IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received April 30, 2020, accepted June 12, 2020, date of publication July 2, 2020, date of current version July 31, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3006555

Pattern Analysis of Topological Attacks in Cyber-Physical Power Systems Considering Cascading Outages

ZHIMEI ZHANG, (Graduate Student Member, IEEE),
SHAOWEI HUANG, (Member, IEEE),
FENG LIU, (Senior Member, IEEE),
AND SHENGWEI MEI, (Fellow, IEEE)
Department of Electrical Engineering, Tsinghua University, Beijing 100084, China

Corresponding authors: Shaowei Huang (huangsw@mail.tsinghua.edu.cn) and Shengwei Mei (meishengwei@mail.tsinghua.edu.cn)

This work was supported by the National Science Foundation of China under Grant U1766203.

ABSTRACT Modern cyber-physical power systems are vulnerable to cyber attacks. Given that cyber and physical networks are coupled tightly, attacks in the cyber layer can penetrate the physical layer, causing the outage of transmission lines and other physical equipment, thus changing the topology of the grid. In some extreme scenarios, the topological change will disrupt the emergency response of the grid, eventually causing cascading outages along with a blackout. Therefore, as the defender, the operator of a cyber-physical power system should identify critical cyber attacks. In this paper, patterns of sequential cyber topological attacks are analyzed. Firstly, a coordinated attack process is established, including mechanism and probability analysis considering the different timescales. Secondly, the concept of patterns is defined as minimal attack sequences aimed at causing blackouts. Furthermore, the representativeness of patterns is illustrated, which can significantly reduce the storage of risky attack sequences. Thirdly, to address the problem that the identification of patterns is computationally intensive, a search strategy that selects the next attack target dynamically and increases the search depth gradually is proposed to avoid unnecessary search trials. Lastly, tests are carried out on the IEEE 39-node system using the AC power flow model, which validates the representativeness of patterns and the performance of the proposed search strategy.

INDEX TERMS Cascading outages, cyber attack, pattern, topological attack, tree search.

I. INTRODUCTION

Modern power systems are more coupled with cyber infrastructures than ever before [1]. The emerging various types of cyber equipment provide information flow, enhance the ability to flexibly and economically control the grid, and thus make power systems smarter and more intelligent. As the two networks interact intensively, modern power systems are no longer physical networks alone in the conventional sense. In this way, both the physical and cyber networks should be considered as an integrated one, called Cyber-Physical Power System (CPPS).

However, if there are outages in the cyber layer, the physical layer will also be affected [2]. During the outage, the delivery of the data packages is delayed or even lost, which makes the situation awareness weakened. The cyber outage will further disrupt the actuation of control or even emergency response, resulting in major blackouts. While the CPPS usually has firewalls and other defenses, it is still vulnerable to malicious attacks. Therefore, the risk of cyber attacks cannot be ignored but should be studied.

Malicious attacks can be divided into three types, namely False Data Injection Attack (FDIA) [3], False Command Injection Attack (FCIA) [4] and Distributed Denial of Service (DDoS) attack [5], [6]. The former two refer to unauthorized agents intruding a system and falsifying its data. The FDIA falsifies measurement data, whereas the FCIA forges control instructions of breakers or other equipment. Therefore, after an FCIA, breakers may malfunction, causing the topology of the grid changed. The DDoS attack aims at paralyzing the communication network by producing mass invalid data packages. This characteristic makes the DDoS attack suitable as an auxiliary attack of the FDIA or FCIA.

The associate editor coordinating the review of this manuscript and approving it for publication was Sofana Reka S.

In general, researches on the FDIA show that it is gentle and does not jeopardize the stability of the system. Although the FDIA can cause economic loss to the CPPS [7], by disrupting the optimal power flow (OPF) in an undetectable manner [8], it is difficult to induce severe outages because of its limitations and constraints [9]. So operators of the CPPS should also pay attention to other kinds of cyber attacks to mitigate the risk of severe blackouts.

According to [10], [11], power networks are heterogeneous complex networks that are vulnerable to intended topological changes. The FCIA can change the topology of a power grid by attacking breakers, so it is a critical part of the topological attack. Researches have highlighted the threat of topological attacks. Ref. [12] predicted risky areas in a heterogeneous CPPS under topological attacks. In both [13] and [14], the authors proposed a cyber-physical coordinated attack scheme, which trips a transmission line physically while falsifying measurements in the cyber layer, to mislead operators and thus cause load shedding. Meanwhile, authors in [15] constructed a framework of topological attacks targeting non-backbone lines, which is to disrupt the economic dispatch of power systems. Not all attacks are necessarily successful, the probability of which depends on the capability (resources) of the attacker. To maximize/minimize the expectation of topological attacks, a model of optimal resource allocation considering both attackers and defenders are presented in [4]. However, the existing work does not consider the consequence of cascading outages. While authors in [14] mentioned the possibility of cascading outages caused by the topological attack, they did not analyze the process in depth. Ref. [16] established a tri-level optimization model and then concluded that attackers should choose the attack strategy that would cause cascading failures. However, it did not illustrate the multilevel cascading process of the power system. Therefore, we still need to explore the mechanism of cyber topological attacks and the process of the following cascading outages.

As the CPPS has several defenses, attackers should use multiple types of attacks to cause a blackout. In this paper, a process of coordinated topological attacks is proposed. To identify risky attacks schemes, the pattern of attacks is defined, as a minimal series of attacks able to initiate cascading outages. So patterns help operators identify truly risky outages. Then an efficient search strategy is proposed. The contributions of this paper are threefold:

1) A process of coordinated cyber topological attacks in the CPPS, which can cause cascading outages, is established. It incorporates different kinds of attacks to achieve the final target and makes cover-up. Therefore, the synthesized attack formulates a novel type of security threat of the CPPS.
2) The concept of the pattern of topological attacks is proposed. In this paper, the pattern is defined as the minimal attack sequence extracted from attack sequences. Therefore, patterns can represent many risky attack sequences, thus reducing the storage and computational resources significantly while keeping the key information. This is helpful for further risk mitigation.
3) An efficient sequential search strategy is presented. It dynamically selects the next attack target and gradually increases the search depth. The above features enhance the performance and accuracy, and make it outperform the existing similar method.

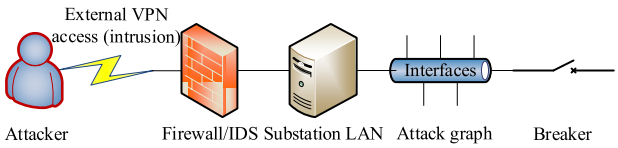

FIGURE 1. Mechanism of the topological attack.

The remainder of this paper is organized as follows. Section II formulates the procedure of coordinated cyber topological attacks. Section III defines the attack sequence and pattern. The loss of the physical network resulting from the attacks is then assessed. Section IV proposes the ''gradual'' search strategy to identify patterns more effectively. Section V presents test results of the IEEE 39-node system. Finally, conclusions are drawn in Section VI.

II. PROCESS OF COORDINATED CYBER TOPOLOGICAL ATTACK

In this Section, we establish the process of a coordinated malicious cyber topological attack, including intrusion, FCIA, and post-contingency DDoS attack. These steps target the confidentiality, integrity, and availability of the CPPS, respectively. After the attack, the outage is transferred from the cyber layer to the physical layer (breaker), as shown in Fig. 1. The mechanism and probability of the three steps are analyzed in the following subsections, respectively. Considering different events have different timescales, it is worth clarifying the time effect of each dynamic at first.

An example of a sequence of successful cyber topological attacks is illustrated in Fig. 2. In this example, the attacker took 10 hours (10 middle-term periods) to learn about a loophole. Then it launched the intrusion, followed by three FCIAs. As a result, three transmission lines were tripped. The defender tried to perform a redispatch but failed due to the interruption of DDoS attacks. Finally cascading outages were induced, which triggered an emergency load shedding with major loss of load. The attacks and the following outages occurred in just several minutes (less than a middle-term period), so the overall process is within a long-term period (96 hours).

A. TIMESCALE OF CPPS DYNAMICS

The attacker needs preparation to successfully implement an intrusion [17]. Meanwhile, the security of the cyber environment has been strengthened with the assistance of the periodic security patch installation. Moreover, after the intrusion, it should instead launch the FCIA as swiftly as possible to let the attack take into effect before detected. Therefore, these different dynamics should be addressed separately.

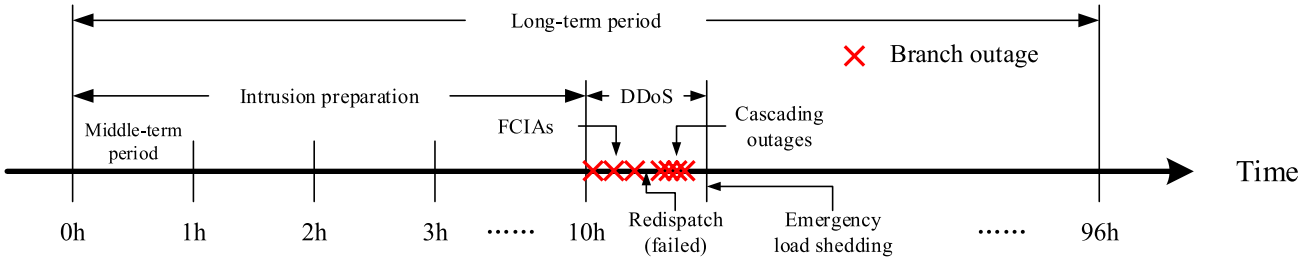

FIGURE 2. Example of cyber topological attacks on a time scale.

TABLE 1. Timescales of Major Dynamics in the CPPS.

Timescale	Time span	Cyber dynamics	Physical dynamics
Short	seconds to minutes	FCIA	Relay protection Emergency control
Middle	quarters to hours	Intrusion preparation DDoS attack	Redispatch
Long	days to weeks	Security patch installation	Topology change

In this paper, we categorize cyber-related processes into long, middle, and short timescales. The main events of each timescale are shown in Table 1, which is slightly different from those in [18] because this paper considers both physical and cyber dynamics.

1) SHORT-TERM PROCESS

The FCIA is with the short-term timescale, which occurs in just a few seconds. Meanwhile, in the physical network, the relay protection will be triggered shortly after the corresponding component is overloaded. The emergency control (load shedding or disconnection) may further be activated if the stability is endangered, which is also performed fast.

2) MIDDLE-TERM PROCESS

This category includes intrusion preparation, DDoS attack, and post-contingency redispatch. Before breaking through cyber defenses to finally accomplish the intrusion, the attacker should first discover and exploit a software loophole, which takes time to make itself well-prepared. The time needed is usually several hours, therefore belonging to the middle-term process. Besides, it takes a quarter or so to ramp up/down generators, so the post-contingency redispatch is also considered in this process. In the meantime, DDoS attacks are executed to interrupt that redispatch, so they should last a period no shorter than that of the redispatch.

3) LONG-TERM PROCESS

Like any other cyber system, the manufacturer of cyber equipment releases security patches periodically, which repair known vulnerabilities and thus strengthen the security level of the CPPS. Additionally, after one day or longer of operation, the grid may change its topology by the unit commitment and bus split. Therefore, both two factors demand that the attacker implement the topological attack within one long-term period, or its preparation will be undone.

B. INTRUSION

1) MECHANISM

Before launching an attack, the attacker should first illegally get access to the cyber system and grab the control authority. Under the normal condition, the network maintains its confidentiality, which prevents an unauthorized agent from obtaining private information. However, according to [19], the confidentiality of the system can be compromised by the local or remote intrusion, which includes exploiting poorly configured firewalls, utilizing backdoors in the network perimeter, and hijacking the VPN connection.

The existence of software loopholes is rare but inevitable, because of the large scale and complexity of the software. To reduce the risk, vendors will release regular security patches, which can plug the known vulnerabilities. Therefore, the attacker should finish the discovery and exploitation of a software loophole within a long-term process, or the loophole will likely expire. Considering the rarity of the loophole, we assume that there is only one available loophole yet to be repaired during a long-term process. Meanwhile, the defender of the CPPS would also scan and try to repair any vulnerability of the cyber network (independent of the software manufacturer). So the two agents compete with each other.

2) PROBABILITY EVALUATION

Both the attacker and the defender would take time to learn about the newly identified loophole to improve their action schemes. Suppose the attacker's and the defender's degree of understanding of the loophole is $K_A(t_A)$ and $K_D(t_D)$, respectively. Either of $K_A(t_A)/K_D(t_D)$ increases with their learning time t_A/t_D, which is a Poisson process [20]. Here, we use different notations of time, because they identify the same loophole independently, maybe at different time points.

Then the probability Pr_1 of a successful intrusion through this loophole is

$$\begin{aligned}\mathrm{Pr}_1(t_A, t_D) &= K_A(t_A)(1 - K_D(t_D)) \\ &= (1 - e^{-\tau_A t_A})e^{-\tau_D t_D}\end{aligned} \tag{1}$$

where τ_A and τ_D are the capability of the attacker and the defender, respectively. A larger τ_A or a smaller τ_D will lead to a larger Pr_1.

The time difference between the attacker and the defender of the discovery of a loophole has a significant impact on Pr_1. Fig. 3 shows an example. While the understanding of the

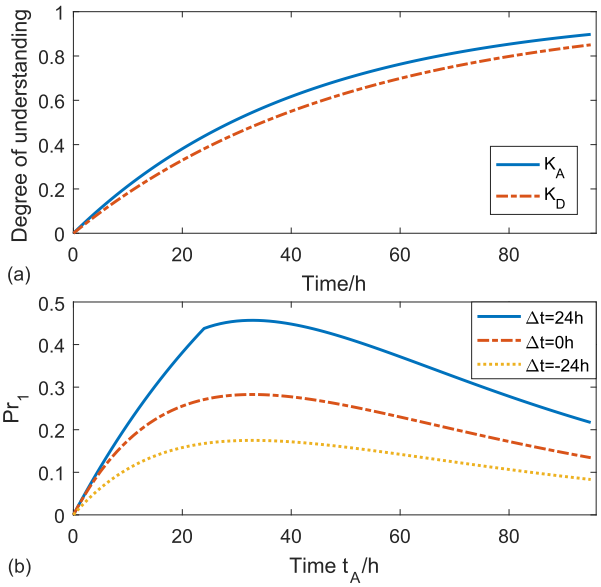

FIGURE 3. (a) Attacker and defender's understanding to a loophole ($\tau_A = 0.024$/h, $\tau_D = 0.02$/h) (b) Impact of time difference $\Delta t = t_A - t_D$ on Pr_1.

attacker to the loophole keeps increasing with time, the overall probability Pr_1 increases at first but decreases later. This is because the defender also gets knowledge of it. If there is a difference of time Δt when they identify a loophole, their progress is also different. The larger Δt is, the higher Pr_1 turns. Then the Pr_1 is affected, as shown in Fig. 3(b).

The strategy of the defender is fixed because it should certainly defend against the loophole immediately upon its discovery. However, as for the attacker, it only has one chance of the intrusion attempt. If it fails, the attacker will be exposed and thus cannot intrude again. The attacker only knows its own t_A, but not aware of t_D, i.e., how long the defender has learned about the loophole. So it cannot exactly pick up the optimal timing of the intrusion. To increase its success probability as much as possible, it should adopt a profitable strategy from different strategies, which will be discussed in Section IV.

C. FCIA

1) MECHANISM

In the field of computer science, the cyber attack is modelled as an attack graph [21], [22], which is also adopted in recent CPPS researches [23], [24]. While different theories including the semi-Markov process [25] and Petri network [26] are used, they can be seen as equivalent from the perspective of probability analysis. Therefore, this paper also uses the attack graph to model the FCIA process.

The attack graph is a data structure that models all possible paths of attacking a cyber system. A typical version is a directed graph as shown in Fig. 4 where nodes represent system states and edges represent the application of an exploit that transforms one state into another, more compromised state. The ending state of the attack graph represents the state in which the attacker has achieved its goals.

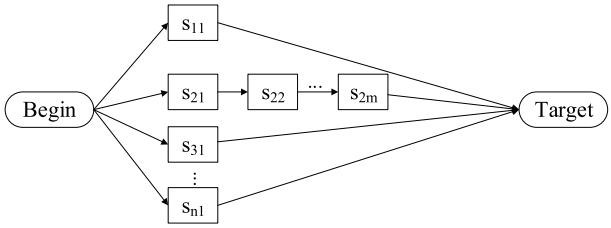

FIGURE 4. Attack graph.

2) PROBABILITY EVALUATION

The attacker should assess the probability of each path and then choose the most probable path. If one path which has m steps is selected, then the probability to finally achieve the goal is

$$Pr_2 = \prod_{i=1}^{m} p_i \tag{2}$$

where p_i is the success probability of the attack at the i-th step.

The attacker should intrude into multiple substations and attack their connecting branches to cause severe outages. For each target, the intrusion is performed collaboratively while attacks are executed individually. If targeted substations share the same software, then they are all vulnerable to the same loophole [27]. Therefore, the probability of the intrusion $Pr_1(t_A, t_D)$ is calculated once. As a contrast, Pr_2 of the multiple FCIAs should be multiplied as the number of actual attacks.

D. POST-CONTINGENCY DDoS INTERRUPTION

The operator will perform a redispatch as long as it is aware of a topological attack. However, both the data collection and instruction delivery rely on the communication network, which is composed of the cyber system of each substation in the CPPS. Information will not flow promptly if the network is jammed. Then the redispatch will not take full effect, that is, not all outages can be addressed. As a result, new outages may occur. The detailed model of the impaired adjustment is discussed in the next Section.

While only part of intruded substations is used to inject false commands, all compromised nodes can contribute to the DDoS attack to jam the communication network. During a DDoS attack, enormous invalid data packages are generated to exhaust the capacity of the intruded and neighboring nodes. Meanwhile, defenders will adopt and update advanced defensive control schemes against cyber attacks, for example, adaptive secure control [28] or reliable leader-to-follower formation control [29]. Affected by these defensive strategies, an individual DDoS attack has a probability to fail at each node. However, the overall DDoS attack has redundancy, so the target of congesting the communication network is to succeed as long as attacks at a few nodes lying in the transmitting link succeed. Therefore, the success probability of overall DDoS Pr_3 is considered to be 1.

According to the above mentioned discussion, if all substations are homogeneous and k branches are attacked,

the overall probability of the whole topological attacks $\Pr_T$ is

$$\Pr_T = \Pr_1(t_A, t_D) \times \Pr_2^k \times \Pr_3 \tag{3}$$

III. PATTERN OF CYBER ATTACK

Due to the $N-1$ security check, a single FCIA tripping only one branch cannot cause cascading outages. The attacker should instead impose a sequence of topological attacks to trigger cascading outages. In the sequence, some attacks play a decisive role, which means that no severe blackout will occur without them. Therefore, the core of an attack sequence is defined as a pattern.

According to the definition of the pattern, branches appearing in patterns are critical. Therefore, system operators should not let branches in the same pattern fail simultaneously, or there will be a blackout. This can be implemented by reasonably configuring the software diversity, so ''available'' branches of the attacker are limited.

A. DEFINITION OF PATTERN

An attack sequence F consists of several member branches $L_{s1}, L_{s2}, \ldots$, each of which corresponds to a targeted branch, denoted as

$$F = (L_{s1}, L_{s2}, \ldots, L_{sk}) \tag{4}$$

Some sequences lead to the loss of load, i.e. $Loss(F) > 0$ or $Loss(F) =$ ''EC'' (meaning that the emergency control is activated).

Under a given threshold TH, we can subtract some members from a sequence F that satisfies $Loss(F) \geq TH$, to get a subsequence F'. Usually, there is a relation that $Loss(F') \leq Loss(F)$, because the disturbance caused by F' is smaller. If F' is the minimal subsequence of F while maintaining that $Loss(F') \geq TH$, then we define that F' is the ''pattern'' of F. In that process of subtraction, the order of remaining branches is kept unchanged. This is because sometimes the order influences the loss. So in this paper, patterns containing the same members but with different orders are temporarily seen as different. If all of them share an approximate loss, then they can be merged as an ''unsequenced'' pattern.

The pattern is representative according to its definition. By adding branches, a large number of risky attacking sequences can be generated from one pattern. On the contrary, however, it may take great efforts to identify the pattern of a sequence F, because F has many subsequences. One can only try the subsequences in turn, which is a computation-intensive process.

B. FORMATION OF PATTERN/SEQUENCE

Every time after an FCIA, the topology of the grid is altered. So the vulnerability of each branch varies at different topology (state). The attacker should judge which branch is ''valuable'' to attack next, dynamically, according to the current state of the CPPS. Ref. [12], [30] figured out that power systems have the Markovian property, so the decision can be made independently with only the current states. This is a tree-layout Markov decision process (MDP), as shown in Fig. 5.

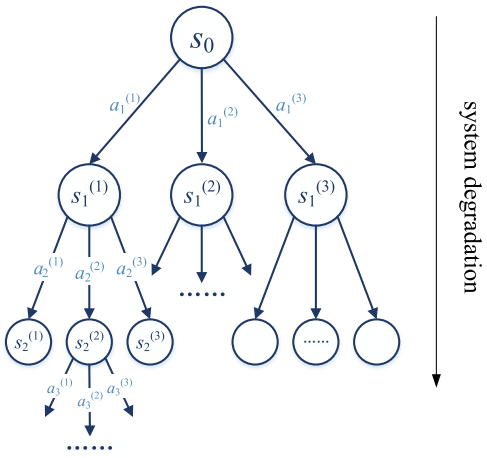

FIGURE 5. MDP with system degradation.

According to the MDP model, the sequence of actions from s_0 (the normal condition with no outage) is the attack sequence. If n nonrepeated search trials are performed, then we will get n attack sequences. Patterns will be extracted from these sequences in the following passage. It should be noted that this MDP is just used to organize attack sequences because some share the same heads. So we do not solve the optimal strategy (corresponding to the riskiest attack sequence) of the attacker, as our previous work [31] has discussed this problem. Instead, every risky pattern is worth attention.

C. SYSTEM DEGRADATION AND LOSS EVALUATION

The change of the topology of the grid will lead to the alteration of the admittance matrix $\mathbf{Y} = \mathbf{G} + j\mathbf{B}$. Therefore, according to the following power flow equation (5), measurements of each node and branch are also changed.

$$\begin{cases} P_i = V_i \sum_j V_j (G_{ij} \cos\theta_{ij} + B_{ij} \sin\theta_{ij}) \\ Q_i = V_i \sum_j V_j (G_{ij} \sin\theta_{ij} - B_{ij} \cos\theta_{ij}) \end{cases} \tag{5}$$

The CPPS is going near its security margin as the attack continues. This is a process of degradation. Meanwhile, operators may try to perform a redispatch as soon as they detect the anomaly. However, the communicational network is jammed by the DDoS attack, so the concentrated adjustment cannot take effect. Instead, only simple automatic adjustments at each component are performed.

1) OUTAGE OF NODES

If measurements, mainly voltage V are beyond their upper or lower bound, the local relay protection will be automatically activated. This may shed part of the load to force V back to their secure region. In this paper, we assume that the power factor of each load keeps constant during the load shed. Therefore, the following constraints should be satisfied

during the clearance of outage at node i

$$\begin{cases} 0 \le P_{D_i} \le P_{D0_i} \\ Q_{D_i} = \dfrac{P_{D_i}}{P_{D0_i}} Q_{D0_i} \quad (\text{if } P_{D0_i} \ne 0) \\ V_{\min} \le V_i \le V_{\max} \end{cases} \tag{6}$$

where P_{D0_i} is the amount of active demand load before shedding. Due to the lack of a concentrated redispatch, the load shedding may not be "optimal", so there is not an objective function in (6).

2) OUTAGE OF BRANCHES

Branches, i.e., transmission lines and transformers also have the risk of an outage, mainly due to overloading. A branch has a rated power limit S_r according to its thermal threshold. If its apparent power $S = \sqrt{P^2 + Q^2} > S_r$, the relay protection will automatically trip it out of the grid. This will not directly result in load loss. However, if islanding occurs and the new island il cannot meet the following power balance, part of load should be shed.

$$\sum_{i \in il} P_{G_i} = \sum_{i \in il} P_{D_i} + p_{n,il} \tag{7}$$

where $p_{n,il}$ is the grid loss caused by the resistance of branches.

3) LOSS EVALUATION

The activation of local protections does not always mitigate the risk, due of the lack of a coordinated redispatch. In some cases, it will worsen the situation, and new outages may emerge. Then the power flow may be updated repeatedly until no more outages or the emergency control is finally activated. After the system degradation ends, the loss of load caused by the attacker can be evaluated in the following way:

(a) If no load is shed, then $Loss = 0$;

(b) If some load is shed and the stability of the system can be maintained, then $Loss > 0$;

(c) If the stability of the system cannot be maintained, then $Loss =$ "EC", which is a special mark meaning that the final loss is determined by the consequent emergency control.

IV. SEARCH STRATEGY OF PATTERNS

For sequences containing two branches (denoted as "2-seq"), we can assert them to be patterns ("2-pat") upon knowing their $Loss \ge TH$ by simulation because they do not have any risky subsequence. Therefore, we can identify risky 3-seqs as patterns directly after finding out all 2-pats in the same way. That is the basis of the gradual increasing search strategy.

Although all 2-pats or 3-pats can be obtained by enumeration, it is very difficult to identify d-pats by checking every d-seqs if the length (search depth) d is large. So we cannot obtain "all" d-pats. Instead, we should begin to search for $(d+1)$-pats when there is enough risky d-seqs. The increase of d is performed by the following practical criteria.

Suppose the search is executed by batch, and one batch contains Δn search trials. If m_i risky sequences have been found during the i batches, then we can calculate performance v_i by

$$v_i = \frac{\Delta m}{\Delta n} = \frac{m_i - m_{i-1}}{\Delta n} \tag{8}$$

In general, given $i > j$, the former v_i is smaller than the latter v_j, because remaining patterns are distributed more sparsely at batch j than i, as the search continues. In this way, the search will step into the next depth d when the v meets the following criteria

$$v_i < v_0^{(d)} / TH_v \tag{9}$$

where $v_0^{(d)}$ is the performance of the first batch at d, and TH_v is a given threshold.

To sum up, the procudure of the pattern identification is

1) Set the initial depth $d \leftarrow 2$.
2) Search begins.
3) Execute the i-th of search, calculate the performance v_i.
4) If the i-th is the first batch at depth d, set $v_0^{(d)} \leftarrow v_i$.
5) If v_i satisfies (9), let $d \leftarrow d + 1$.
6) Loop step 3) – 5) until search ends.

Lastly, we use the accuracy to compare different strategies. After finding m risky sequences, they are checked whether they are "true" patterns or not. If p patterns are eventually identified, then the accuracy is

$$A = p/m \tag{10}$$

If all strategies find p patterns, then the strategy with a larger A is better, because it means less false positive samples and thus save the time of checking.

V. TEST RESULTS

A. CASE SETUP

In this paper, we use the IEEE 39-node system (New England) to validate the representativeness of the pattern and the efficiency of the strategy. The CPPS has 29 buses (numbered 1, 2, . . ., 29), 46 branches (transmission lines and transformers), and 10 generators. Every node is equipped with a cyber communicational and control system. The cyber systems are interconnected by the same topology of the physical network. Additionally, we suppose that generators cannot be penetrated.

The software configuration of the cyber system in [32] is adopted. Besides, the capacity of the attacker and the defender are the same as Fig. 3(a). The durations of long and medium timescales are 168 and 1 hour, respectively.

Lastly, the case is carried out by MATLAB R2016a software on a laptop with an Intel i5-3210M CPU and 8GB RAM.

B. PROBABILITY EVALUATION

1) OPTIMAL TIMING OF INTRUSION

According to (1), the success probability of intrusion $\Pr_1$ is affected by both the attacker and the defender. They scan loopholes independently, and the attacker does not know when the regular security patch will arrive. We denote t_{A0},

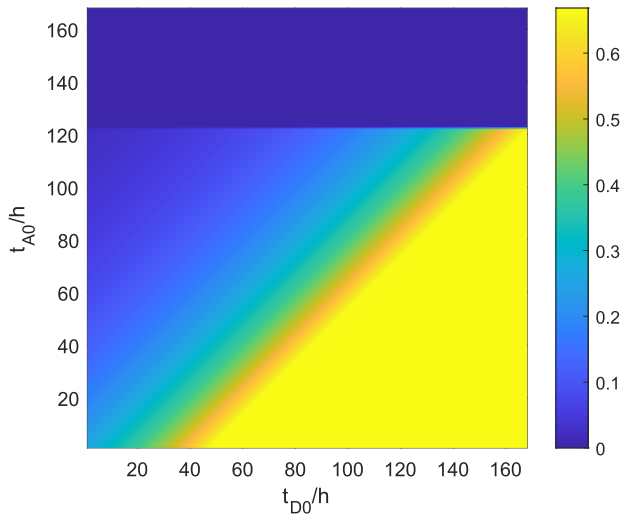

FIGURE 6. Distribution of Pr_1 at different (t_{A0}, t_{D0}) (if launching intrusion 46h after discovery, i.e. $t_A = 46$h).

TABLE 2. Paths and probabilities of the attack graph.

No.	Path	Pr_2
1	IHMI→ CSWI→ XCBR	0.7×0.4=0.28
2	ITMI→ IHMI→ CSWI→ XCBR	0.8×0.7×0.4=0.224
3	ITCI→ CSWI→ XCBR	0.7×0.4=0.28
4	IHMI→ MMET→ CSWI→ XCBR	0.7×0.6×0.4=0.168
5	TSGN→ MMET→ CSWI→ XCBR	0.4×0.6×0.4=0.096
6	IHMI→ PTRC→ CSWI→ XCBR	0.7×0.6×0.4=0.168
7	TCTR→ PTRC→ CSWI→ XCBR	0.4×0.6×0.4=0.096

t_{D0} as the discovery time of the attacker and the defender, respectively. Besides, the pair (t_{A0}, t_{D0}) the time of discovery is uniformly distributed across the 168 × 168 square region. So the Pr_1 at each grid can be calculated, as shown in Fig. 6.

The attacker should launch an intrusion at a proper time, neither too early nor too late. To this end, it should maximize the average Pr_1 to obtain the optimal timing, which is

$$\max_{t_A} \sum_{t_{A0}=0}^{167} \sum_{t_{D0}=0}^{167} Pr_1(t_A, t_D)/168^2 \tag{11}$$

where $t_D = \max(t_{A0} + t_A - t_{D0}, 0)$. Pr_1 in (11) can be calculated according to (1), except that $Pr_1 = 0$ if $t_{A0} + t_A \geq 168$, because the timing is beyond the long-term period.

After optimization according to the case setup, the attacker should launch an intrusion 46h after discovery. Therefore, the expected success rate of an intrusion is $Pr_{1,\max} = 30\%$.

2) SUCCESS PROBABILITY OF FCIA

There are 7 paths in the attack graph introduced in [32]. Each path contains 2 to 3 steps. The vulnerability of every step can be assessed by the common vulnerability scoring system (CVSS), according to [33].

As shown in Table 2, path 1 and 3 both have the highest probability, so the attacker will launch attacks along either of these two paths with $Pr_{2,\max} = 28\%$.

TABLE 3. Loss and risk of attack sequences.

Sequence	Loss/p.u.	Pr_T/%	Risk/p.u.
(L_{28}, L_{33}, L_{38})	0.0407	0.66	2.67×10^{-4}
(L_{28}, L_{33}), (L_{28}, L_{38}) and other 4 subsequences	0	2.35	0
(L_{28}, L_{38}, L_{33})	0.0407	0.66	2.67×10^{-4}
(L_{33}, L_{28}, L_{38})	0.0407	0.66	2.67×10^{-4}
$(L_2, L_{28}, L_{33}, L_{38})$	0.0407	0.18	7.33×10^{-5}
$(L_{28}, L_{33}, L_{35}, L_{38})$	0.0845	0.18	1.52×10^{-5}
$(L_{28}, L_{33}, L_{38}, L_{41})$	0.1332	0.18	2.40×10^{-4}

TABLE 4. Number of patterns and risky sequences.

Length	2	3	4	Sum
Pattern	135	481	952	1568
Risky sequence	270	14766	657786	672882
Potential sequence	2070	91080	$>3.9\times10^6$	$>4\times10^6$

C. REPRESENTATIVENESS OF PATTERN

Let $TH = 0.01$p.u. (1p.u. = 6254.2MW, i.e. the amount of load supplied by the grid), we discuss the representativeness from both qualitative and quantitative perspectives.

1) QUALITY OF PATTERN

From the evaluation, the sequence (L_{28}, L_{33}, L_{38}) is identified as an unsequenced pattern. The loss and risk of this pattern and some of its subsequences and derivatives are listed in Table 3.

As for this unsequenced pattern, the order does not affect the loss. After adding other branches, the loss may be larger or not. However, the risk is smaller than the pattern itself, because a longer sequence needs more continuous successful attacks, which leads to a smaller Pr_T. Therefore, patterns keep the core part that can cause a blackout and thus has the highest risk among their derivatives.

2) QUANTITY OF PATTERN

In this part, we analyze the number of derivatives that one pattern can represent. Table 4 shows the number of attack sequences and patterns ≤ 4 branches by enumeration.

In this case, one pattern can represent 429 risky sequences on average. Besides, while the number of risky sequences increases drastically as the length grows from 2 to 4, the number of patterns increases rather smoothly. Meanwhile, it is very computationally expensive to enumerate all risky 4-seqs, but we can derive them from patterns with high accuracy. Therefore, the "pattern" is a reasonable concept that can substantially compress the storage of risky topological attack schemes for operators.

D. EFFICIENCY OF THE STRATEGY

Three strategies are compared. All of them search for patterns no longer than 5-pats. The first one is according to (9) ("Gradual"), where the parameter $TH_v = 3$. The latter two are control groups. One does not limit the search depth ("Constant"), whereas the other takes a naïve increase strategy ("Naïve"), which increases the depth by 1 every 10 batches. Additionally, given that there are only $46 \times 45 = 2070$ 2-seqs in the 39-node system, the initial depth of the "Naïve" strategy is set to be 3.

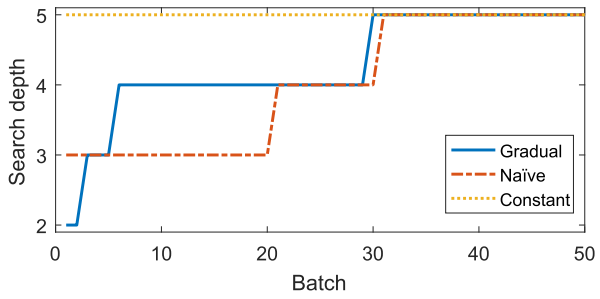

FIGURE 7. Search depth.

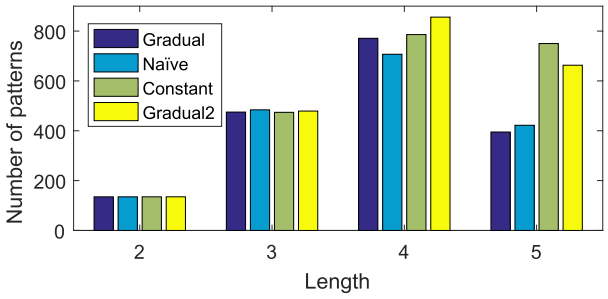

FIGURE 8. Search results.

TABLE 5. Performance of each strategy.

Strategy	Search trials	Batches	Patterns	Accuracy	Time/s
Gradual	5×10^4	50	1776	91.88%	24914
Naïve	5×10^4	50	1748	85.73%	25964
Constant	5×10^4	50	2145	78.92%	34589
Gradual2	6.5×10^4	65	2133	91.15%	33382
MRC [35]	–	–	384	12.79%	23442

All the strategies search for 5×10^4 times, which consists of 50 batches of 1×10^3 search trials. At each search trial, the attack would choose branches that have heavy power flow but less visit counts [34]. The search depth of each batch is shown in Fig. 7.

The numbers of identified patterns with different lengths are shown in Fig. 8. The number of 2-pats, 3-pats, and 4-pats of the three strategies is near. However, the "Gradual" strategy finds fewer 5-pats than the control groups. Then we extend the search trials of "Gradual" to 6.5×10^4, as the blue bar in Fig. 8 ("Gradual2"). The extra 1.5×10^4 search trials find more 4-pats and 5-pats, making the total found patterns reach the "Constant" strategy, as shown in Table 5. Moreover, because the $\Pr_T$ of 4-pats (0.18%) is larger than that of 5-pats (0.05%), so we can conclude that the proposed strategy identifies more risky patterns than the control groups, using the same computational resource.

According to Table 5, the proposed strategy used less time than the other two, because it prioritizes shorter patterns. Shorter patterns mean fewer topological changes. Given that the power flow should be updated every time after the topological change, the proposed method needs fewer calculations.

Meanwhile, the "Gradual" keeps the highest accuracy, which is the ratio of "true" patterns to pattern candidates. For example, the proposed method found 1933 risky attack sequences within the 5×10^4 search trial. Theses are candidates for the following check. After checking, 1776 passed as "true" patterns, so the accuracy is 1776/1933=91.88%. As they finally found roughly equal patterns, the strategy with higher accuracy avoids more false positive candidates and thus saves extra checking time.

Then we compare the performance of our method to [35]. Ref. [35] proposed a similar concept called "minimal $N-k$ contingencies", which can be adapted to the "attack pattern" of this paper. The difference is that "minimal $N-k$ contingencies" occur simultaneously not sequentially. Therefore, we accustom the "RC" method in [35] to the search for patterns. The Modified "RC" (MRC) has two steps. First, it generates many "minimal $N-k$ contingencies" as [35] did. Second, it checks whether these sets of contingencies are patterns or not according to Section III-A.

The result of MRC is shown in Table 5. While there is no concept like "search trial" or "batch" in MRC, we can compare their found patterns and accuracy. Although using nearly the same time, MRC finds fewer patterns than both "Gradual" and "Naïve" strategies, and has even less accuracy. Thus our method has superiority to this existing similar method.

E. DISCUSSIONS

1) SCALABILITY

The proposed method of the pattern analysis applies to large-scale CPPSes as well. To validate the scalability, a real province-level CPPS in China that has 741 nodes and 1254 branches is studied in this part. 40000 search trials are executed using DC power flow to search for patterns that ≤ 6 branches. Then 579 risky attack sequences are found, of which 81 patterns are identified. This CPPS has a wider security margin than the virtual New England system, so cyber attacks have fewer patterns and thus do less harm. Therefore, this result is reasonable, which verifies the scalability of the proposed method.

2) TUNING OF TH_v

The value of TH_v can affect the performance of the "Gradual" strategy. We test different TH_vs and then the distribution of obtained patterns is illustrated in Fig. 9. The numbers of 2-pats and 3-pats are almost the same, whereas the numbers of 4-pats and 5-pats are different. As TH_v increases from 2 to 4, the number of 4-pats also increases while the number of 5-pats decreases. This is because a smaller TH_v allows the search stage at depth $d=5$ longer but at $d=4$ shorter. Meanwhile, 2-pats and 3-pats are easy to obtain, so TH_v does not affect them. Therefore, in this case, different TH_vs show different search preferences, and all of 2, 3, or 4 are acceptable values.

3) MITIGATION MEASURE

As each pattern suggests a kind of risk, operators of the CPPS should take measures to reduce the number of patterns. In this paper, we give a preliminary discussion based on the

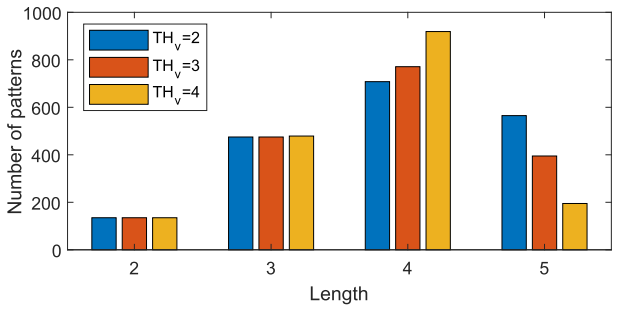

FIGURE 9. Impact of TH_V on the distribution of obtained patterns.

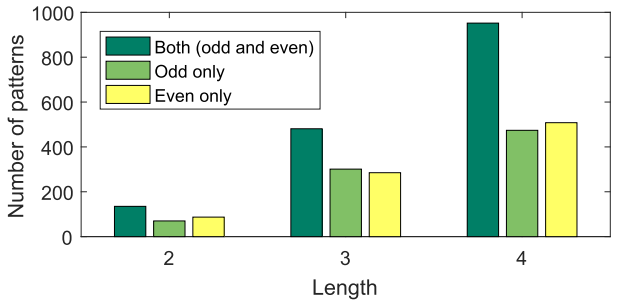

FIGURE 10. Effect of software diversity to eliminate patterns.

data of Table 4. If the attacker can intrude into all substations, there are 1568 patterns ($\leq$ 4-pats). However, when planning and constructing the cyber network, managers of real CPPSes usually purchase cyber software from different vendors. Considering that different software does not have the same loophole, the ''available'' substations and branches of the attacker are limited.

Suppose the cyber software from two vendors is adopted. One is installed at substations with an odd number (1, 3, . . ., 29), and the other is at those with an even number (2, 4, . . ., 28). For example, L_{43} (26–28) is not available for the attacker intruding odd-numbered substations because the attacker can only discover one loophole. Then the number of patterns reduces to 845 and 880, respectively, if the loophole discovered by the attacker is odd and even-numbered substations, as shown in Fig. 10. Furthermore, the software can be configured more precisely if considering the distribution of patterns, which will be studied in the future.

VI. CONCLUSION

In this paper, the coordinated topological attack from the cyber system to the physical network in modern CPPSes is analyzed. The attacker can utilize multiple forms to illegally get access to physical components, alter the topology, disrupt the redispatch, and finally jeopardize the security of the CPPS. To protect the CPPS from critical topological attacks, the pattern of attack sequences is introduced and discussed. Then a novel search strategy is presented, which dynamically selects the next attack target and gradually increases the search depth according to the search performance. The case study on the IEEE 39-node CPPS demonstrates that the pattern is representative from both the qualitative and quantitative perspectives. Case studies illustrate that the introduction of the pattern significantly reduces the storage for risky attack sequences while keeping the key information. Results also show that the proposed search strategy further enhances performance and accuracy, and outperforms the existing similar method.

Next, the authors would explore the configuration of the software diversity to mitigate cyber risk and try to apply the pattern analysis to a larger CPPS.

APPENDIX A
NOMENCLATURE

Acronyms and abbreviations

CPPS	Cyber-physical power system
FDIA	False data injection attack
FCIA	False command injection attack
DDoS	Distributed denial of service
VPN	Virtual private network
MDP	Markov decision process
Pr	Probability
EC	Emergency control
d-seq	Attack sequence that contains d branches
d-pat	Attack pattern that contains d branches
XCBR	Circuit breaker
IHMI and other notations in Table 2	Interim states of an attack path
p.u.	Per unit, the amount of load supplied by the grid

Cyber attack

Pr_1	Probability of a successful intrusion
Pr_2	Probability of a successful FCIA
Pr_3	Probability of a successful DDoS attack
Pr_T	Probability of the whole topological attack
K_A, K_D	Attacker's/defender's understanding degree of a loophole
t_A, t_D	Time from the discovery of a loophole by the attacker/defender, loophole learning time
t_{A0}, t_{D0}	Discovery time of a loophole from the beginning of a long-term period by the attacker/defender
τ_A, τ_D	Capacity of the attacker/defender
Δt	Difference of t_A and t_D
n	Number of attack paths of a substation
m	Number of steps of an attack path
p_i	Probability of a successful attack at the i-th step
k	Number of attacked branches

System degradation

F	Attack sequence
$L_{s1}, L_{s2}, \ldots$	Attacked branches in an F
$Loss$	Loss of load of an F
TH	Threshold of loss

s_0	Normal condition of a CPPS with no outage
$s_j^{(i)}$	i-th state at the j-th level
$a_j^{(i)}$	i-th attack to the j-th level
$\mathbf{Y}$	Admittance matrix of the physical network of a CPPS
$\mathbf{G}$	Real part of $\mathbf{Y}$
$\mathbf{B}$	Imaginary part of $\mathbf{Y}$
P_i	Active power injected at node i
Q_i	Reactive power injected at node i
V_i	Voltage at node i
θ_{ij}	Difference of phase angle between node i and j
P_{D_i}, Q_{D_i}	Demand power of node i
P_{G_i}	Generated active power of node i
P_{D0_i}, Q_{D0_i}	Demand power of node i at s_0
$p_{n,il}$	Grid loss of island il
S, S_r	Actual/apparent power flow of a branch

Pattern analysis

n	Number of nonrepeated search trials
m	Number of risky attack sequences
d	Search depth
v	Search performance
$v_0^{(d)}$	Search performance of the first batch at depth d
p	Number of attack patterns
A	Accuracy
TH_v	Threshold of performance

REFERENCES

[1] L. Shi, Q. Dai, and Y. Ni, "Cyber-physical interactions in power systems: A review of models, methods, and applications," *Electr. Power Syst. Res.*, vol. 163, pp. 396–412, Oct. 2018, doi: 10.1016/j.epsr.2018.07.015.

[2] Y. Cai, Y. Cao, Y. Li, T. Huang, and B. Zhou, "Cascading failure analysis considering interaction between power grids and communication networks," *IEEE Trans. Smart Grid*, vol. 7, no. 1, pp. 530–538, Jan. 2016, doi: 10.1109/TSG.2015.2478888.

[3] Z. Wang, Y. Chen, F. Liu, Y. Xia, and X. Zhang, "Power system security under false data injection attacks with exploitation and exploration based on reinforcement learning," *IEEE Access*, vol. 6, pp. 48785–48796, 2018, doi: 10.1109/ACCESS.2018.2856520.

[4] 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 Trans. Power Syst.*, vol. 31, no. 6, pp. 4379–4394, Nov. 2016, doi: 10.1109/TPWRS.2015.2510626.

[5] J. Qin, M. Li, L. Shi, and X. Yu, "Optimal denial-of-service attack scheduling with energy constraint over packet-dropping networks," *IEEE Trans. Autom. Control*, vol. 63, no. 6, pp. 1648–1663, Jun. 2018, doi: 10.1109/TAC.2017.2756259.

[6] B. Gao and L. Shi, "Modeling an attack-mitigation dynamic game-theoretic scheme for security vulnerability analysis in a cyber-physical power system," *IEEE Access*, vol. 8, pp. 30322–30331, 2020, doi: 10.1109/ACCESS.2020.2973030.

[7] L. Xie, Y. Mo, and B. Sinopoli, "Integrity data attacks in power market operations," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 659–666, Dec. 2011, doi: 10.1109/TSG.2011.2161892.

[8] Z. Li, M. Shahidehpour, A. Alabdulwahab, and A. Abusorrah, "Analyzing locally coordinated cyber-physical attacks for undetectable line outages," *IEEE Trans. Smart Grid*, vol. 9, no. 1, pp. 35–47, Jan. 2018, doi: 10.1109/TSG.2016.2542925.

[9] L. Che, X. Liu, Z. Shuai, Z. Li, and Y. Wen, "Cyber cascades screening considering the impacts of false data injection attacks," *IEEE Trans. Power Syst.*, vol. 33, no. 6, pp. 6545–6556, Nov. 2018, doi: 10.1109/TPWRS.2018.2827060.

[10] P. Hines, S. Blumsack, E. C. Sanchez, and C. Barrows, "The topological and electrical structure of power grids," in *Proc. 43rd Hawaii Int. Conf. Syst. Sci.*, Honolulu, HI, USA, Jan. 2010, pp. 1–10, doi: 10.1109/HICSS.2010.398.

[11] R. Albert, H. Jeong, and A.-L. Barabási, "Error and attack tolerance of complex networks," *Nature*, vol. 406, no. 6794, pp. 378–382, Jul. 2000, doi: 10.1038/35019019.

[12] Z. Qu, Q. Xie, Y. Liu, Y. Li, L. Wang, P. Xu, Y. Zhou, J. Sun, K. Xue, and M. Cui, "Power cyber-physical system risk area prediction using dependent Markov chain and improved grey wolf optimization," *IEEE Access*, vol. 8, pp. 82844–82854, 2020, doi: 10.1109/ACCESS.2020.2991075.

[13] J. Zhang and L. Sankar, "Physical system consequences of unobservable state-and-topology cyber-physical attacks," *IEEE Trans. Smart Grid*, vol. 7, no. 4, pp. 2016–2025, Jul. 2016, doi: 10.1109/TSG.2016.2552178.

[14] 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 Trans. Smart Grid*, vol. 10, no. 4, pp. 4577–4588, Jul. 2019, doi: 10.1109/TSG.2018.2865316.

[15] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "A framework for cyber-topology attacks: Line-switching and new attack scenarios," *IEEE Trans. Smart Grid*, vol. 10, no. 2, pp. 1704–1712, Mar. 2019, doi: 10.1109/TSG.2017.2776325.

[16] K. Lai, M. Illindala, and K. Subramaniam, "A tri-level optimization model to mitigate coordinated attacks on electric power systems in a cyber-physical environment," *Appl. Energy*, vol. 235, pp. 204–218, Feb. 2019, doi: 10.1016/j.apenergy.2018.10.077.

[17] B. Li, Y. Chen, S. Huang, R. Yao, Y. Xia, and S. Mei, "Graphical evolutionary game model of virus-based intrusion to power system for long-term cyber-security risk evaluation," *IEEE Access*, vol. 7, pp. 178605–178617, 2019, doi: 10.1109/ACCESS.2019.2958856.

[18] R. Yao, S. Huang, K. Sun, F. Liu, X. Zhang, and S. Mei, "A multi-timescale quasi-dynamic model for simulation of cascading outages," *IEEE Trans. Power Syst.*, vol. 31, no. 4, pp. 3189–3201, Jul. 2016, doi: 10.1109/TPWRS.2015.2466116.

[19] Y. Mo, T. Hyun-Jin Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli, "Cyber–physical security of a smart grid infrastructure," *Proc. IEEE*, vol. 100, no. 1, pp. 195–209, Jan. 2012, doi: 10.1109/JPROC.2011.2161428.

[20] Y. Chen, J. Hong, and C.-C. Liu, "Modeling of intrusion and defense for assessment of cyber security at power substations," *IEEE Trans. Smart Grid*, vol. 9, no. 4, pp. 2541–2552, Jul. 2018, doi: 10.1109/TSG.2016.2614603.

[21] S. Jha, O. Sheyner, and J. Wing, "Two formal analyses of attack graphs," in *Proc. 15th IEEE Comput. Secur. Found. Workshop (CSFW)*, Cape Breton, NS, Canada, Jun. 2002, pp. 49–63, doi: 10.1109/CSFW.2002.1021806.

[22] M. Yousefi, N. Mtetwa, Y. Zhang, and H. Tianfield, "A reinforcement learning approach for attack graph analysis," in *Proc. 17th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun./ 12th IEEE Int. Conf. Big Data Sci. Eng. (TrustCom/BigDataSE)*, New York, NY, USA, Aug. 2018, pp. 212–217, doi: 10.1109/TrustCom/BigDataSE.2018.00041.

[23] N. Liu, J. Zhang, H. Zhang, and W. Liu, "Security assessment for communication networks of power control systems using attack graph and MCDM," *IEEE Trans. Power Del.*, vol. 25, no. 3, pp. 1492–1500, Jul. 2010, doi: 10.1109/TPWRD.2009.2033930.

[24] Q. Dai, L. Shi, and Y. Ni, "Risk assessment for cyberattack in active distribution systems considering the role of feeder automation," *IEEE Trans. Power Syst.*, vol. 34, no. 4, pp. 3230–3240, Jul. 2019, doi: 10.1109/TPWRS.2019.2899983.

[25] Y. Zhang, L. Wang, and Y. Xiang, "Power system reliability analysis with intrusion tolerance in SCADA systems," *IEEE Trans. Smart Grid*, vol. 7, no. 2, pp. 669–683, Mar. 2016, doi: 10.1109/TSG.2015.2439693.

[26] R. Fu, X. Huang, Y. Xue, Y. Wu, Y. Tang, and D. Yue, "Security assessment for cyber physical distribution power system under intrusion attacks," *IEEE Access*, vol. 7, pp. 75615–75628, 2019, doi: 10.1109/ACCESS.2018.2855752.

[27] M. Touhiduzzaman, A. Hahn, and A. K. Srivastava, "A diversity-based substation cyber defense strategy utilizing coloring games," *IEEE Trans. Smart Grid*, vol. 10, no. 5, pp. 5405–5415, Sep. 2019, doi: 10.1109/TSG.2018.2881672.

[28] X. Huang and J. Dong, "Reliable leader-to-follower formation control of multiagent systems under communication quantization and attacks," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 50, no. 1, pp. 89–99, Jan. 2020, doi: 10.1109/TSMC.2019.2894946.

[29] X. Huang and J. Dong, "An adaptive secure control scheme for T-S fuzzy systems against simultaneous stealthy sensor and actuator attacks," *IEEE Trans. Fuzzy Syst.*, early accesss, Apr. 28, 2020, doi: 10.1109/TFUZZ.2020.2990772.

[30] J. Guo, F. Liu, J. Wang, J. Lin, and S. Mei, "Toward efficient cascading outage simulation and probability analysis in power systems," *IEEE Trans. Power Syst.*, vol. 33, no. 3, pp. 2370–2382, May 2018, doi: 10.1109/TPWRS.2017.2747403.

[31] Z. Zhang, S. Huang, Y. Chen, S. Mei, W. Wei, and L. Ding, "Key branches identification for cascading failure based on Q-learning algorithm," in *Proc. IEEE Int. Conf. Power Syst. Technol. (POWERCON)*, Wollongong, NSW, Australia, Sep./Oct. 2016, doi: 10.1109/POWERCON.2016.7753996.

[32] Y. Zhang, M. Ni, Y. Sun, and M. Li, "Quantitative risk assessment of cyber-physical system for cyber-attacks in distribution network," *Autom. Electr. Power Syst.*, vol. 43, no. 21, pp. 12–30 and 33, 2019.

[33] H. Wang, Z. Chen, J. Zhao, X. Di, and D. Liu, "A vulnerability assessment method in industrial Internet of Things based on attack graph and maximum flow," *IEEE Access*, vol. 6, pp. 8599–8609, 2018, doi: 10.1109/ACCESS.2018.2805690.

[34] Z. Zhang, R. Yao, S. Huang, Y. Chen, S. Mei, and K. Sun, "An online search method for representative risky fault chains based on reinforcement learning and knowledge transfer," *IEEE Trans. Power Syst.*, vol. 35, no. 3, pp. 1856–1867, May 2020, doi: 10.1109/TPWRS.2019.2951171.

[35] M. J. Eppstein and P. Hines, "A 'random chemistry' algorithm for identifying collections of multiple contingencies that initiate cascading failure," *IEEE Trans. Power Syst.*, vol. 27, no. 3, pp. 1698–1705, Aug. 2012, doi: 10.1109/TPWRS.2012.2183624.

ZHIMEI ZHANG (Graduate Student Member, IEEE) received the B.E. degree in electrical engineering from Tsinghua University, Beijing, China, in 2016, where he is currently pursuing the Ph.D. degree in electrical engineering. His research interest includes computational analysis of power systems.

SHAOWEI HUANG (Member, IEEE) received the B.S. and Ph.D. degrees from the Department of Electrical Engineering, Tsinghua University, Beijing, China, in July 2006 and June 2011, respectively. From 2011 to 2013, he held a postdoctoral position with the Department of Electrical Engineering, Tsinghua University, where he is currently an Associate Professor. His research interests include power systems modeling, simulation power system parallel and distributed computing, complex systems and its application in power systems, and artificial intelligence.

FENG LIU (Senior Member, IEEE) received the B.Sc. and Ph.D. degrees in electrical engineering from Tsinghua University, Beijing, China, in 1999 and 2004, respectively.

From 2015 to 2016, he was a Visiting Associate with the California Institute of Technology, Pasadena, CA, USA. He is currently an Associate Professor with Tsinghua University. He is the author/coauthor of more than 200 peer-reviewed technical articles and two books. He holds more than 20 issued/pending patents. His research interests include stability analysis, optimal control, robust dispatch, and game theory-based decision making in energy and power systems. He serves as an Associate Editor for several international journals, including the IEEE TRANSACTIONS ON SMART GRID, the IEEE POWER ENGINEERING LETTERS, IEEE ACCESS, and so on. He also served as a Guest Editor for the IEEE TRANSACTIONS ON ENERGY CONVERSION.

SHENGWEI MEI (Fellow, IEEE) received the B.S. degree in mathematics from Xinjiang University, Urumqi, China, in 1984, the M.S. degree in operations research from Tsinghua University, Beijing, China, in 1989, and the Ph.D. degree in automatic control from the Chinese Academy of Sciences, Beijing, in 1996. He is currently a Professor with the Department of Electrical Engineering, Tsinghua University. His research interests include power system analysis and control and game theory and its application in power systems.