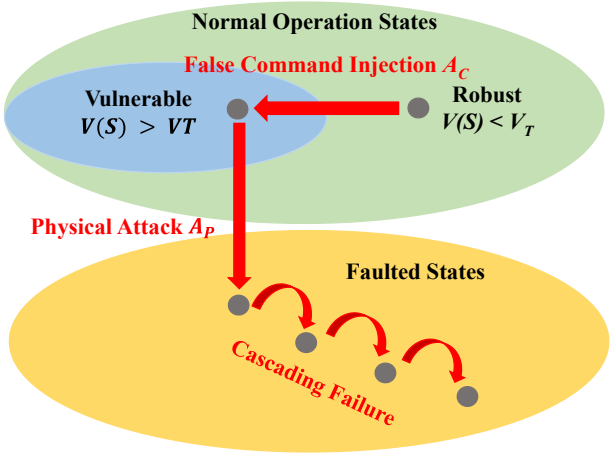

Fig. 2. A new coordinated cyber-physical attacking mode.

As shown in Fig.1, FDI implements the attacks before the measurement data are transmitted to the decision-making segment in the control center. Its aim is to mislead the operation decision-making by manipulating the input information. However, there are great uncertainties regarding the operation decision-making process, especially concerning human intervention. Therefore, the consequence of that data manipulation is difficult to be accurately predicted. On the contrary, FCI directly manipulates the control commands. Nevertheless, if the injected commands are too extreme, one can foresee that they will be suspected as abnormal. The absence of coordinated masks in the feedback measurement renders the attacks undetectable using conventional detection methods, reducing the optimum time frame for FCI to a limited duration. Therefore, FCI may not be quite appropriate to be used independently. Furthermore, as shown in Fig. 1, another possible attacking mode which has never been considered (to the best of our knowledge) is algorithm attack. Following an intrusion into the control center (by itself very difficult), if the algorithm used by the control decision making (such as optimal power flow, unit commitment, automatic generation control) is manipulated, the consequence would be catastrophic.

A new coordinated cyber-physical attacking mode is shown in Fig. 2. In normal operation states, although all operation constraints in terms of equality or inequality could be met, a concrete operation state S could be robust or vulnerable with respect to a specific physical attack strategy A_P. This could be evaluated by a vulnerability metric $V(S)$. By comparing with a threshold V_T, the operation states could be classified into robust or vulnerable. Previous studies about physical attacks have shown that it is difficult to quantitatively evaluate the vulnerability of state S with respect to a physical attack strategy, less so concerning the transition from robust to vulnerable states.

In the new coordinated cyber-physical attacking mode studied here, the FCI attack A_C is performed first. Its purpose is to deceive the system guiding its state from the robust area to the vulnerable area. These robust and vulnerable areas are defined according to the quantitative evaluation $V(s)$. Once the FCI part succeeds, a physical attack strategy A_P is implemented triggering a large-scale cascading failure. As mentioned above, it is not straightforward for a FCI attack acting in isolation to provoke important damages within a short time window. A more suitable role for FCI is to provide leading assistance for physical attacks. On the other hand, the immediate system defense after physical attacks will make more difficult the implementation of a cyber intrusion.

Previous studies concerning physical attacks seldom considered how critical it might be the moment an attack is launched for its effectiveness. This opportune moment for an attack mostly depends on the operational states of the system as determined by the commands from the control center. In the attacking mode studied here, the purpose of the leading cyber FCI attacks is to create better opportune moments for following physical attacks.

For analyzing this FCI-based attacking mode, the following critical issues should be solved:

1. A metric $V(s)$ should be defined to quantitatively assess the vulnerability of the system state regarding potential cascading failures caused by a physical attack strategy A_P.
2. A FCI attack strategy A_C should be identified, and able to transfer the system state from a robust area to a vulnerable area. This attack strategy should typically come from solutions to an optimization problem aiming at the maximization of $V(s)$.
3. The targets of the physical attack A_P should be identified according to the effects of the cyber attack A_C. Consequences of A_C may clearly indicate the most vulnerable components which could be exploited by A_P.

III. Inverse-community structure in power flow distribution

A. *Inverse community structure*

The stability and reliability of power grids can be severely compromised by cascading failures, resulting in catastrophic consequences for public life and significant economic costs for society. A prime example of this is the 2012 Indian blackouts, which caused extensive social impacts and economic losses [34]. The three key characteristics of the cascading failure process are as follows.

- The initial trend is the occurrence of considerable power imbalances between local subnetworks, leading to extensive power transfers between these subnetworks. This can result in voltage instability and potential blackouts.
- The power flowing through transmission lines that connect subnetworks is higher compared to the power flowing through internal transmission lines of each subnetwork.
- The occurrence of initial contingencies in boundary lines can result in a shift of power flow towards other boundary lines with already high loading levels, thereby increasing the probability of cascading failures.

Community structure, within the complex network theory, refers to a group of nodes that are strongly interconnected. Occasionally, clusters of nodes can be strongly linked but only loosely connected to the rest of the network [35], [36]. Our earlier research presented the notion of an inverse-community structure built on the experiences obtained from the cascading failure in India [37]. This approach takes into account the link weights that signify the strength of the interactions within a network. The significant aspects of an IC structure are as follows: (1) The topological correlations are consistent with standard communities; (2) The weight of intra-community links is less than that of inter-community links; (3) With the gradual strengthening of IC features, the network becomes progressively more prone to cascading failures, leading to an increase in its vulnerability level.

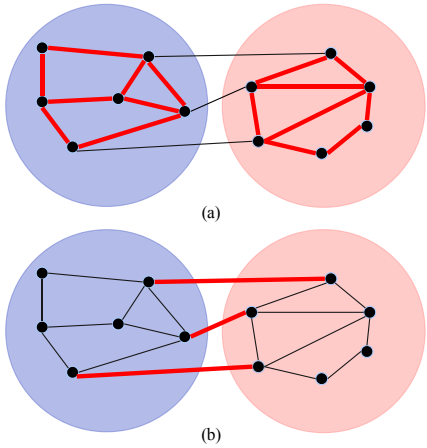

Fig. 3. The illustration of (a) normal community and (b) inverse community.

Fig. 3 illustrates two different network structures: one with a normal community structure and the other with an inverse-community structure. Both structures consist of two separate communities, with the thickness of the branches indicating the relative strength of the connections between nodes. The primary distinguishing feature between the two structures lies in the distribution of weights. In particular, the interactions, such as for power transmission, between communities are considerably more robust compared to those within the communities, which is in stark contrast to the typical community structures characterized by their internal connections being stronger.

B. Inverse modularity

In previous studies about community structures, modularity Q [38] was considered a standard metric to evaluate community features in complex networks [39-41].

In this paper, in order to evaluate the IC structure properties of the network and thus assess its vulnerability, we will apply Q to inverse-modularity, *i.e.* we will define Q_{IC}. First, considering the electrical characteristic of power grids and the features of IC, we propose to quantify the power flow distribution in a specific time section by a temporal weight. The temporal weight τ_{vw} at time t is defined as

$$\tau_{vw}(t) = \frac{1}{|p_{vw}(t)|}, \qquad (1)$$

where $|p_{vw}(t)|$ is the absolute value of power flow in line l_{vw} between bus v and bus w at time t, thus describing the operating state of the power grid at a particular moment t.

The temporal weight matrix $\mathbf{T}_{vw}(t)$ is presented as Equation (2), which taking into account the structural characteristics of power networks.

$$\mathbf{T}_{vw}(t) = \begin{cases} \tau_{vw}(t), & \text{if there is an branch among bus } v \text{ and } w, \\ 0, & \text{otherwise.} \end{cases} \qquad (2)$$

The use of temporal weights allows for the consideration of both the structural properties and operating conditions of power grids, providing insights into the IC structure of networks. Specifically, smaller values of τ_{vw} indicate branches that support greater power transfers. Additionally, the magnitude of τ_{vw} varies across different operating states of power grids.

Based on (1) and (2), **the detection of IC in power flow distribution has been converted into the detection of conventional communities in temporal weight distribution**. Then, the conventional Q is redefined as inverse-modularity Q_{IC} by temporal weight. The Q_{IC} is defined as

$$Q_{IC} = \sum_{vw} \left[\frac{\tau_{vw}}{2\mathrm{M}} - \frac{\tau_v}{2\mathrm{M}} \frac{\tau_w}{2\mathrm{M}} \right] \delta(c_v, c_w) , \qquad (3)$$

where τ_{vw} is the element from bus v to bus w in the temporal weight matrix. The total temporal weight of the whole power gris is expressed as M.

$$\mathrm{M} = \frac{1}{2} \sum_{vw} \mathbf{T}_{vw} . \qquad (4)$$

τ_v (τ_w) is computed as Equation (5), which is the temporal weight degree of bus $v(w)$.

$$\tau_v = \sum_w \tau_{vw} . \qquad (5)$$

In (3), the δ-function is 1 if buses v and w are in the same community, otherwise it is 0.

C. Inverse-community detection

To detect and assess the partitioning outcomes of a network with IC characteristics at a specific time point t, the customary Newman fast algorithm [42] is employed to recognize the inverse community structure by substituting the conventional Q with the inverse modularity. The IC detection algorithm is outlined in Algorithm 1.

Algorithm 1: Inverse-community detection for power network	
	Input: network data, temporal weight matrix
	Output: partitioning results
1 :	Initialize power network with N communities;
2 :	Calculate the inverse modularity Q_{IC};
3 :	**while** the number of communities is not 1 **do**
4 :	Calculate the increments of inverse modularity ΔQ_{IC};
5 :	Select the partitioning with maximum ΔQ_{IC}
6 :	Recalculate Q_{IC} according to the result of partitioning;
7 :	Conserve the number of communities (The maximum number of mergers is N-1);
8 :	**end while**

The objective of this algorithm is to utilize an inverse-community detection approach to partition power networks into smaller sub-communities. The procedure commences by establishing N communities in the power network and computing the Q_{IC}. Subsequently, the algorithm enters a loop where it identifies the maximum ΔQ_{IC} and implements the partitioning with the most significant gain in inverse modularity increments. The number of communities is preserved throughout the process (with the maximum mergers limited to N-1), and Q_{IC} is recalculated based on the partitioning outcome until only one community remains. The algorithm's output is the partitioning outcome.

IV. VULNERABILITY ASSESSMENT BASED ON FULL MALICIOUS POWER DISPATCH

The concept of inverse modularity is a dynamic measure that is influenced by the changing power flow distribution throughout the network over time. For a power grid with specific structural characteristics, such as the network topology, line parameters, and the location and capacity of generators and load buses, there exists a theoretical upper limit for the inverse-modularity value. This Q_{IC}^{MAX} can serve as a metric to assess the grid's vulnerability based solely on its structural attributes.

This section studies a **full malicious power dispatch** (FMPD) attack, considering Q_{IC}^{MAX}. A full malicious power dispatch situation is an optimization problem that considers the output power of all generators and the power demand of all load buses as decision variables and the maximum inverse modularity as the objective function. Based on that, the conventional genetic algorithm (GA) is redesigned to find solutions for this optimization problem.

The power network's condition is influenced by the output power of generators P_g^f and the power consumed by loads P_d^f, resulting in distinct IC structures of the power grids under various power flow situations. The decision variables in this scenario are represented by P_g^f and P_d^f.

$$P_g^f = [P_{g_1}, P_{g_2}, \ldots, P_{g_m}]^T , \qquad (6)$$

$$P_d^f = [P_{d_1}, P_{d_2}, \ldots, P_{d_n}]^T , \qquad (7)$$

where the m represents the total number of generator buses, and the n represents the total number of load buses.

The aim is to maximize the value of Q_{IC}, which can be mathematically represented as:

$$R_{FMPD}(P_g^f, P_d^f) = \mathrm{Max}\left[Q_{IC}(P_g^f, P_d^f) \right] . \qquad (8)$$

In order to make it difficult for the control center to realize that an attacker is using malicious commands to replace the power dispatch's regulation plan, the constraints of the FMPD are consistent with the normal operation of the grid. The constraints are presented as:

$$P_{g_i}^{\min} \le P_g^f \le P_{g_i}^{\max}, \; i = 1, 2, \ldots, m , \qquad (9)$$

$$P_{d_j}^{\min} \le P_d^f \le P_{d_j}^{\max},\ j=1,2,\ldots,n, \tag{10}$$

$$\sum_{i=1}^{m} P_{g_i}^f - \sum_{j=1}^{n} P_{d_i}^f = 0, \tag{11}$$

$$S_{l_\alpha} \le S_{l_\alpha}^{\max}, \alpha = 1, 2, \ldots, L, \tag{12}$$

The generator and load capacity constraints are expressed in Equation (9) and Equation (10), which respectively limit the active power of each generator within lower and upper bounds ($P_{g_i}^{min}$ and $P_{g_i}^{max}$) and the loads within lower and upper bounds of $P_{d_j}^{min}$ and $P_{d_j}^{max}$. The power balance constraint is described in Equation (11), which mandates that the total generator power output matches the load demand in a DC power flow model. Transmission line loadings are constrained by Equation (12), which restricts the maximum power flow on transmission line α to $S_{l_\alpha}^{max}$.

V. Coordinated Attack Based on Partial Malicious Power Dispatch and Line Disconnection

Different from FMPD which utilizes the power of all generators and all load buses as decision variables, in practice, the power of most loads cannot be controlled or dispatched by system operators. Therefore, a **partial malicious power dispatch** (PMPD) is defined here, which only utilizes the output power of all controllable generators as decision variables to search maximum inverse-modularity; while the power of load buses is considered as a given condition.

The objective function of PMPD is expressed as

$$R_{PMPD}(P_g^p) = \mathrm{Max}\left[Q_{IC}(P_g^p)\right]. \tag{13}$$

The decision variables are the actual output power of generators P_g^p.

$$P_g^g = [P_{g_1}, P_{g_2}, \ldots, P_{g_m}]^T \tag{14}$$

The constraints are the same of FMPD, except for the load capacity constraint.

As discussed when describing the coordinated cyber-physical attacking mode in Section II, the inverse-modularity is selected as the metric $V(s)$ to assess the vulnerability of state S to cascading failures. The partial malicious power dispatch is designed as the FCI attack A_C that deceives the system operation to evolve into a vulnerable state. The summarized coordinated cyber-physical attack strategy that he proposed is as follows:

Step 1. The attackers infiltrate the system and gather information about the structure and parameters of the power networks.

Step 2. With structural factors and parameters from the reconnaissance, as well as load distribution for a specific moment t, a partial malicious power dispatch problem is formulated.

Step 3. The partial malicious power dispatch problem corresponding to time t is solved by a genetic algorithm with solutions for generators' output power and corresponding inverse-modularity, as well as the partition solution of ICs.

Step 4. With a given prediction of load for a different moment t, a series of solutions could be obtained from step 3. Based on a comparison of the value of inverse-modularity value, an attacking moment t_A is selected.

Step 5. At t_A, the corresponding solutions of generators' output power from partial malicious power dispatch are injected into EMS as false commands, the output power of generators is changed to the manipulated values, the system operation then reaches a vulnerable state.

Step 6. From the partition solution in step 3 for t_A, all boundary lines of IC structures are collected as potential targets of physical disconnection attacks.

Step 7. According to the resource constraints of physical attacks, the attacker performs disconnection attacks on vulnerable lines selected from the targets set in step 6.

A relative metric R^r for a PMPD attack A_C could be defined as the ratio between its corresponding inverse-modularity Q_{PMPD} and the system inherent vulnerability Q_{FMPD}, which can be expressed as

$$R^r(A_C) = Q_{PMPD} / Q_{FMPD}, \tag{15}$$

where R^r represents to what extent the PMPD attack has utilized the system's inherent vulnerability characteristic.

VI. Case Study

A. Simulation results

In this section, we aim to explore the correlation between Q_{IC} and the likelihood of cascading failures. To this end, we employ a GA to search for power dispatch solutions that vary in theirQ_{IC} values, using the IEEE-300 system as our testbed. The solver we used is the MATLAB global optimization toolbox. We rely on MATCASC [43] to simulate the cascading failure processes. Previous studies [44] have shown this tool to be highly effective for simulating such failures in power grids, as it offers three removal strategies: random removal, edge betweenness centrality, and electrical node significance. However, given the specific IC structure features we wish to examine, we propose an additional removal strategy that leverages the power flow rank of IC boundaries to trigger cascading failures.

To demonstrate a broader range of operating scenarios with notably distinct Q_{IC} values, we have augmented the power capacities of all generators in the IEEE-300 system, thus generating more extreme scenarios. Using the MATCASC tool, we have plotted the Q_{IC} values of various power dispatch scenarios and the corresponding remaining loads after cascading failures in Fig. 4. Our findings indicate that the remaining load diminishes as Q_{IC} increases, clearly illustrating a positive link between inverse-modularity and the likelihood of cascading failures.

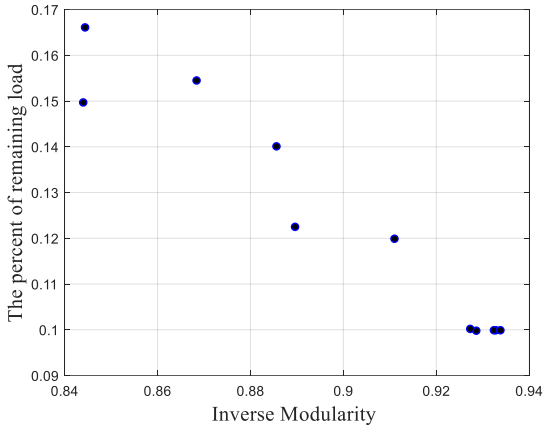

Fig. 4. The different power dispatching schemes in the IEEE-300 system and their corresponding Q_{IC} and remaining loads.

To evaluate the efficacy of the proposed attack approach and metrics, we conduct a second experiment using the IEEE-118 system with standard parameters. Firstly, we employ the Monte Carlo simulation (MCS) to emulate diverse operational scenarios across a 24-hour period for the IEEE-118 bus system. Subsequently, we execute an optimal power flow calculation every hour, considering sampled loads, and obtain the outcomes of the probabilistic load flows via MATPOWER. The stochastic model implemented to represent the loads within the system follows a Gaussian distribution, as stated in [45], [46].

In order to assess the efficacy of our attack approach and measurements, we carried out an additional trial utilizing the customary settings of the IEEE-118 framework. We used Monte Carlo simulation (MCS) to simulate various operating conditions of the system over a 24-hour period. Each hour's optimal power flow was then calculated using sampled loads, and the resulting probabilistic load flow was determined using MATPOWER. The load distribution in the system was modeled using a Gaussian distribution [45], [46].

$$f_{load}(x) \sim N(\mu, \sigma^2). \qquad (16)$$

The probability density function that describes load leveling during the specified target periods, denoted as f_{load}, was determined based on the hourly and seasonal peak loads provided by the IEEE-RTS [47]. The parameters μ and σ were calculated using this data. For IEEE 118 system, the values of μ and σ were set at 0.641 and 0.019 on weekdays and 0.551 and 0.014 on weekend days, respectively. The execution times for IEEE 118 is 40 minutes.

Subsequently, the proposed PMPD is carried out for different load conditions in 24 hours. A critical value of inverse-modularity $Q_{IC}^{critical}$ is set to filter candidate attacking scenarios. The attackers will only consider time points with Q_{IC} larger than $Q_{IC}^{critical}$ as candidate attacking times. In this case, we set the $Q_{IC}^{critical}$ to 0.85. Fig. 5 is the results of Q_{IC} greater than the critical value corresponding to each hour.

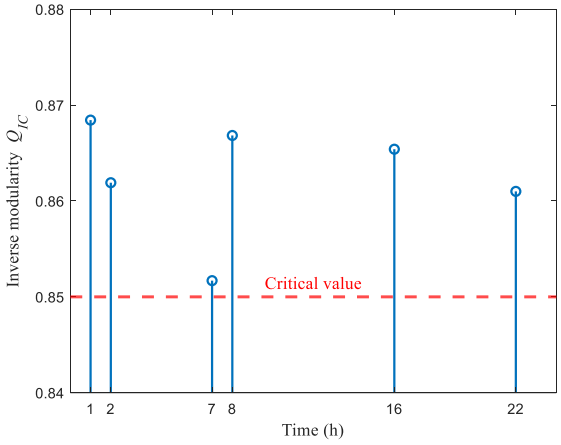

Fig. 5. The inverse-modularity per hour for different loads condition.

The operation states in Fig. 5 have strong IC structural characteristics at the candidate time points. In other words, these moments have higher risks of triggering cascading failures. In this scenario, the residual load is employed as an indicator of the impact of cascading failures on the network.

Table II shows the simulation results of cascading failures at the selected moments in Fig. 5. In Table II, t_1 and t_2 are considered as the moments for continuous PMPD attack. t_1 and t_2 are continuous moments that may provide more length of effective time window to implement subsequent physical attacks. Furthermore, the magnitude of Q_{IC} is close at t_1 and t_2, indicating that the power dispatch commands and system state are not significantly different in this period, which may reduce the risk of being suspected of data manipulation.

TABLE II
THE REMAINING LOAD AT DIFFERENT MOMENT IN FIG. 4.

Time	Q_{IC}	Remaining load
t_1	0.868	62.1%
t_2	0.862	64.2%

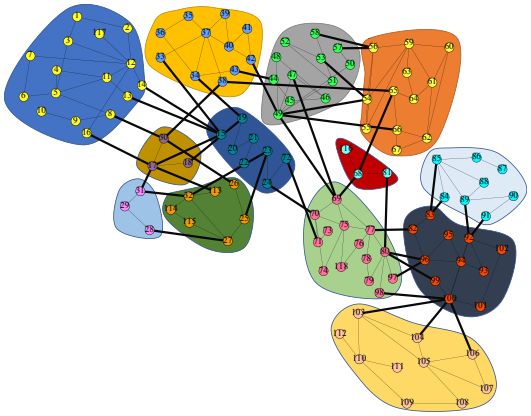

Fig. 6. Inverse community structure of Case 1.

Particularly, the PMPD conforms to the constraints of the system's regular operation. For this reason, the attackers might use the malicious command to replace the regulation plan of power dispatch, as it may not be perceived as a dangerous operation by the system.

B. The effect of PMPD combined with physical attacks

The attackers would intend to inject partial malicious power dispatch commands to make the network reach a greater IC condition. This condition would comply with the standard operational limitations of the power grid, but it would increase the susceptibility of the network to certain targeted physical attack tactics.

Case 1 refers to the simulation results at t_1, which have the most significant impact on the power grid, as shown in Table II. This case is analyzed in detail to investigate the effects of PMPD and physical attacks. At this particular moment, the Q_{IC} of Case 1 has reached its peak value of 0.868, which represents the maximum difference between the weight of the network's external and internal connections. Essentially, this dispatch command has elevated the IC condition of the system. To further illustrate the structure of ICs in Case 1, refer to Fig. 6, while Table III provides information on the power flow rankings of the boundaries between each IC, highlighted by bold lines.

TABLE III
THE POWER FLOW OF IC BOUNDARIES IN CASE 1.

From	To	Power flow (MW)	From	To	Power flow (MW)	From	To	Power flow (MW)
68	69	935.19	26	30	117.85	91	92	32.63
65	68	744.82	42	49	104.27	14	15	28.46
38	65	380.24	83	85	97.1	89	92	28.35
30	38	359.77	96	97	83.42	49	66	20.52
81	80	217.01	80	96	79.7	16	17	20.37
77	82	206.61	15	33	77.76	13	15	19.52
100	103	191.07	19	34	73.39	17	31	19.44
8	30	186.85	83	84	71.64	56	58	16.63
71	72	157.25	100	104	63.64	53	54	15.54
47	69	146.98	43	44	62.85	49	54	13.11
49	69	145.69	17	113	58.78	31	32	12.38
23	25	142.28	23	32	51.96	56	57	12.15
80	99	139.98	100	106	51.95	27	28	9.2
24	70	136.01	18	19	43.77			
98	100	135.51	15	17	37.93			

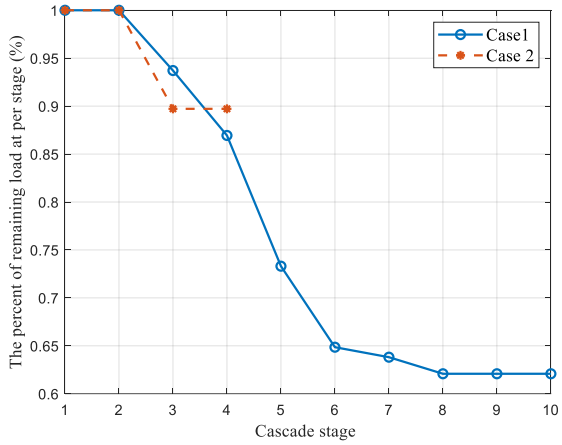

Fig. 7. The load that is left after each cascade stage in Case 1 and Case 2.

We assume that the attackers can at this moment tamper the original plan of generators into malicious power dispatch by cyber-attack. Subsequently, the attackers choose the boundaries with larger power flow as the target of physical attacks to trigger cascading failures. Fig. 7 shows for Case 1 the severity of cascading failures when the boundary (68-69) is attacked. The remaining load is 62.1% at the last cascade stage, that is, 38% of loads are damaged.

To confirm the efficiency of the examined cyber-physical attack model, the conventional optimal power flow (OPF) based on MATPOWER is utilized for simulating the usual power dispatch from the power control center. We set a Case 2 with the same load condition with Case 1, but where the power dispatch of generators is obtained by OPF. Three boundary lines (8-30, 12-16 and 15-17) are disconnected to simulate a physical attack. For Case 2, the Q_{IC} is 0.697, smaller than in Case 1 (Q_{IC}=0.868). Therefore, the IC structure of Case 2 is obviously weaker than in Case1. In other words, Case 2 is more insensitive to cascading failure than Case 1. The remaining load per cascade stage of Case 1 and Case 2 is illustrated in Fig. 7. It can be seen from the dashed line that Case 2 did not have a cascading failure, but only some areas lost loads due to line disconnection. The remaining load of Case 2 is 89.7%, much higher than in Case 1 (62.1%). This result supports the previous conclusions and verifies that the studied malicious power dispatch attack model causes more severe damage to power grids than normal operation of the grids.

To understand how various attack strategies can potentially impact networks, we compared our proposed removal strategy, which is based on power flow at boundaries, to other removal strategies in [43]. Table IV displays the remaining loads for different attack strategies in Case 1 and Case 2. The results show that the effects of all three attack strategies are similar and that Case 1 is more severe than Case 2. This finding supports the notion that the state based on PMPD is highly vulnerable to cascading failures when subjected to targeted physical attacks. Additionally, we found that the physical attack strategy that relies on power flow at IC boundaries with malicious power dispatch inflicts more damage on power grids than the other two strategies.

TABLE IV
THE LOAD LEFT IN CASE 1 AND CASE 2 UNDER DIFFERENT ATTACK STRATEGIES.

	IC Boundaries power flow	Edge betweenness centrality	Electrical node significance
Case 1	**62.1%**	66.3%	68.2%
Case 2	89.7%	89.7%	89.7%

C. *Vulnerability assessed by full malicious power dispatch*

In this section, the IEEE-118 and IEEE-300 bus systems are used to study the potential effectiveness of a full FMPD, in order to evaluate the most vulnerable state of the system. We assume that a cyber-attack can alter the power dispatch plan for both loads and generators. This may not be quite achievable in practice because the injected false commands cannot control most loads. However, in theory, this most vulnerable state only depends on inherent system structure and parameters. Nevertheless, we can suppose that physical attacks with the same attack strategy discussed in the previous section could be implemented following this FMPD.

In Fig. 8, we observe the remaining loads post-physical attacks that follow FMPD. For the state of IEEE-118, the Q_{IC}value is 0.887, and the remaining load in the final cascade stage is approximately 47.2%, which is substantially lower compared to the results obtained for Case 1 and Case 2. Notably, the cascading failure process precipitated by FMPD unfolds more rapidly. This finding implies that the power system exhibits lower tolerance to FMPD compared to Case 1 and Case 2.

Although FMPD is an extreme case not achievable in practice, this analysis indicates that with more demand side resources involved in power dispatch in the future for smart grids, the risks under coordinated cyber-physical attacks may increase significantly. The ratio R^r_{case1} in Case 1 is 0.9788, which is higher than for Case 2 (R^r_{case2}=0.7860). The result means that Case 1 exploits the inherent vulnerability of the system more than Case 2, that is, PMPD can make the best of system's inherent vulnerability characteristic.

The study also employs the IEEE-300 system to validate the inherent vulnerability of various power systems. Simulation of FMPD in the IEEE-300 system yields Q_{IC} value of 0.8938. The higher Q_{IC} value compared to the IEEE-118 system indicates that the inherent structure and parameters of the IEEE-300 system make it more susceptible. In Fig.8, the simulated outcome for the IEEE-300 bus system is presented by the dashed line. The remaining load for this system is around 14.4%, which is significantly lower than the remaining load of the IEEE-118 system (47.2%). This result indicates that the cascade failure process in the IEEE-300 bus system progresses at a faster pace, underscoring its lower tolerance capacity.

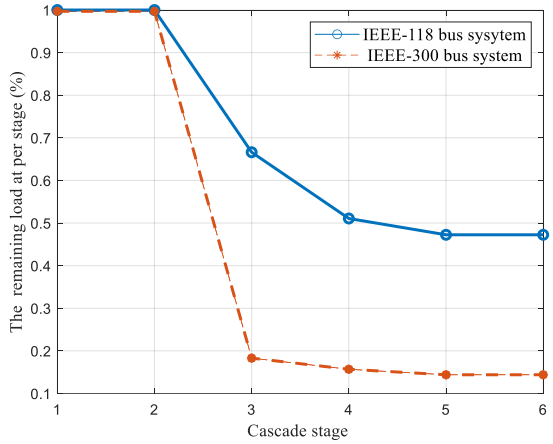

Fig.8. The residual load at each stage is determined by the intentional power dispatch on loads and generators.

VII. CONCLUSION

The present study investigates a novel cyber-physical attack methodology that leverages FCI, distinguishing it from preceding examinations into CCPA. In this approach, FCI serves as a means to maneuver the system functionality towards a vulnerable state. Although this FCI attack alone may not trigger significant-scale disruptions, it can be combined with physical attacks to amplify its impact.

The paper also shows how IC in power flow distribution can be utilized by this attack strategy to state the vulnerability of system states. We examine both FMPD and PMPD as means for reaching the objective of maximum inverse modularity. The purpose of FMPD is to evaluate the inherent system vulnerability. PMPD advances the FCI attack strategy by facilitating the triggering of cascading failures following the disconnection of a line.

Our analysis and simulation have indicated that FCI attacks may not be suitable to work in isolation. On the contrary, their potential increases by coordinating them with specific physical attacks. In this way, the studied CCPA strategy may cause significant damage to the targeted system.

The PMPD conforms to the constraints on the normal operation of power grids, which means that the control center would hardly be aware that the attackers use malicious commands to replace the regulation plan for power dispatch. The simulation results indicate that the studied malicious power dispatch attack model has the potential to cause more severe damage to the power grids than other approaches.

As far as our understanding goes, malicious power dispatch has not been contemplated as a system-wide FCI attack strategy until now. The inclusion of line disconnection attacks in the PMPD is just one instance of this proposed method. This mode presents vast opportunities for expansion via alternative vulnerability metrics, diverse FCI attack strategies, and physical attack strategies. The integration of FMPD and PMPD findings, together with greater involvement of demand side resources in power dispatch, could substantially heighten the system's vulnerability to CCPA.

Acknowledgments

This work was partially supported by the project of the National Natural Science Foundation of China (52377117), the XJTLU Research Development Fund (RDF-18-01-04) and partially supported by the XJTLU AI University Research Centre, Jiangsu Province Engineering Research Centre of Data Science and Cognitive Computation at XJTLU and SIP AI innovation platform (YZCXPT2022103).

CRediT authorship contribution statement

Xiaoliang Wang: Conceptualization, Software, Visualization, Writing – original draft, Writing – review & editing. **Fei Xue**: Methodology, Investigation, Supervision, Writing – review & editing. **Shaofeng Lu**: Methodology. **Lin Jiang:** Conceptualization, Validation. **Ettore Bompard**: Supervision, Writing – review & editing. **Marcelo Masera**: Methodology, Writing – review & editing. **Qigang Wu:** Validation, Data curation.

Declaration of Competing

Interest The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

The data that has been used is confidential.

REFERENCES

[1] S. Xu, Y. Xia, and H.-L. Shen, "Analysis of malware-induced cyber attacks in cyber-physical power systems," *IEEE Transactions on Circuits and Systems II: Express Briefs,* vol. 67, no. 12, pp. 3482-3486, 2020.

[2] L. Chen, D. Yue, C. Dou, J. Chen, and Z. Cheng, "Study on attack paths of cyber attack in cyber-physical power systems," *IET Generation, Transmission Distribution,* vol. 14, no. 12, pp. 2352-2360, 2020.

[3] S. K. Mazumder, A. Kulkarni, S. Sahoo, F. Blaabjerg, H. A. Mantooth, J. C. Balda, Y. Zhao, J. A. Ramos-Ruiz, P. N. Enjeti, and P. Kumar, "A Review of Current Research Trends in Power-Electronic Innovations in Cyber–Physical Systems," *IEEE Journal of Emerging Selected Topics in Power Electronics,* vol. 9, no. 5, pp. 5146-5163, 2021.

[4] S. Amini, F. Pasqualetti, and H. Mohsenian-Rad, "Dynamic load altering attacks against power system stability: Attack models and protection schemes," *IEEE Transactions on Smart Grid,* vol. 9, no. 4, pp. 2862-2872, 2016.

[5] A. S. Musleh, G. Chen, and Z. Y. Dong, "A survey on the detection algorithms for false data injection attacks in smart grids," *IEEE Transactions on Smart Grid,* vol. 11, no. 3, pp. 2218-2234, 2019.

[6] Y. Ding, X. Wang, D. Zhang, X. Wang, L. Yang, and T. Pu, "Research on key node identification scheme for power system considering malicious data attacks," *Energy Reports,* vol. 7, pp. 1289-1296, 2021.

[7] H. Zhang, B. Liu, and H. Wu, "Smart grid cyber-physical attack and defense: A review," *IEEE Access,* vol. 9, pp. 29641-29659, 2021.

[8] A. Farraj, E. Hammad, A. Al Daoud, and D. Kundur, "A game-theoretic analysis of cyber switching attacks and mitigation in smart grid systems," *IEEE Transactions on Smart Grid,* vol. 7, no. 4, pp. 1846-1855, 2015.

[9] J. Zhang, and L. Sankar, "Physical system consequences of unobservable state-and-topology cyber-physical attacks," *IEEE Transactions on Smart Grid,* vol. 7, no. 4, 2016.

[10] H.-M. Chung, W.-T. Li, C. Yuen, W.-H. Chung, Y. Zhang, and C.-K. Wen, "Local cyber-physical attack for masking line outage and topology attack in smart grid," *IEEE Transactions on Smart Grid,* vol. 10, no. 4, pp. 4577-4588, 2018.

[11] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information System Security,* vol. 14, no. 1, pp. 1-33, 2011.

[12] Y. Yuan, Z. Li, and K. Ren, "Modeling load redistribution attacks in power systems," *IEEE Transactions on Smart Grid,* vol. 2, no. 2, pp. 382-390, 2011.

[13] J. Fu, L. Wang, B. Hu, K. Xie, H. Chao, and P. Zhou, "A sequential coordinated attack model for cyber-physical system considering cascading failure and load redistribution," *2018 2nd IEEE Conference on Energy Internet and Energy System Integration (EI2)*, pp. 1-6, 2018.

[14] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, "A review of false data injection attacks against modern power systems," *IEEE Transactions on Smart Grid,* vol. 8, no. 4, pp. 1630-1638, 2016.

[15] E. Naderi and A. Asrari, "Approaching Optimal Power Flow From Attacker's Standpoint To Launch False Data Injection Cyberattack," 2020 IEEE Green Energy and Smart Systems Conference (IGESSC), Long Beach, CA, USA , pp. 1-6, 2020.

[16] E. Naderi and A. Asrari, "A Deep Learning Framework to Identify Remedial Action Schemes Against False Data Injection Cyberattacks Targeting Smart Power Systems," in *IEEE Transactions on Industrial Informatics*, 2023.

[17] M. K. Hasan, A. K. Habib, et al. "Review on cyber-physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations." in *Journal of Network and Computer Applications*, vol. 209, pp. 103540, 2023.

[18] S. Kim, K. -J. Park and C. Lu, "A Survey on Network Security for Cyber–Physical Systems: From Threats to Resilient Design," in *IEEE Communications Surveys & Tutorials*, vol. 24, no. 3, pp. 1534-1573, 2022.

[19] Z. Li, M. Shahidehpour, A. Alabdulwahab, and A. Abusorrah, "Analyzing locally coordinated cyber-physical attacks for undetectable line outages," *IEEE Transactions on Smart Grid,* vol. 9, no. 1, pp. 35-47, 2016.

[20] Z. Li, M. Shahidehpour, A. Alabdulwahab, and A. Abusorrah, "Bilevel model for analyzing coordinated cyber-physical attacks on power systems," *IEEE Transactions on Smart Grid,* vol. 7, no. 5, pp. 2260-2272, 2015.

[21] R. Deng, P. Zhuang, and H. Liang, "CCPA: Coordinated cyber-physical attacks and countermeasures in smart grid," *IEEE Transactions on Smart Grid,* vol. 8, no. 5, pp. 2420-2430, 2017.

[22] R. J. R. Kumar, and B. Sikdar, "Detection of stealthy cyber-physical line disconnection attacks in smart grid," *IEEE Transactions on Smart Grid,* vol. 12, no. 5, pp. 4484-4493, 2021.

[23] D. Bienstock, and M. Escobar, "Stochastic defense against complex grid attacks," *IEEE Transactions on Control of Network Systems,* vol. 7, no. 2, pp. 842-854, 2019.

[24] W. Bi, K. Zhang, Y. Li, K. Yuan, and Y. Wang, "Detection scheme against cyber-physical attacks on load frequency control based on dynamic characteristics analysis," *IEEE Systems Journal,* vol. 13, no. 3, pp. 2859-2868, 2019.

[25] S. Soltan, P. Mittal, and H. V. Poor, "Line failure detection after a cyber-physical attack on the grid using Bayesian regression," *IEEE Transactions on Power Systems,* vol. 34, no. 5, pp. 3758-3768, 2019.

[26] H. He, S. Huang, Y. Liu, and T. Zhang, "A tri-level optimization model for power grid defense with the consideration of post-allocated DGs against coordinated cyber-physical attacks," *International Journal of Electrical Power Energy Systems,* vol. 130, pp. 106903, 2021.

[27] Y. Zhang, L. Wang, Y. Xiang, and C.-W. Ten, "Inclusion of SCADA cyber vulnerability in power system reliability assessment considering optimal resources allocation," *IEEE Transactions on Power Systems,* vol. 31, no. 6, pp. 4379-4394, 2016.

[28] S. Liu, B. Chen, T. Zourntos, D. Kundur, and K. Butler-Purry, "A coordinated multi-switch attack for cascading failures in smart grid," *IEEE Transactions on Smart Grid,* vol. 5, no. 3, pp. 1183-1195, 2014.

[29] S. Liu, S. Mashayekh, D. Kundur, T. Zourntos, and K. Butler-Purry, "A framework for modeling cyber-physical switching attacks in smart grid," *IEEE Transactions on Emerging Topics in Computing,* vol. 1, no. 2, pp. 273-285, 2013.

[30] F. Wei, Z. Wan, and H. He, "Cyber-attack recovery strategy for smart grid based on deep reinforcement learning," *IEEE Transactions on Smart Grid,* vol. 11, no. 3, pp. 2476-2486, 2019.

[31] J. Yan, H. He, X. Zhong, and Y. Tang, "Q-learning-based vulnerability analysis of smart grid against sequential topology attacks," *IEEE Transactions on Information Forensics Security and Communication Networks,* vol. 12, no. 1, pp. 200-210, 2016.

[32] S. Chakrabarty, and B. Sikdar, "Detection of hidden transformer tap change command attacks in transmission networks," *IEEE Transactions on Smart Grid,* vol. 11, no. 6, pp. 5161-5173, 2020.

[33] S. Chakrabarty, and B. Sikdar, "Detection of malicious command injection attacks on phase shifter control in power systems," *IEEE Transactions on Power Systems,* vol. 36, no. 1, pp. 271-280, 2020.

[34] T. E. C. M. o. Power, "Report of the enquiry committee on grid disturbance in northern region on 30th July 2012 and in northern, eastern and north-eastern region on 31st july 2012," *Government of India.Tech. Rep*, August, 2012.

[35] S. Fortunato, "Community detection in graphs," *Physics Reports-Review Section of Physics Letters,* vol. 486, no. 3-5, pp. 75-174, Feb, 2010.

[36] M. Newman, *Networks*: Oxford university press, 2018.

[37] X. Wang, F. Xue, Q. Wu, S. Lu, L. Jiang, and Y. Hu, "Evaluation for Risk of Cascading Failures in Power Grids by Inverse-Community Structure," *IEEE Internet of Things Journal*, vol. 10, no. 9, pp. 7459-7468, May 2023.

[38] M. E. J. Newman, "Fast algorithm for detecting community structure in networks," *Physical Review E,* vol. 69, no. 6, Jun, 2004.

[39] X. Zhou, K. Yang, Y. Xie, C. Yang, and T. Huang, "A novel modularity-based discrete state transition algorithm for community detection in networks," *Neurocomputing,* vol. 334, pp. 89-99, 2019.

[40] J. Zhu, B. Chen, and Y. Zeng, "Community detection based on modularity and k-plexes," *Information Sciences,* vol. 513, pp. 127-142, 2020.

[41] D. Zhuang, J. M. Chang, and M. Li, "DynaMo: Dynamic community detection by incrementally maximizing modularity," *IEEE Transactions on Knowledge Data Engineering,* vol. 33, no. 5, pp. 1934-1945, 2019.

[42] M. E. J. Newman, "Analysis of weighted networks," *Physical Review E,* vol. 70, no. 5, Nov, 2004.

[43] Y. Koc, T. Verma, N. A. M. Araujo, and M. Warnier, "MATCASC: A tool to analyse cascading line outages in power grids," *2013 IEEE International Workshop on Intelligent Energy Systems (IWIES)*, pp. 143-148, 2013.

[44] R. Sen 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, Mar, 2021.

[45] K. Zou, A. P. Agalgaonkar, K. M. Muttaqi, and S. Perera, "Distribution System Planning With Incorporating DG Reactive Capability and System Uncertainties," *IEEE Transactions on Sustainable Energy,* vol. 3, no. 1, pp. 112-123, Jan, 2012.

[46] Y. V. Makarov, C. Loutan, J. Ma, and P. de Mello, "Operational Impacts of Wind Generation on California Power Systems," *IEEE Transactions on Power Systems,* vol. 24, no. 2, pp. 1039-1050, May, 2009.

[47] C. Grigg, and e. al., "The IEEE reliability test system - 1996. A report prepared by the reliability test system task force of the application of probability methods subcommittee," *IEEE Transactions on Power Systems,* vol. 14, no. 3, pp. 1010-1018, Aug, 1999.