UNIVERSITY OF LEEDS

This is a repository copy of *Revealing Vulnerability of N-1 Secure Power Systems to Coordinated Cyber-Physical Attacks*.

White Rose Research Online URL for this paper:
https://eprints.whiterose.ac.uk/188986/

Version: Accepted Version

Article:
Zhou, M, Liu, C, Abiri Jahromi, A et al. (3 more authors) (2022) Revealing Vulnerability of N-1 Secure Power Systems to Coordinated Cyber-Physical Attacks. IEEE Transactions on Power Systems. ISSN 0885-8950

https://doi.org/10.1109/tpwrs.2022.3169482

© 2021 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.

Reuse
Items deposited in White Rose Research Online are protected by copyright, with all rights reserved unless indicated otherwise. They may be downloaded and/or printed for private study, or other acts as permitted by national copyright laws. The publisher or other rights holders may allow further reproduction and re-use of the full text version. This is indicated by the licence information on the White Rose Research Online record for the item.

Takedown
If you consider content in White Rose Research Online to be in breach of UK law, please notify us by emailing eprints@whiterose.ac.uk including the URL of the record and the reason for the withdrawal request.

White Rose university consortium
Universities of Leeds, Sheffield & York

eprints@whiterose.ac.uk
https://eprints.whiterose.ac.uk/

Revealing Vulnerability of N-1 Secure Power Systems to Coordinated Cyber-Physical Attacks

Min Zhou, *Student Member, IEEE,* Chensheng Liu, *Member, IEEE,* Amir Abiri Jahromi, *Senior Member, IEEE,* Deepa Kundur, *Fellow, IEEE,* Jing Wu, *Senior Member, IEEE,* and Chengnian Long, *Senior Member, IEEE*

***Abstract*—Coordinated cyber-physical (CCP) attacks have attracted wide attention in power systems because of their potential to cause severe disturbance including cascading failures. However, as realistic power systems operate within the N-1 security criterion, existing CCP attacks may be in part mitigated. As such, this paper analyzes impacts of CCP attacks on the vulnerability of the power systems that employ the N-1 security constrained optimal power flow (SCOPF). Specifically, a tri-level model is proposed to analyze the CCP attack impacts, whereby the adversary coordinates a physical attack with cyber attacks to initiate and propagate post-contingency overload based on N-1 SCOPF. A methodology utilizing semidefinite programming (SDP) relaxation and primal-dual formulation is proposed to transform the tri-level model into a conic optimization, such that the model can be easily solved by SDP solvers. Case studies on the IEEE 14, 57, and 118 bus test systems demonstrate that the CCP attacks in power systems with N-1 security criterion are able to cause N-1-1 contingency and even trigger cascading failures.**

***Index Terms*—Cyber-physical systems, power systems, coordinated cyber-physical attacks, tri-level optimization, N-1 security**

I. Introduction

WIDESPREAD blackouts in power systems are low-probability, high-impact events. The initiating contingency in blackouts is usually a single line outage that overloads the remaining lines; these overloaded lines are then tripped by protective relays resulting in cascading failures [1]. To reduce such risks, effective preventive and corrective measures, such as generation redispatch, line switching and load shedding, have been implemented to alleviate the post-contingency overload and prevent the false line tripping [2]–[4]. In general, if these protective measures are properly implemented, the system will remain post-contingency stable and secure. However, due to increasing cyber-security-related events in power systems [5], [6], protective measures may be hindered or even misled by cyberattacks, which will increase the likelihood of cascading events. A recent real-world example was the 2015 Ukraine grid attack [7] that resulted in blackout of hundreds of thousands of people. Therefore, it is imperative to investigate the impact of malicious attacks on cascading failure risks.

The literature has revealed the impact of both physical and cyber attacks on transmission line outages and the associated line tripping that may result in cascading failures. The potential of physical attacks to trigger line outages was studied in [8]–[10], where the attacks identify the critical components to target to initiate cascading failures. The potential of cyberattacks to trigger line outages was studied in [11]–[13]. In [11], the adversary identifies initial contingencies as system weak points, which are then leveraged to assist in the design of the false data injection attacks to cause sequential outages. In [12], [13], load redistribution (LR) attacks were proposed to overload the transmission lines, by misleading the security-constrained economic dispatch through load measurement manipulation. These studies include the relay tripping of the overloaded lines as an attack consequence, assuming that no immediate corrective action is taken by the operators. In practical operations, however, it would be feasible for operators to detect and relieve the overload before the relay acts, since LR attacks cannot mask line overloads.

Recently, it has been pointed out that *coordinated cyber-physical* (CCP) attacks have the potential to cause more severe cascading failures [14], if a physical attack and a cyber attack act collaboratively to create an initiating contingency and mask the post-contingency overloads. In this case, since the corrective actions are impossible due to the undetectable overloads, the overloads will propagate and cause cascading outages. The basic principle for CCP attacks to mask physical damage on power systems was introduced in [15], where the physical damage was modeled as an attack vector injected into the meter measurements. The worst-case CCP attacks to overload a target line with limited attack resources was studied in [16], where the adversary could access only a sub-network of the system. By coordinating a LR attack with a physical attack, Li *et al.* [17] designed a CCP attack that maximizes the total power redistribution and proposed a bi-level optimization problem to identify the most damaging attack. The attack model was further extended to a local attack with incomplete network information in [18]. Since these studies analyze the impact of the CCP attacks based on the DC power flow model, which might be unrealistic for practical power systems, Chung *et al.* [19] studied the CCP attack based on the AC power flow model, where the attack increased the cascading failure risks by falsifying the uploaded information of the line-outage

This work was supported by the National Natural Science Foundation of China under Grants 62136006, 62073215, 62073138, and 61873166. (Corresponding authors: Jing Wu; Chengnian Long.)

Min Zhou, Jing Wu and Chengnian Long are with the Department of Automation, Shanghai Jiao Tong University, Shanghai 200240, China. (email: {zhoumin15, jingwu, longcn}@sjtu.edu.cn)

Chensheng Liu is with the Key Laboratory of Smart Manufacturing in Energy Chemical Process, Ministry of Education, East China University of Science and Technology, Shanghai 200237, China (e-mail: cliu@ecust.edu.cn)

A. Abiri Jahromi is with the School of Electronic and Electrical Engineering, University of Leeds, Leeds, LS2 9JT, United Kingdom. (email: a.abirijahromi@leeds.ac.uk)

Deepa Kundur is with the Department of Electrical and Computer Engineering, University of Toronto, Toronto, ON M5S 3G4, Canada. (email: dkundur@ece.utoronto.ca)

location. Nevertheless, existing studies evaluate the impact of the proposed CCP attacks on cascading failures under the assumption that the power systems are unstable after N-1 contingency, i.e., additional line overloads can be caused after the physical attack initiates an outage. In realistic power systems, however, the system operates with "N-1 security criterion". That is, protective schemes are deployed to ensure that for any single credible contingency event, the system moves to a secure state without exceeding normal operation limits; such power systems are considered to be N-1 secure and have proven to be robust against some traditional cyberattacks [20]. Unfortunately, as the protective schemes are implemented to prevent cascading failures, they have also become the target of the malicious attack. Therefore, it is necessary to study the vulnerability of N-1 secure power systems to CCP attacks.

In this paper, we focus on power systems where the N-1 security constrained optimal power flow (SCOPF) is employed to protect the system to be post-contingency stable. For the first time, the system vulnerabilities are investigated by exploring a CCP attack that misleads the protective measures to maximize system cascading failure risks. In particular,

1) this paper demonstrates the cascading failure vulnerability of N-1 secure power systems due to CCP attacks. It shows how protective power grid mechanisms can be maliciously leveraged by adversaries to aggravate the propagation of line outages.
2) a novel three-step CCP attack strategy is proposed by exploiting the vulnerability of the N-1 SCOPF, with an AC-based tri-level optimization formulated to analyze the attack impact. We show that although the N-1 SCOPF can mitigate the impact of traditional CCP attacks, the proposed CCP attack strategy can cause consecutive line tripping that may evolve into cascading failures.
3) a methodology based on semidefinite programming relaxation and primal-dual formulation method is proposed to transform the tri-level optimization into conic optimization, making the AC-based tri-level attack model more tractable.
4) numerical studies of the IEEE 14, 57, and 118 bus test systems verify the vulnerability of N-1 secure power systems and the impact of the CCP attack on cascading failures. The results shed light on defense measures and help to identify the transmission lines that are highly prone to CCP attacks.

II. Preliminaries

We consider a power network $\mathcal{G} = \{\mathcal{N}, \mathcal{L}\}$ with the set of buses $\mathcal{N} = \{1, ..., n\}$, the set of generator buses $\mathcal{N}_g \subseteq \mathcal{N}$, the set of transmission lines $\mathcal{L} \subseteq \mathcal{N} \times \mathcal{N}$. The line $k \in \mathcal{L}$ that connects bus i and bus j is denoted by $k = \{i, j\}$. Some important notations in this paper are summarized in Table I.

TABLE I: Summary of Nomenclature

Notation	Definition
V_i^{min}, V_i^{max}	minimum, maximum voltage magnitude of bus i
$P_{gi}^{min}, P_{gi}^{max}$	minimum, maximum real power of generator i
$Q_{gi}^{min}, Q_{gi}^{max}$	minimum, maximum reactive power of generator i
$DF_{k,m}$, $GF_{k,i}$	line outage distribution, generation shift factors
$\mathcal{M}$	set of screened contigency cases
P_{fk}^{max}	The flow limit of line k
$\boldsymbol{P}_d^{true}$	vector of actual load distribution
$\boldsymbol{P}_g^{(0)}$	vector of N-1 secure generation before attack
$\boldsymbol{P}_f^{(0)}$	vector of pre-attack line flows
τ	Upper bound of $\Delta P_{di}/P_{di}^{true}$ for each bus i
l_a	index of the line tripped by the physical attack
$\boldsymbol{P}_d$	vector of observed load distribution
$\Delta \boldsymbol{P}_d$	vector of injected load measurements by the attack
$\boldsymbol{P}_g^{(1)}$	vector of N-1 secure generation after attack
$\boldsymbol{P}_f^{(1)}$	vector of post-attack line flows
P_{fk}^A, Q_{fk}^A	false power flow measurements in cyber attack (A)
P_{fk}^B, Q_{fk}^B	false power flow measurements in cyber attack (B)
T	the nonconjugate transpose operator

A. AC Power flow model

In the AC power flow model, the power balance equations at bus i are stated as follows:

$$P_i - P_{gi} + P_{di} = 0 \tag{1a}$$
$$Q_i - Q_{gi} + Q_{di} = 0, \tag{1b}$$

where $P_{gi} + jQ_{gi}$, $P_{di} + jQ_{di}$, and $P_i + jQ_i$ are respectively the complex power generation, the load consumption, and the power injection at bus i.

In (1), the real and reactive power injections at bus i can be expressed as functions of voltage angles and magnitude:

$$P_i(\boldsymbol{V}, \boldsymbol{\theta}) = V_i \sum_{j=1}^{n} V_j [G_{ij} \cos\theta_{ij} + B_{ij} \sin\theta_{ij}] \tag{2a}$$
$$Q_i(\boldsymbol{V}, \boldsymbol{\theta}) = V_i \sum_{j=1}^{n} V_j [G_{ij} \sin\theta_{ij} - B_{ij} \cos\theta_{ij}], \tag{2b}$$

where V_i is the voltage magnitude of bus i, $\theta_{ij} = \theta_i - \theta_j$ is the phase angle difference between bus i and bus j, G_{ij} and B_{ij} are the real and imaginary part, respectively, of the $(i,j)^{th}$ element of nodal admittance matrix $\mathbf{Y} = \mathbf{G} + j\mathbf{B}$.

The active and reactive power flows on line $k = \{i, j\}$ are given by

$$P_{f_k}(\boldsymbol{V}, \boldsymbol{\theta}) = V_i^2(g_{si} + g_{ij}) - V_i V_j [g_{ij} \cos\theta_{ij} + b_{ij} \sin\theta_{ij}] \tag{3a}$$
$$Q_{f_k}(\boldsymbol{V}, \boldsymbol{\theta}) = -V_i^2(b_{si} + b_{ij}) - V_i V_j [g_{ij} \sin\theta_{ij} - b_{ij} \cos\theta_{ij}], \tag{3b}$$

where g_{ij} and b_{ij} are the conductance and the susceptance of line k, respectively. g_{si} and b_{si} are respectively the shunt conductance and the susceptance at bus i.

B. N-1 SCOPF

A single line outage may cause subsequent violations in line flow limits, called post-contingency overloads. As a preventive protection strategy, N-1 SCOPF aims to avoid the post-contingency overloads after a single contingency. This can be achieved by making real generation power adjustments to base-case generation [21].

The base-case generation only ensures the security of the power system without any contingency. It is obtained by solving the base-case optimal power flow (OPF), which is

$$\min_{\boldsymbol{P}_g} f(\boldsymbol{P}_g) = \sum_{i\in\mathcal{N}_g} c_i P_{gi} \tag{4a}$$

$$s.t.\quad P_i(\boldsymbol{V},\boldsymbol{\theta}) - P_{gi} + P_{di} = 0,\quad i\in\mathcal{N} \tag{4b}$$

$$Q_i(\boldsymbol{V},\boldsymbol{\theta}) - Q_{gi} + Q_{di} = 0,\quad i\in\mathcal{N} \tag{4c}$$

$$V_i^{min} \le V_i \le V_i^{max},\quad i\in\mathcal{N} \tag{4d}$$

$$P_{gi}^{min} \le P_{gi} \le P_{gi}^{max},\quad i\in\mathcal{N}_g \tag{4e}$$

$$Q_{gi}^{min} \le Q_{gi} \le Q_{gi}^{max},\quad i\in\mathcal{N}_g \tag{4f}$$

$$-P_{f_k}^{max} \le P_{f_k}(\boldsymbol{V},\boldsymbol{\theta}) \le P_{f_k}^{max},\quad k\in\mathcal{L}. \tag{4g}$$

The objective (4a) is to minimize the generation cost. The equality constraints (4b)-(4c) consist of nonlinear real power balance equations, the inequality constraint (4d) represents the voltage magnitude limits, (4e)-(4f) represent the generation limits, and (4g) represents the N-0 security constraints that prevent overloads when there is no contingency. Denote the solved base-case generation by $\boldsymbol{P}_g^e$. It is known that $\boldsymbol{P}_g^e$ does not guarantee line flow within the limits after a contingency.

To guarantee N-1 security, generation adjustment is made to the $\boldsymbol{P}_g^e$ by solving the OPF problem (4) with added N-1 security constraints, which are given by [21]

$$-P_{fk}^{max} \le P_{fk}^e + \Delta P_{f_{k,m}} \le P_{fk}^{max},\quad k\in\mathcal{L},\ m\in\mathcal{M}. \tag{5}$$

Here P_{fk}^e is the base-case line flow on line k corresponding to the generation $\boldsymbol{P}_g^e$, m is the index of the outage line, $\mathcal{M}$ is the set of worst contingency cases screened by the contingency analysis. $\Delta P_{f_{k,m}}$ is the post-contingency power flow deviation of line k under the adjusted power generation, which can be expressed based on the sensitivity factors:

$$\Delta P_{f_{k,m}} = DF_{k,m}\cdot P_{fm}^e + \sum_{i\in\mathcal{N}_g}(GF_{k,i} + DF_{k,m}\cdot GF_{m,i})\cdot(P_{gi} - P_{gi}^e). \tag{6}$$

In (6), $GF_{k,i}$, known as the generation shift factor, denotes the change of the power flow at line k with a change in generation of generator i; $DF_{k,m}$, known as the line outage distribution factor, denotes the change of the power flow at line k due to an outage of line m. Consequently, the secure generation can be obtained by solving the N-1 SCOPF problem (4a)-(6).

For ease of description, we represent the feasible regions of the base-case OPF and the N-1 SCOPF problems with set-valued mapping in the rest of the paper. That is, for a given observed load vector $\boldsymbol{P}_d$, let $\Omega_0(\boldsymbol{P}_d)$ denote the feasible region, the region constrained by (4b)-(4g), of the base-case OPF problem, and let $\Omega_1(\boldsymbol{P}_d, \boldsymbol{P}_g^e)$ denote the feasible region, the region constrained by (4b)-(6), of the N-1 SCOPF problem, where

$$\boldsymbol{P}_g^e := argmin\{f(\boldsymbol{P}_g) : \boldsymbol{P}_g \in \Omega_0(\boldsymbol{P}_d)\}. \tag{7}$$

Note that in AC power flow model, the line flow limits can be expressed in the form of apparent power, real power, or current flows [22, sec. IV.A]. For the purpose of making the problem easier to solve, and considering that thermal power limits on overhead transmission lines are intended to limit the conductor temperature whereas the effect of heat gain due to reactive power is negligible [23], this paper expresses the line flow limits in the form of real power for the N-0 and N-1 security constraints (4g)-(5). Also, although the dynamic line rating technology that determines the line thermal limits in real-time has been developed recently [24], this paper uses the line flow limits $P_{f_k}^{max}$ as constant parameters, since the NERC reliability guideline [25, pp. 17] has stated that interconnection reliability operating limits (which include thermal limits) should be established prior to real-time operation.

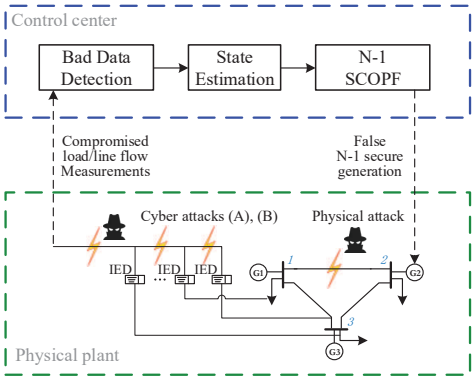


Fig. 1: System under the CCP attack.

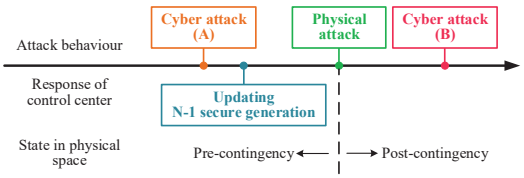


Fig. 2: Timeline of the CCP attack.

III. CCP ATTACKS IN N-1 SECURE POWER SYSTEMS

In this paper, a CCP attack is developed to analyze its impact on N-1 secure power systems. A block diagram of the system under the CCP attack is given in Fig. 1.

A. Assumptions

Considering practical situations in power systems, we make the following assumptions on the adversary's capabilities: 1) the adversary can observe and modify the power flow and the load measurements by eavesdropping and intruding the sensing channel [26], since the integration of information technology makes it easier for adversaries to access network traffic; 2) the adversary has knowledge of the network topology and parameters, since these information can be learned from historical data using the linear regression method [27]; 3) the adversary cannot modify the generation dispatch control command, since such attack can be easily detected by the watermarking-based methods [28]. We also assume that the actual load distribution does not change during the attack period, considering that power systems behave in a quasi-static manner [29].

B. A three-step model of the CCP attack

The primary objective of the CCP attack is to cause consecutive line tripping resulting cascading failures. In N-1 secure power systems, a physical attack on a single line is unable to induce consecutive line tripping, because the SCOPF prevents post-contingency overloads. In the CCP attack, to incite post-contingency overloads following the physical attack, a cyber

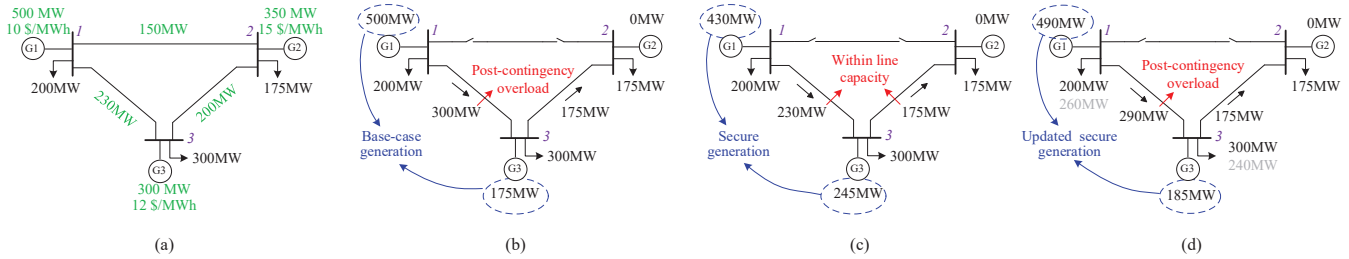


Fig. 3: Impact comparison of CCP attacks: (a) parameters, (b) impact of the traditional CCP attack on the system employing base-case OPF, (c) impact of the traditional CCP attack on the system employing N-1 SCOPF, (d) impact of the proposed CCP attack on the system employing N-1 SCOPF.

attack (A) is launched before the physical attack to deceive the control center into making a false generation dispatch. This is achieved through tampering with load measurements. After the cyber attack (A) in step 1 and the physical attack in step 2, a cyber attack (B) is launched in step 3 to mask the actual overload to hinder corrective actions. After the three steps, additional lines would be tripped by protective relays if they get overloaded above the tripping threshold. Such tripping would lead to the propagation of overload since no corrective action is taken. If this process continues, the initial outage would evolve into cascading failures. The timeline of the CCP attack is given in Fig. 2. Note that the CCP attack cannot purposely disconnect multiple lines through physical attacks, because 1) some critical transmission lines are secured and thus are hard to compromise, and 2) it is difficult to coordinate multiple physical attacks simultaneously, since the transmission lines spread over a large geographical area [15]. By contrast, based on the collaboration between the physical attack and cyberattacks, it is easier to achieve time coordination between the steps of the attack.

The impacts of CCP attacks on systems employing base-case OPF and N-1 SCOPF, respectively, are compared based on a simple 3-bus system, which further explains the motivation of studying the CCP attack based on N-1 SCOPF. The generator capacity, marginal cost, line capacity, and the load data are shown in Fig. 3(a). For a traditional CCP attack modeled without considering the N-1 security criterion, its impact on the system employing base-case OPF is shown in Fig. 3(b), where post-contingency overload occurs after the attack disconnects line 1-2. However, the traditional CCP attack fails to cause overload in the N-1 secure system, as shown in Fig. 3(c). For the proposed CCP attack, to make post-contingency overload possible in the N-1 secure system, as shown in Fig. 3(d), the cyber attack (A) falsifies the load measurements at bus 1 and bus 3 as 260 MW and 240 MW, respectively. The control center updates the generation dispatch to respond to the observed load perturbation, where the setting values of generator 1 and generator 3 are changed to 490 MW and 185 MW, respectively. Since the actual load distribution does not change, line 1-3 gets overloaded following the disconnection of line 1-2 under the updated generation. Assume the information of line status is not uploaded to the control center during the attack period, the cyber attack (B) masks the actual post-contingency overload by falsifying the line flows on line 1-2, line 1-3, and line 3-2 with the fake value 150 MW, 80 MW, and 25 MW, respectively. Since the fake line flow are consistent with the topology, generation and load known to the control center, the attack would not be detected.

C. Mathematical formulation of the proposed CCP attack

1) Objective function of CCP attack: The attack objective function is modeled to maximize the actual post-contingency line flow on an additional line after the cyber attack (A) and the physical attack, considering that the tripping probability is an increasing function of the line flow seen by the protective relay [30]. Suppose the CCP attack has misled the control center to make the false generation dispatch $\boldsymbol{P}_g^{(1)}$ and purposely disconnected line l_a. Let $\boldsymbol{P}_g^{(0)}$ and $\boldsymbol{P}_f{}^{(0)}$ denote respectively the power generation vector and the line flow vector in the normal system. Then after the cyber attack (A) and the physical attack, the actual line flow on a target line k, $k \in \mathcal{L}$, can be expressed as

$$P_{fk}^{(1)} = P_{fk}^{(0)} + DF_{k,l_a} \cdot P_{fl_a}^{(0)} + \sum_{i \in \mathcal{N}_g} (GF_{k,i} + DF_{k,l_a} \cdot GF_{l_a,i})(P_{gi}^{(1)} - P_{gi}^{(0)}). \tag{8}$$

2) Constraints of cyber attack (A): Cyber attack (A) aims to mask the falsified load measurements as a legitimate load perturbation. On the one hand, the "load perturbation" should be maintained within a reasonable range. On the other hand, state estimation error misled by load measurement changing should not be detected by the bad data detector. Motivated by these considerations, we obtain the following constraints for the cyber attack (A).

Suppose $\Delta \boldsymbol{P}_d$ is the change in load measurements injected by the attack, and $\boldsymbol{P}_d^{true}$ is the actual value of the load distribution. Firstly, to make the "load perturbation" reasonable, we have the constraint (9) for the cyber attack (A) such that the injected load measurement does not exceed fraction τ of its actual value and the observed total load value remains unchanged. Note that the value of τ may vary for different types of loads [12]. In this paper, the values of τ are set to $\tau \leq 50\%$.

$$\begin{aligned} \mathbf{1}^T \cdot \Delta \boldsymbol{P}_d &= 0 \\ -\tau \boldsymbol{P}_d^{true} \leq \Delta \boldsymbol{P}_d &\leq \tau \boldsymbol{P}_d^{true}. \end{aligned} \tag{9}$$

Secondly, to ensure that the compromised load measurements can bypass the bad data detector, the line flow mea-

surements are coordinately modified to satisfy physical laws. Suppose $\boldsymbol{P}_d$ is the compromised load measurements, i.e.,

$$\boldsymbol{P}_d = \boldsymbol{P}_d^{true} + \Delta \boldsymbol{P}_d. \tag{10}$$

Since the load and generation known to the control center in this stage are $\boldsymbol{P}_d$ and $\boldsymbol{P}_g^{(0)}$, respectively, the fake line flow measurements should be constructed according to (3) with the voltage values estimated from $\boldsymbol{P}_d, \boldsymbol{P}_g^{(0)}$. Consequently, we have the second constraint for the cyber attack (A)

$$\begin{aligned} &P_{fk}^A - P_{fk}(\hat{\boldsymbol{V}}_0, \hat{\boldsymbol{\theta}}_0) = 0, \quad k \in \mathcal{L} \\ &Q_{fk}^A - Q_{fk}(\hat{\boldsymbol{V}}_0, \hat{\boldsymbol{\theta}}_0) = 0, \quad k \in \mathcal{L}, \end{aligned} \tag{11}$$

where P_{fk}^A and Q_{fk}^A are the fake flow measurements of line k falsified by the cyber attack (A), and $\hat{\boldsymbol{V}}_0$ and $\hat{\boldsymbol{\theta}}_0$ are the estimated voltage values consistent with $\boldsymbol{P}_g^{(0)}$ and $\boldsymbol{P}_d$.

With contraints (9), (11) satisfied, the control center would update the generation dispatch to $\boldsymbol{P}_g^{(1)}$ by solving the N-1 SCOPF based on the falsified load measurements $\boldsymbol{P}_d$.

3) Constraints of cyber attack (B): Cyber attack (B) aims to mask the overload in the physical system caused by the cyber attack (A) and the physical attack. In normal operations, after the control center adjusts the generation dispatch, the system will transition to a new stable state. As such, the control center can detect the attack from the inconsistency between the expected value and the observed value of line flows after the generation redispatch. Hence, cyber attack (B) should make the line flow measurements conform to the expected line flow value. After the generation redispatch, the load and generation known to the control center are $\boldsymbol{P}_d$ and $\boldsymbol{P}_g^{(1)}$, respectively, thus the constraint for cyber attack (B) is

$$\begin{aligned} &P_{fk}^B - P_{fk}(\hat{\boldsymbol{V}}_1, \hat{\boldsymbol{\theta}}_1) = 0, \quad k \in \mathcal{L} \\ &Q_{fk}^B - Q_{fk}(\hat{\boldsymbol{V}}_1, \hat{\boldsymbol{\theta}}_1) = 0, \quad k \in \mathcal{L}, \end{aligned} \tag{12}$$

where P_{fk}^B and Q_{fk}^B are the fake flow measurements of line k falsified by the cyber attack (B). $\hat{\boldsymbol{V}}_1, \hat{\boldsymbol{\theta}}_1$ are the vectors of estimated voltage values consistent with $\boldsymbol{P}_g^{(1)}$ and $\boldsymbol{P}_d$.

4) Proposed CCP attack model: Distinct from traditional CCP attacks which are modeled as bilevel problems, the CCP attack considering "N-1 security criterion" is formulated as a tri-level optimization problem shown in Fig. 4. The mathematical formulation of the tri-level model is

$$\text{(P1)} \max_{l_a, \Delta \boldsymbol{P}_d} \quad P_{fk}^{(1)} \tag{13a}$$

$$s.t. \quad (9) - (12)$$

$$\boldsymbol{P}_g^{(1)} = \arg\min\{f(\boldsymbol{P}_g) : \boldsymbol{P}_g \in \Omega_1(\boldsymbol{P}_d, \boldsymbol{P}_g^e)\} \tag{13b}$$

$$\boldsymbol{P}_g^e = \arg\min\{f(\boldsymbol{P}_g) : \boldsymbol{P}_g \in \Omega_0(\boldsymbol{P}_d)\} \tag{13c}$$

The decision variables of the tri-level attack model are $\{l_a, \Delta \boldsymbol{P}_d\}$, and the optimization variables involved in the model are $\{l_a, \Delta \boldsymbol{P}_d, \boldsymbol{P}_g^{(1)}, \boldsymbol{P}_g^e, \boldsymbol{P}_d\}$.

In the attack model (13), the upper-level problem, also the outer optimization problem, is formulated from the adversary's perspective, to determine the value of the attack vector that maximizes the post-attack flow of a target line. The middle-level (13b) and the lower-level (13c) formulate the N-1 SCOPF from the operator's perspective, in which the lower level represents the base-case OPF whose optimal solution is required to construct the N-1 security constraints as shown in equations (5)-(6). In this tri-level optimization, the result of the upper-level problem, i.e., the attack vector $\Delta \boldsymbol{P}_d$, is used to update both the middle-level and the lower-level problems, because the operator needs to solve the base-case OPF and the N-1 SCOPF using the observed load distribution, whereas the observed load distribution is false information which has been compromised by $\Delta \boldsymbol{P}_d$. That is, given an attack vector $\Delta \boldsymbol{P}_d$ from the upper level, the lower-level problem first solves the base-case OPF to determine the optimal base-case generation $\boldsymbol{P}_g^e$, which is then transferred to the middle-level problem to determine the optimal secure generation $\boldsymbol{P}_g^{(1)}$. And this secure generation $\boldsymbol{P}_g^{(1)}$ is transferred back to the upper-level problem to update the attack vector $\Delta \boldsymbol{P}_d$. Note that in this model, by formulating the N-1 SCOPF based on the base-case OPF solution, we linearize the N-1 security constraints and make the tri-level problem easier to solve.

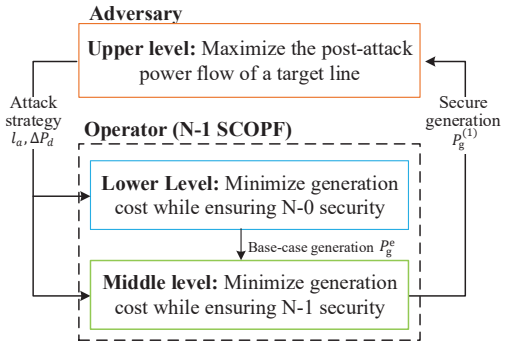


Fig. 4: Proposed tri-level model of the CCP attack.

IV. Solution Methodology of CCP Attack Model

The CCP attack model (13) is difficult to solve because of its tri-level structure and the non-convexity of the middle-level and the lower-level problems. To solve the CCP attack model, the middle-level and lower-level problems are convexified with semidefinite programming (SDP) relaxations and merged into one convex single-level problem. In this way, the tri-level attack model can be transformed into a bilevel optimization which has a convex inner problem. The convexity of the inner problem makes it possible to reduce the bilevel problem to a single-level problem using either strong duality theorem or KKT conditions. As a result, the original tri-level attack model can be transformed into a conic optimization problem, which can be solved by commercial solvers, such as "MOSEK" [31]. Note that constraints (11), (12) are omitted when solving the attack model, because they are redundant constraints, whose deletion does not change the feasible region.

A. Convexification of middle-level and lower-level problems

Let $\tilde{\boldsymbol{V}}^e$ and $\tilde{\boldsymbol{V}}$ be the vectors of the complex-valued voltage variables of the lower-level and the middle-level problems (13b), (13c), respectively, and define the variable $\mathbf{X}^e$, $\mathbf{X}$ as

$$\begin{aligned} \mathbf{X}^e &= [\mathrm{Re}\{\tilde{V}_1^e\} \quad ... \quad \mathrm{Re}\{\tilde{V}_n^e\} \quad \mathrm{Im}\{\tilde{V}_1^e\} \quad ... \quad \mathrm{Im}\{\tilde{V}_n^e\}]^T, \\ \mathbf{X} &= [\mathrm{Re}\{\tilde{V}_1\} \quad ... \quad \mathrm{Re}\{\tilde{V}_n\} \quad \mathrm{Im}\{\tilde{V}_1\} \quad ... \quad \mathrm{Im}\{\tilde{V}_n\}]^T. \end{aligned}$$

According to Lemma 1 in [32], the middle-level and the lower-level problems can be represented in a new form with the only optimization variables $\mathbf{X}^e$ and $\mathbf{X}$. The description of the new form is omitted to save space. By the change of variable $\mathbf{W}^e = \mathbf{X}^e\mathbf{X}^{eT}$, $\mathbf{W} = \mathbf{X}\mathbf{X}^T$, the middle-level and lower-level problems are reformulated as the bilevel optimization (20); see Appendix A for the detailed formulation. If $\mathbf{W}^e, \mathbf{W}$ are positive semidefinite, then the bilevel problem (20) is an SDP relaxation of the middle-level and the lower-level problems, which is a convex problem.

B. Simplified bilevel CCP attack model

With the special structure that the decision variable of the outer problem is not involved in the inner problem, i.e., the inner optimal is not affected by the outer optimal, the bilevel problem (20), i.e., the SDP of the middle-level and lower-level problems of the CCP attack model, can be merged into a single level problem by combining the objective functions of the outer and the inner problems with a weighting factor ω, and directly including the constraints (20b)-(20f) and (20h)-(20k) in the converted single-level problem.

As a result, the original CCP attack model is reduced to the following bilevel problem

$$\text{(P2)} \max_{l_a, \Delta \boldsymbol{P}_d} \quad P_{fk}^{(1)} \tag{14a}$$

$$s.t. \quad (9)-(10)$$

$$P_{gi}^{(1)} - P_{di} - \text{Tr}\{\mathbf{Y}_i\mathbf{W}\} = 0, \quad i \in \mathcal{N}_g \tag{14b}$$

$$\text{where } \mathbf{W} = \arg\Big\{$$

$$\min \sum_{i\in\mathcal{N}_g} c_i(\text{Tr}\{\mathbf{Y}_i\mathbf{W}^e\}+P_{di}) + \omega \sum_{i\in\mathcal{N}_g} c_i(\text{Tr}\{\mathbf{Y}_i\mathbf{W}\}+P_{di}) \tag{14c}$$

$$s.t. \quad (20b)-(20f), (20h)-(20k)\Big\}$$

whose inner optimization is the resulting single-level problem from problem (20). Based on Theorem 1 in [33], this inner optimization problem has the same optimal solution as the problem (20) if the value of ω is selected appropriately.

Since the inner optimization of problem (14) is a SDP, its necessary and sufficient conditions for optimality can be provided by Karush-Kuhn-Tucker (KKT) conditions or primal-dual formulation. Therefore, it is possible to reduce problem (14) to a single-level problem by replacing the inner optimization by its necessary and sufficient conditions, which is introduced in the following subsection.

C. Reduced single-level CCP attack model

Considering that using KKT conditions would introduce binary variables when linearizing large number of nonlinear complementary slackness conditions, and it is difficult to solve the problem involving both integer variables and semidefinite matrix variables, we adopt the primal-dual formulation in this section to convert problem (14) to a single-level problem.

Let

- $\underline{\kappa_i}(\overline{\kappa_i})$, $\underline{\lambda_i}(\overline{\lambda_i})$, $\underline{\gamma_i}(\overline{\gamma_i})$, $\underline{\mu_k}(\overline{\mu}_k)$, $\underline{\upsilon}_{k,m}(\overline{\upsilon}_{k,m})$ be the Lagrange multipliers associated with the lower (upper) bound of the inequality constraints (20b), (20c), (20d), (20e), and (20f), respectively.
- $\underline{\kappa_i^e}(\overline{\kappa_i^e})$, $\underline{\lambda_i^e}(\overline{\lambda_i^e})$, $\underline{\gamma_i^e}(\overline{\gamma_i^e})$, $\underline{\mu_k^e}(\overline{\mu}_k^e)$ be the Lagrange multipliers associated with the lower (upper) bound of the inequality constraints (20h), (20i), (20j), and (20k), respectively.

In the primal-dual formulation, the inner optimization of problem (14) is replaced by its primal constraints, dual constraints, and the strong duality theorem equality, which yields the following single-level CCP attack model

$$\text{(P3)} \max_{l_a, \Delta \boldsymbol{P}_d} \quad P_{fk}^{(1)} \tag{15a}$$

$$s.t. \quad (9)-(10)$$

$$P_{gi}^{(1)} - P_{di} - \text{Tr}\{\mathbf{Y}_i\mathbf{W}\} = 0, \quad i \in \mathcal{N}_g \tag{15b}$$

$$(20b)-(20f), (20h)-(20k)$$

$$\underline{\kappa_i^e} \geq 0, \overline{\kappa_i^e} \geq 0, \underline{\kappa_i} \geq 0, \overline{\kappa_i} \geq 0, \quad i \in \mathcal{N} \tag{15c}$$

$$\underline{\lambda_i^e} \geq 0, \overline{\lambda_i^e} \geq 0, \underline{\lambda_i} \geq 0, \overline{\lambda_i} \geq 0, \quad i \in \mathcal{N} \tag{15d}$$

$$\underline{\gamma_i^e} \geq 0, \overline{\gamma_i^e} \geq 0, \underline{\gamma_i} \geq 0, \overline{\gamma_i} \geq 0, \quad i \in \mathcal{N} \tag{15e}$$

$$\underline{\mu_k^e} \geq 0, \overline{\mu}_k^e \geq 0, \underline{\mu_k} \geq 0, \overline{\mu}_k \geq 0, \quad i \in \mathcal{N} \tag{15f}$$

$$\underline{\upsilon}_{k,m} \geq 0, \overline{\upsilon}_{k,m} \geq 0, \quad k \in \mathcal{L},\ m \in \mathcal{M} \tag{15g}$$

$$\mathbf{\Gamma}^e \succcurlyeq 0, \mathbf{\Gamma} \succcurlyeq 0 \tag{15h}$$

$$\boldsymbol{S} = 0 \tag{15i}$$

where (20b)-(20f) and (20h)-(20k) are the primal constraints, (15c)-(15h) are the dual constraints, (15i) is the strong duality theorem equality. The expressions of $\mathbf{\Gamma}^e$, $\mathbf{\Gamma}$ and $\boldsymbol{S}$ are given in Appendix B.

In the single-level attack model (15), it can be seen that for each l_a, all the constraints are convex except for the constraint (15i), whose nonconvexity is due to the bilinear terms which are the product of Lagrange multipliers and P_{di}. In order to linearize the constraint (15i), we apply McCormick relaxation [34] to replace the bilinear terms in (15i) with

$$\underline{\beta_i^e} = \underline{\lambda_i^e} P_{di},\ \overline{\beta_i^e} = \overline{\lambda_i^e} P_{di},\ \underline{\beta_i} = \underline{\lambda_i} P_{di},\ \overline{\beta_i} = \overline{\lambda_i} P_{di}, \tag{16}$$

where the additional constraints on $\underline{\beta_i^e}, \overline{\beta_i^e}, \underline{\beta_i}, \overline{\beta_i}$ are given based on the bounds of $\underline{\lambda_i^e}, \overline{\lambda_i^e}, \underline{\lambda_i}, \overline{\lambda_i}$ and P_{di}. To save space, here we only give the McCormick relaxation of the bilinear term $\underline{\lambda_i} P_{di}$ as an example. Suppose $0 \leq \underline{\lambda_i} \leq b^u$ and the bounds on P_{di} are given by (9) and (10), i.e., $(1-\tau)P_{di}^{true} \leq P_{di} \leq (1+\tau)P_{di}^{true}$, the bilinear term $\underline{\lambda_i} P_{di}$ is replaced by $\underline{\beta_i}$ with the additional constraints given by

$$\begin{aligned} &(1-\tau)P_{di}^{true}\underline{\lambda}_i \leq \underline{\beta}_i \leq (1-\tau)P_{di}^{true}(\underline{\lambda}_i - b^u) + b^u P_{di} \\ &(1+\tau)P_{di}^{true}(\underline{\lambda}_i - b^u) + b^u P_{di} \leq \underline{\beta}_i \leq (1+\tau)P_{di}^{true}\underline{\lambda}_i \end{aligned} \tag{17}$$

Consequently, the single-level CCP attack model is converted to a conic optimization for each l_a, which can be solved using SDP solvers.

D. Discussion

Considering that the proposed CCP attack is for real-time application, the optimal CCP attack should be solved very quickly. The proposed method could be slow in solving the CCP attack model for large-scale power systems, as the number of semidefinite variables and nonlinear constraints increases with the system size. In order to improve the scalability of the proposed CCP attack method in large-scale

power systems, we discuss the following three possible ways to speed up the process of solving the CCP attack:

1. Use an approximate model of the power system (e.g., DC power flow model) in the formulation of the CCP attack model to reduce the computing complexity;
2. Select only the important physical attack cases[1], where the corresponding CCP attack will result in nontrivial impacts, for detailed analysis to reduce the number of runs (this method is referred to as "selection method" in the remainder of this paper);
3. Use professional computing facilities made up of multiple processors or vector processors to speed up calculations.

For the first method, the use of DC power flow model can faciliate fast CCP attack solutions but at the cost of accuracy. This method can be used to design the CCP attack for power systems where the voltage magnitudes are not of great concern or large-scale power systems with thousands of buses. For example, Chu et al. [35] analyzed the vulnerability of Polish system with 2383 buses to false data injection attacks using the DC power flow model. However, for the power systems where the voltage magnitude and reactive power are of great concern, the attack based on the DC power flow model could be easily detected. In such cases, the AC power flow model must be considered for modeling the CCP attack, where the accuracy can be improved but at the cost of timeliness. Thus, there exists a trade-off between using the DC power flow model and using the AC power flow model for attack modeling. The trade-off analysis is out of scope of this paper and could be studied in our future work.

When the AC power flow model is used in the modeling of the CCP attack, the process of solving the optimal CCP attack consists of running the conic optimization (P3) for each possible physical attack case. Considering all possible physical attack cases for detailed anaylsis could significantly increase the computing time, especially in large-scale power systems. Fortunately, only for very few of the physical attack cases the corresponding CCP attack will have severe impact. That is, most of the time spending for multiple runs of the conic optimization (P3) will go for solutions of the CCP attack that cause no overload in the power system. Therefore, the second method to speed up the process of solving the CCP attack is to select the important physical attack cases (where the corresponding CCP attack can cause overload) to perform the detailed analysis, and leave the other cases unanalyzed. In this paper, we can select the transmission lines that are adjacent to 1) the target line of the CCP attack, or, 2) the transmission lines being congested before attack, to be the candidates for the physical attack, as the existing studies have stated that:" an outage only has a limited geographical effect" [21, Chapter 11.3.5], and "when transmission elements trip out of service, the power that was flowing on the element must be picked up by the remaining transmission system. The majority of power will be transferred on the electrically close transmission elements" [25, Chapter 5]. Note that using this selection method might cause an error of not including all the physical attack cases where overload can occur after the CCP attack. This error does not affect the attack implementation, because the adversaries do not have to launch the optimal CCP attack if a suboptimal CCP attack can also have nontrivial impact on power systems.

For the third method, the use of better computing environments could significantly improve the speed of solving the CCP attack. Special computing facilities including specialized parallel computers, cluster computing, grid computing, and vector processors, etc., can facilitate the the real-time solutions of the CCP attack by running the conic optimization (P3) for different physical attack cases in parallel. This method can also be coordinated with the second method for a faster solution.

[1]different physical attack cases correspond to different values of l_a.

V. Case studies

In this section, case studies are conducted on the IEEE 14, 57, and 118 bus test systems, to illustrate the basic ideas of the proposed CCP attack, test the feasibility of the attack with limited attack resources, and validate the effect of attack limitation on attack consequences. We also compare the impacts of the proposed CCP attack strategy designed to mislead the N-1 SCOPF and the existing CCP attack strategy designed to mislead the base-case OPF.

Since the cascading failures result from line tripping in essence, we measure the tripping probability at the target line under the CCP attack using the following function [30]

$$prob = \begin{cases} 0, & 0 \le |P_{fk}^{(1)}| < P_{fk}^{max} \\ \frac{|P_{fk}^{(1)}| - P_{fk}^{max}}{(\alpha-1)\cdot P_{fk}^{max}}, & P_{fk}^{max} \le |P_{fk}^{(1)}| < \alpha \cdot P_{fk}^{max} \\ 1, & |P_{fk}^{(1)}| \ge \alpha \cdot P_{fk}^{max}. \end{cases} \quad (18)$$

That is, the tripping probability at the target line k is zero when the post-contingency power flow $P_{fk}^{(1)}$ is within the line flow limit P_{fk}^{max} and increase linearly to 1 when the post-contingency power flow $P_{fk}^{(1)}$ exceeds the α times the line flow limit P_{fk}^{max}. In the following case studies, α is set to be 120%, based on NERC Standard PRC-023-1 R1.2 [36] indicating that "transmission line relays are set so they do not operate at or below 115% of the facility's highest rating".

All tests are conducted on a AMD EPYC 3GHz based server with 32 cores and 128 GB of RAM. The software toolbox MATPOWER [22] is used to provide initial information of the test system, and to calculate the physical power flow after the CCP attack by running "runpf". The toolbox "YALMIP" [37] together with the "MOSEK" solver [31] are used to solve the reduced single-level optimization (15) to obtain the optimal CCP attack strategy.

A. Implementation and consequences of the CCP attack

To show the attack implementation and consequences in detail, we use the IEEE 14-bus system as the test system. The load data used in the tests are given in Table II. The line flow limits are given in the $9th$ column of Table III. The real power limits for generator 1 and generator 2 are 200MW and 500MW, respectively. Other configuration data of the test system is obtained from the MATPOWER package [38].

Table III shows the optimal attack strategy for the target line 2-5 (line connecting bus 2 and bus 5) and $\tau = 0.3$, where the

TABLE II: Load data (MW)

Bus	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Load	0	146.7	14.2	17.8	82.6	11.2	0	0	29.5	9	3.5	6.1	13.5	16.9

TABLE III: The optimal attack strategy and consequences

Line	$\boldsymbol{P}_f^{(0)}$ (MW)	$\boldsymbol{P}_f^{(1)}$ (MW)	$\boldsymbol{P}_f^A$ (MW)	$\boldsymbol{Q}_f^A$ (MVAr)	$\boldsymbol{P}_f^B$ (MW)	$\boldsymbol{Q}_f^B$ (MVAr)	N-1-1 (MW)	P_{fk}^{max} (MW)
1-2	3.63	-13.04	8.22	21.21	3.91	22.62	-54.74	100
1-5	34.87	55.01	29.51	8.03	35.17	8.45	**101.22**	100
2-3	25.54	43.53	21.28	11.34	24.90	10.62	**74.58**	60
2-4	41.38	0	34.96	0.30	42.52	-0.26	0	100
2-5	42.86	**73.43**	34.68	0.43	43.12	0.03	0	60
3-4	10.99	28.475	9.22	-12.12	12.77	-11.98	57.98	60
4-5	3.57	-25.209	-3.19	0.43	-0.02	0.89	1.39	60
4-7	19.03	22.45	18.27	-6.96	23.09	-8.17	23.23	60
4-9	10.90	12.83	10.46	1.24	13.22	0.48	13.25	100
5-6	-2.90	16.20	-4.78	12.45	11.97	11.12	14.96	100
6-11	17.18	13.71	18.06	0.48	13.18	1.77	12.92	100
6-12	9.15	8.75	9.27	1.89	8.67	2.15	8.69	100
6-13	23.40	21.64	23.88	5.84	21.39	6.43	21.26	100
7-8	0	0	0	-17.40	0	-17.20	0	100
7-9	19.03	22.45	18.27	9.70	23.09	7.89	23.23	90
9-10	-4.28	-0.97	-5.08	8.11	-0.43	6.32	-0.20	90
9-14	4.71	6.75	4.23	6.25	7.17	5.08	7.18	90
10-11	-13.30	-9.97	-14.13	2.24	-9.46	0.49	-9.20	90
12-13	2.96	2.56	3.06	0.09	2.47	0.37	2.50	90
13-14	12.50	10.39	13.04	-0.57	10.02	0.43	9.95	90

actual load is given in Table II. The pre- and post-attack line flows, and the false line flow measurements in cyber attack (A) and cyber attack (B) are listed. It shows that after the CCP attack, the real power flow on the target line 2-5 is 73.43 MW, which exceeds 120% of the line flow limit. According to the function (18), the tripping probability of line 2-5 is equal to 1. Thus, the N-1-1 contingency, i.e., consecutive losses of two lines, is caused by the CCP attack. To further study the consequences of the CCP attack, we verify the real power flows in the physical system after the N-1-1 contingency. The results are given in the $8th$ column of Table III. It can be seen that the real power flows on line 1-5 and line 2-3 are 101.22 MW and 74.58 MW, respectively, which are greater than the corresponding line flow limits. Therefore, two additional lines get overloaded after the N-1-1 contingency. These results show that an adversary is able to induce cascading failures by starting with only one line outage, if coordinated cyber attacks are launched simultaneously.

Given the optimal attack strategy, the suitability and justification of the solution methodology presented in Section IV, including the convexification and merging of the middle-level and lower-level problems, is validated as follows. We compare the base-case and N-1 secure generation values obtained by solving the detailed model of the middle-level and lower-level problems with the values obtained by solving the simplified (e.g. convexified and merged) model presented in Section IV. Note that the detailed model of the N-1 SCOPF is solved by extending the "runopf" function provided in MATPOWER, where the Newtons's method is used. Table IV shows the generation values corresponding to the detailed and simplified models, and the Euclidean distance between them. It can be seen that the Euclidean distances for the base-case generation is 0.3428, which is 0.11% of the generation

TABLE IV: Comparison between the detailed model and the simplified model

# of	Base-case gen. (MW)		N-1 secure gen. (MW)	
gen.	detailed model	simplified model	detailed model	simplified model
1	51.534	51.776	38.762	38.872
2	304.85	304.6	276.91	276.88
3	0	0	0	0
4	0	0	39.11	39.025
5	0	0	0	0.0003
Eucl. dist.	0.3428		0.1411	

magnitude of the detailed model. And the Euclidean distances for the N-1 secure generation is 0.1411, which is 0.05% of the corresponding generation magnitude of the detailed model. Therefore, the differences in the results obtained by solving the detailed model and the simplified model are small enough to ignore. This indicates that the detailed model can be well approximated by the simplified model.

B. Approximating attack vector for reducing attack cost

Considering limited attack resources in practical operation, it is better for the attacker to compromise fewer measurements to achieve the attack goal. In this paper, although the attack vector $\Delta \boldsymbol{P}_d$, the malicious modification of load measurements, is not a sparse vector, most of its elements are small enough to ignore. Thus it is possible to reduce the attack cost in practical operation by approximating the calculated attack vector with a sparse attack vector. For instance, an approximation of $\Delta \boldsymbol{P}_d$, denoted by $\Delta \boldsymbol{P}'_d$, can be given by

$$\Delta P'_{di} = \begin{cases} 0, & \text{if } |\Delta P_{di}| \leq \epsilon \cdot P_{di}^{true}, \ \epsilon \text{ is a small value} \\ \Delta P_{di}, & \text{otherwise.} \end{cases} \tag{19}$$

Here we use IEEE 14-bus test system as an example to show the feasibility of the approximation. The actual load is given in Table II. The value of ϵ is determined considering both the attacker's capability and the change in attack consequence caused by the approximation. Table V shows the test results with $\epsilon = 1\%$.

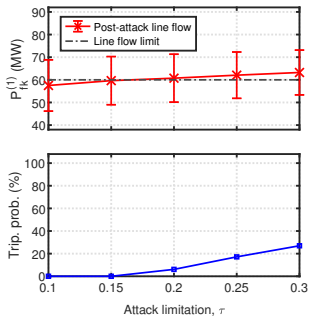
TABLE V: Load attack vectors (MW) & post-attack line flows (MW) before and after approximation.

Bus	$\tau = 0.1$		$\tau = 0.3$		$\tau = 0.5$	
	$\Delta \boldsymbol{P}_d$	$\Delta \boldsymbol{P}'_d$	$\Delta \boldsymbol{P}_d$	$\Delta \boldsymbol{P}'_d$	$\Delta \boldsymbol{P}_d$	$\Delta \boldsymbol{P}'_d$
1	0	0	0	0	0	0
2	1.079	0	23.462	23.462	50.928	50.928
3	-0.711	-0.711	-2.411	-2.411	-6.684	-6.684
4	0.014	0	0.045	0	0.090	0
5	0.067	0	-17.935	-17.935	-39.468	-39.468
6	-0.515	-0.515	-3.36	-3.36	-5.268	-5.268
7	0	0	0	0	0	0
8	0	0	0	0	0	0
9	0.024	0	0.074	0	0.150	0
10	0.007	0	0.023	0	0.046	0
11	0.003	0	0.009	0	0.018	0
12	0.005	0	0.015	0	0.031	0
13	0.011	0	0.034	0	0.069	0
14	0.014	0	0.043	0	0.087	0
$P_{fk}^{(1)}$	61.770	61.714	73.431	73.521	87.279	87.461

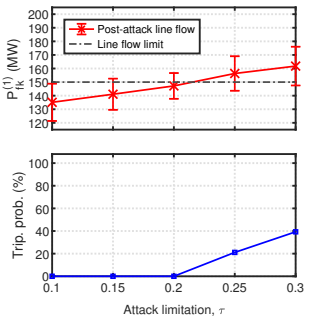
Table V gives the calculated attack vector $\Delta \boldsymbol{P}_d$ and the approximated attack vector $\Delta \boldsymbol{P}'_d$, and the resulting post-attack line flows at the target line 2-5 for different τ. It is shown that the attacker needs to compromise no more than **four** load measurements after approximating the load attack vector, which is a small number compared to the number of buses. And the post-attack power flow under the approximated attack vector $\Delta \boldsymbol{P}'_d$ is very close to that under the calculated attack vector $\Delta \boldsymbol{P}_d$. This indicates that the approximation barely has impacts on the attack consequences. Hence, making approximation is a reasonable and useful way for the attacker with limited attack resources to launch attack in practical.

C. Influence of attack limitation

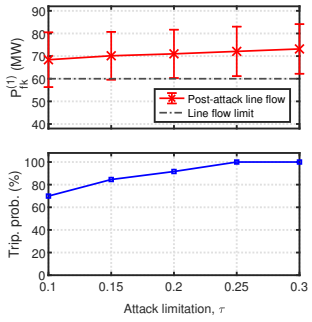
It is known from the CCP attack model (13) that the optimal attack strategy is limited by the value of τ in constraint (9). In order to learn its impact on the risk of cascading failures, we test the attack consequences with different values of τ ranging from 0.1 to 0.3. Moreover, considering the possible influence of the actual load, we conduct the tests at both a low load level and a high load level, where 100 load profiles are randomly generated for each load level[2].



(a) Low load level (200 MW).

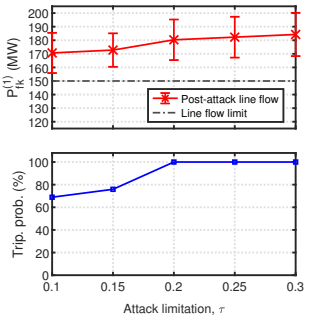


(a) Low load level (1000 MW).



(b) High load level (300 MW).

Fig. 5: Post-attack power flow & tripping probability at line 2-5 (14-bus system).



(b) High load level (1500 MW).

Fig. 6: Post-attack power flow & tripping probability at line 8-9 (57-bus system).

Fig. 5 and Fig. 6 illustrate the average post-attack power flow (with errorbars demonstrating the standard deviation) and tripping probability at the target line in the IEEE 14-bus system and IEEE 57-bus system, respectively. The total load of the different load levels are shown in the figures. It can be seen that in both test systems, the post-attack power flow at the target line increases with the value of τ. In the IEEE 14-bus system at a low load level of 200 MW, the average post-attack line flow at the targte line 2-5 does not exceed the line flow limit until the value of τ is larger than 0.2; although line 2-5 gets overloaded when $\tau > 0.2$, its post-attack line flow does not exceed 120% of the line flow limit. That is, in this case, the CCP attack does not cause false tripping of the target line, which does not induce cascading failures as a result. However, in the IEEE-14 bus system at a high load level of 300 MW, line 2-5 gets overloaded even when $\tau = 0.1$, and its tripping probability increases to 1 when $\tau \geq 0.25$. Similarly, in the IEEE 57-bus system at a low load level of 1000 MW, the post-attack power flow at the target line 8-9 is within the line flow limit when $\tau \leq 0.2$, whereas at a high load level of 1500 MW, line 8-9 is overloaded for all values of τ from 0.1 to 0.3, and its tripping probability increases to 1 when $\tau \geq 0.2$. These results indicate that even if the adversary has full control over the system measurements, the attack impact over the system are extremely limited by the value of τ. And the systems operating at a high load level would be more vulnerable to the CCP attacks.

D. Comparison of CCP attack strategies with and without consideration of N-1 security criterion

For comparison, we test both the proposed CCP attack and the traditional CCP attack [17], [18], which are respectively called the tri-level and the bilevel attacks in the following, to observe their impacts. The IEEE 57-bus test system is used as an example, where the flow limit of the lines 7∼16 is 150 MW, and the remaining lines have the flow limit 110 MW. The value of τ is set as 0.3. To better illustrate the comparison results, we have exhaustively targeted all the transmission lines to implement the bilevel attack, and find that the bilevel attack causes the largest increase in the power flow at line 8-9. Hence, in the comparison test, line 8-9 is selected as the target line for both of the attacks. The results show that, with the same purpose to maximize the post-attack power flow on line 8-9, the optimal strategy for the tri-level CCP attack is to disconnect line 7-29 while the optimal strategy for the bilevel CCP attack is to disconnect line 7-8. To save space, we do not list the value of $\Delta \boldsymbol{P}_d$. Instead, for the both attack strategies, we record in Table VI the false generation dispatches (including the base-case generation and the N-1 secure generation), and the corresponding post-attack line flow on line 8-9.

As shown in Table VI, the tri-level attack is more threatening than the bilevel attack. The tri-level CCP attack is able to cause post-contingency overload in both the systems employing the base-case OPF and the N-1 SCOPF, with the post-attack line flows being 227.69 MW and 178.75 MW, respectively. However, for the bilevel CCP attack, the post-attack line flow on line 8-9 exceeds the capacity only in the system employing the base-case OPF, while it remains within the capacity in the system employing the N-1 SCOPF. This indicates that the impact of the tri-level attack on the N-1 secure power systems is more severe than that of the bilevel attack, even in the best case of the bilevel attack.

[2]The load profiles where the N-1 SCOPF does not converge are not selected during the tests.

TABLE VI: False generation dispatch (MW) and post-attack line flow (MW) corresponding to different attack strategies

# of	Without attack		Tri-level attack		Bilevel attack	
gen.	base. gen.	sec. gen.	base. gen.	sec. gen.	base. gen.	sec. gen.
1	310	313	256.99	321.21	249.60	284.05
2	0	0	0	0	0	0
3	140	124.44	140	131.57	140	116.32
4	0	0	0	41.4	0	3.47
5	407.06	323.77	458.32	362.48	470.41	363.93
6	0	94.29	0	0	0	91.82
7	410	410	410	409.98	410	410
$P_{fk}^{(1)}$	–	–	**227.69**	**178.75**	**231.15**	137.08

E. Impact of different physical attacks

In this subsection, the impact of different physical attacks on the consequence of the CCP attack is tested on the IEEE 118-bus test system, which has 186 transmission lines and 54 generators. The system data is available in https://jbox.sjtu.edu.cn/l/9F3eT2. Note that it is a key step in the CCP attack to purposely disconnect a transmission line l_a through the physical attack to initiate a line outage. Even though the physical attack should disconnect the line whose outage will further cause the most severe overload at the target line, the line may be inaccessible to the physical attack in practical operation. In this case, other lines need to be considered for the physical attack. Also, from the defender's perspective, it helps to design the defense strategy by identifying the most damaging physical attacks. To learn how different physical attacks affect the implementation and consequence of the CCP attack, we conduct the CCP attacks where different l_a is disconnected. The value of τ is set to be $\tau = 0.3$, and line 17-30 is selected as the target line of the CCP attacks.

TABLE VII: The most damaging physical attacks

Physical attack	$P_{fk}^{(1)}$ (MW)	Overloaded lines
Line 8-30	292.471	{17-30, 38-65}
Line 5-8	287.222	{17-30, 38-65}
Line 37-38	247.231	{17-30, 8-30, 30-38, 38-65}
Line 25-27	188.107	{38-65}
Line 33-37	177.176	{38-65}
Line 23-32	176.857	{38-65}

Table VII shows the most damaging physical attacks ranked according to the post-attack power flow at line 17-30. For each physical attack, the resulting overloaded transmission lines and power flow at line 17-30 after the CCP attack are listed correspondingly. Note that the line flow limit at line 17-30 is 200 MW. It can be seen that the best physical attack is to disconnect line 8-30 that is adjacent to the target line, and the corresponding post-attack power flow at line 17-30 is 292.471 MW, which exceeds the 120% of the line flow limit. In addition to this physical attack, disconnecting line 5-8 and line 37-38 can also result in post-attack overload at line 17-30. We observe that even though disconnecting line 37-38 does not cause the most severe overload at the target line, the number of overloaded lines is the largest, and most of the overloaded lines are adjacent to each other. Moreover, the results show that line 38-65 gets overloaded in all the cases, even in the case where line 17-30 does not get overloaded. This is because line 38-65 is a congested line before attack, with the pre-attack power flow being -291.91 MW and the line flow limit being 300 MW. The above results indicate that the transmission lines that are congested and adjacent to the target line are more vulnerable to the CCP attack.

F. Utilization of selection method for reducing the computing time of CCP attack

As discussed in Section IV-D, in order to improve the scalability of the proposed CCP attack, three methods have been taken into account to reduce the computing time of the CCP attack. The first method is about using DC power flow model, which is out of scope of this paper; and due to the limited access to professional computing facilities (i.e., the third method), here we only show the effect of the selection method on improving the scalability of the proposed CCP attack, by comparing the computing time of the CCP attack with and without applying the selection method. Table VIII shows the results regarding computing time on the IEEE 14, 57, and 118-bus test systems.

TABLE VIII: Computing time with/without selection method for different test systems

Test system	Computing Time (seconds)	
	Without selection method	With selection method
14-bus system	10.438	1.341
57-bus system	2.84e3	264.426
118-bus system	5.79e5	5.26e3

It can be seen from Table VIII that even in our computing environment, the computing time of CCP attack with selection method is less than 15 minutes for both the IEEE 14-bus system and the IEEE 57-bus system, which is within the time frame of real-time OPF operations. Even though the computing time for IEEE 118-bus test system is still more than 15 minutes with selection method applied, it has been significantly reduced to 0.91% of its original value without selection method; and coordinating the high performance computing facilities with the selection method would further improve the computing efficiency and enhance the scalability of the CCP attack in practical operations.

Moreover, as pointed out in Section IV-D, using this selection method might cause an error of not including all the cases where overload can occur after the CCP attack. In this case, solving the CCP attack model (13) with the selection method might not yield the optimal attack solution. To evaluate the solution quality of the selection method, we solve the problem (13) without the selection method to find the optimal CCP attack, and compare it with the CCP attack obtained by the selection method. We repeat the test based on 100 load profiles which are randomly generated to obtain statistical results. The tests are conducted based on the IEEE 14 and 57-bus test systems, and the value of τ is set to be 0.15 in the tests. Note that the tests on the IEEE 118-bus test system are not

TABLE IX: Solution quality of the selection method

Test system	Success rate	Subopt. rate	Quality of subopt.
14-bus system	90.25%	7.25%	97.43%
57-bus system	93%	4.5%	90.4%

implemented, because the process of solving the CCP attack model without using the selection method is difficult to repeat in our computing environment, making it impossible to obtain the optimal solution as the benchmark for comparison. The results regarding the solution quality of the selection method are provided in Table IX, with the following performance indicators calculated:

1) *success rate*, at which the CCP attack obtained using the selection method is the same as the optimal CCP attack obtained without using the selection method;
2) *suboptimal solution rate*, at which the CCP attack obtained with the selection method is less optimal than the attack obtained without using the selection method, but can also result in nontrivial attack impact in the system;
3) *quality of suboptimal solutions*, which is calculated as the ratio of the average post-attack power flow (at the target line) under the suboptimal CCP attack to the average post-attack power flow under the corresponding optimal CCP attack.

The results in Table IX show that the success rate of the selection method is more than 90% in both the test systems. The suboptimal solution rates are 7.25% and 4.5% for the IEEE 14-bus system and the IEEE 57-bus test system, respectively. And the sum of the success rate and the suboptimal solution rate is more than 97% in both the test systems. Besides, even in the suboptimal solution cases the impact of the suboptimal CCP attack is nontrivial compared to that of the corresponding optimal CCP attack, as the average post-attack power flow caused by the suboptimal CCP attack is more than 90% of that caused by the optimal CCP attacks. This validates the high quality of the suboptimal solutions.

VI. Conclusion

This paper analyzed the vulnerabilities of power systems secured against N-1 contingencies to CCP attacks. A tri-level CCP attack model was proposed, which aims to cause cascading line trippings after a physical attack by coordinating cyber attacks to mislead the N-1 SCOPF and mask the line overload in physical systems. A methodology was proposed to convert the tri-level attack model into a conic optimization. Case studies demonstrate that the proposed CCP attack can cause tripping of additional lines, i.e., N-1-1 contingency, in N-1 secure systems, and the attack impact is extremely limited by the bound of change in load measurements. The proposed model provides a risk assessment tool and helps in improving related system protection strategies. Future work will address additional problems, e.g., mitigation method of CCP attacks, trade-off analysis between using the DC power flow model and using the AC power flow model for attack modeling.

Appendix A

The reformulation of the middle-level and lower-level problems is given as follows, where the value of $\mathrm{Tr}\{\mathbf{Y}_i\mathbf{W}\}+P_{di}$ is equal to the value of $P_{gi}^{(1)}$, and the value of $\mathrm{Tr}\{\mathbf{Y}_i\mathbf{W}^e\}+P_{di}$ is equal to the value of P_{gi}^{e}.

$$\min_{\mathbf{W}} \sum_{i\in\mathcal{N}_g} c_i(\mathrm{Tr}\{\mathbf{Y}_i\mathbf{W}\}+P_{di}) \tag{20a}$$
$$s.t.\ \ (V_i^{min})^2 \le \mathrm{Tr}\{\mathbf{M}_i\mathbf{W}\} \le (V_i^{max})^2,\ \ i\in\mathcal{N} \tag{20b}$$
$$P_{gi}^{min}-P_{di} \le \mathrm{Tr}\{\mathbf{Y}_i\mathbf{W}\} \le P_{gi}^{max}-P_{di},\ \ i\in\mathcal{N} \tag{20c}$$
$$Q_{gi}^{min}-Q_{di} \le \mathrm{Tr}\{\bar{\mathbf{Y}}_i\mathbf{W}\} \le Q_{gi}^{max}-Q_{di},\ \ i\in\mathcal{N} \tag{20d}$$
$$-P_{fk}^{max} \le \mathrm{Tr}\{\mathbf{Z}_k\mathbf{W}\} \le P_{fk}^{max},\ \ k\in\mathcal{L} \tag{20e}$$
$$\begin{aligned}-P_{fk}^{max} \le{}& \mathrm{Tr}\{\mathbf{Z}_k\mathbf{W}^e\}+DF_{k,m}\cdot\mathrm{Tr}\{\mathbf{Z}_m\mathbf{W}^e\}\\ &+\sum_{i\in\mathcal{N}_g}(GF_{k,i}+DF_{k,m}GF_{m,i})\cdot(\mathrm{Tr}\{\mathbf{Y}_i\mathbf{W}\}-\mathrm{Tr}\{\mathbf{Y}_i\mathbf{W}^e\})\\ &\le P_{fk}^{max},\ \ k\in\mathcal{L},\ m\in\mathcal{M}\end{aligned} \tag{20f}$$
$$\text{where } \mathbf{W}^e = arg\Big\{$$
$$\min_{\mathbf{W}^e} \sum_{i\in\mathcal{N}_g} c_i(\mathrm{Tr}\{\mathbf{Y}_i\mathbf{W}^e\}+P_{di}) \tag{20g}$$
$$s.t.\quad (V_i^{min})^2 \le \mathrm{Tr}\{\mathbf{M}_i\mathbf{W}^e\} \le (V_i^{max})^2,\ \ i\in\mathcal{N} \tag{20h}$$
$$P_{gi}^{min}-P_{di} \le \mathrm{Tr}\{\mathbf{Y}_i\mathbf{W}^e\} \le P_{gi}^{max}-P_{di},\ \ i\in\mathcal{N} \tag{20i}$$
$$Q_{gi}^{min}-Q_{di} \le \mathrm{Tr}\{\bar{\mathbf{Y}}_i\mathbf{W}^e\} \le Q_{gi}^{max}-Q_{di},\ i\in\mathcal{N} \tag{20j}$$
$$-P_{fk}^{max} \le \mathrm{Tr}\{\mathbf{Z}_k\mathbf{W}^e\} \le P_{fk}^{max},\ \ k\in\mathcal{L}\Big\} \tag{20k}$$

The parameter matrices $\mathbf{M}_i$, $\mathbf{Y}_i$, $\bar{\mathbf{Y}}_i$, $\mathbf{Z}_k$ in (20) are derived from the nodal admittance matrix $\mathbf{Y}$, series admittance y_{ij} of line $k, k=\{i,j\}$, and shunt element value $\bar{y}_{ij}$ at bus i associated with the line k. Let $\widetilde{\mathbf{Y}}_i = \mathbf{e}_i\mathbf{e}_i^T\mathbf{Y},\ \ i\in\mathcal{N}$, and $\widetilde{\mathbf{Z}}_k = (\bar{y}_{ij}+y_{ij})\mathbf{e}_i\mathbf{e}_i^T - y_{ij}\mathbf{e}_i\mathbf{e}_j^T,\ \ k=\{i,j\}$, $\mathbf{e}_i$ is a unit vector with 1 at the ith position and zeros elsewhere, then

$$\mathbf{M}_i = \begin{bmatrix}\mathbf{e}_i\mathbf{e}_i^T & 0\\ 0 & \mathbf{e}_i\mathbf{e}_i^T\end{bmatrix}$$
$$\mathbf{Y}_i = \frac{1}{2}\begin{bmatrix}\mathrm{Re}\{\widetilde{\mathbf{Y}}_i+\widetilde{\mathbf{Y}}_i^T\} & \mathrm{Im}\{\widetilde{\mathbf{Y}}_i^T-\widetilde{\mathbf{Y}}_i\}\\ \mathrm{Im}\{\widetilde{\mathbf{Y}}_i-\widetilde{\mathbf{Y}}_i^T\} & \mathrm{Re}\{\widetilde{\mathbf{Y}}_i+\widetilde{\mathbf{Y}}_i^T\}\end{bmatrix}$$
$$\bar{\mathbf{Y}}_i = -\frac{1}{2}\begin{bmatrix}\mathrm{Im}\{\widetilde{\mathbf{Y}}_i+\widetilde{\mathbf{Y}}_i^T\} & \mathrm{Re}\{\widetilde{\mathbf{Y}}_i-\widetilde{\mathbf{Y}}_i^T\}\\ \mathrm{Re}\{\widetilde{\mathbf{Y}}_i^T-\widetilde{\mathbf{Y}}_i\} & \mathrm{Im}\{\widetilde{\mathbf{Y}}_i+\widetilde{\mathbf{Y}}_i^T\}\end{bmatrix}$$
$$\mathbf{Z}_k = \frac{1}{2}\begin{bmatrix}\mathrm{Re}\{\widetilde{\mathbf{Z}}_k+\widetilde{\mathbf{Z}}_k^T\} & \mathrm{Im}\{\widetilde{\mathbf{Z}}_k^T-\widetilde{\mathbf{Z}}_k\}\\ \mathrm{Im}\{\widetilde{\mathbf{Z}}_k-\widetilde{\mathbf{Z}}_k^T\} & \mathrm{Re}\{\widetilde{\mathbf{Z}}_k+\widetilde{\mathbf{Z}}_k^T\}\end{bmatrix}$$

The definitions of $P_{gi}^{min}, P_{gi}^{max}, Q_{gi}^{min}, Q_{gi}^{max}$ are extended from $i\in\mathcal{N}_g$ to every $i\in\mathcal{N}$, with $P_{gi}^{min}, P_{gi}^{max}, Q_{gi}^{min}, Q_{gi}^{max}=0$ for $i\in\mathcal{N}\setminus\mathcal{N}_g$. Note that the original voltage magnitude constraint are changed to the square form to derive (20b) and (20h).

Appendix B

The expressions of $\mathbf{\Gamma}^e$, $\mathbf{\Gamma}$ and $\boldsymbol{S}$ in P3 are given as

$$\begin{aligned}\mathbf{\Gamma}^e = {}& \sum_{i\in\mathcal{N}_g} c_i\mathbf{Y}_i + \sum_{k\in\mathcal{L}}(\overline{\mu_k^e}-\underline{\mu_k^e})\mathbf{Z}_k + \sum_{k\in\mathcal{L}}\sum_{m\in\mathcal{M}}(\overline{\upsilon}_{k,m}-\underline{\upsilon}_{k,m})\cdot\Big\{\mathbf{Z}_k\\ &+DF_{k,m}\mathbf{Z}_m-\sum_{i\in\mathcal{N}_g}(GF_{k,i}+DF_{k,m}\cdot GF_{m,i})\mathbf{Y}_i\Big\}\\ &+\sum_{i\in\mathcal{N}}\Big\{(\overline{\kappa_i^e}-\underline{\kappa_i^e})\mathbf{M}_i+(\overline{\lambda_i^e}-\underline{\lambda_i^e})\mathbf{Y}_i+(\overline{\gamma_i^e}-\underline{\gamma_i^e})\bar{\mathbf{Y}}_i\Big\}\end{aligned}$$

$$\boldsymbol{\Gamma}=\sum_{k\in\mathcal{L}}\sum_{m\in\mathcal{M}}\Big\{(\overline{\upsilon}_{k,m}-\underline{\upsilon}_{k,m})\cdot\sum_{i\in\mathcal{N}_g}(GF_{k,i}+DF_{k,m}\cdot GF_{m,i})\mathbf{Y}_i\Big\}$$
$$+\sum_{i\in\mathcal{N}}\Big\{(\overline{\kappa_i}-\underline{\kappa_i})\mathbf{M}_i+(\overline{\lambda_i}-\underline{\lambda_i})\mathbf{Y}_i+(\overline{\gamma_i}-\underline{\gamma_i})\bar{\mathbf{Y}}_i\Big\}$$
$$+\omega\sum_{i\in\mathcal{N}_g}c_i\mathbf{Y}_i+\sum_{k\in\mathcal{L}}(\overline{\mu_k}-\underline{\mu_k})\mathbf{Z}_k$$

$$\boldsymbol{S}=\sum_{i\in\mathcal{N}}\Big\{(\underline{\kappa_i^e}+\underline{\kappa_i})(V_i^{min})^2-(\overline{\kappa_i^e}+\overline{\kappa_i})(V_i^{max})^2+(\underline{\lambda_i^e}+\underline{\lambda_i})P_{gi}^{min}$$
$$-(\overline{\lambda_i^e}+\overline{\lambda_i})P_{gi}^{max}+(\overline{\lambda_i^e}-\underline{\lambda_i^e}+\overline{\lambda_i}-\underline{\lambda_i})P_{di}+(\underline{\gamma_i^e}+\underline{\gamma_i})Q_{gi}^{min}$$
$$-(\overline{\gamma_i^e}+\overline{\gamma_i})Q_{gi}^{max}+(\overline{\gamma_i^e}-\underline{\gamma_i^e}+\overline{\gamma_i}-\underline{\gamma_i})Q_{di}\Big\}-\sum_{k\in\mathcal{L}}\Big\{(\underline{\mu_k^e}+\overline{\mu}_k^e$$
$$+\underline{\mu}_k+\overline{\mu}_k)P_{fk}^{max}\Big\}-\sum_{k\in\mathcal{L}}\sum_{m\in\mathcal{M}}\Big\{(\underline{\upsilon}_{k,m}+\overline{\upsilon}_{k,m})P_{fk}^{max}\Big\}$$
$$-\sum_{i\in\mathcal{N}_g}c_i\,\mathrm{Tr}\{\mathbf{Y}_i\mathbf{W}^e\}-\omega\sum_{i\in\mathcal{N}_g}c_i\,\mathrm{Tr}\{\mathbf{Y}_i\mathbf{W}\}.$$

REFERENCES

[1] *U.S. Canada Power System Outage Task Force, Final Report on the August 14, 2003 Blackout in the United State and Canada: Causes and Recommendations*, 2006. [Online]. Available: https://www.energy.gov/

[2] Y. Wang, L. Huang, M. Shahidehpour, L. L. Lai, H. Yuan, and F. Y. Xu, "Resilience-constrained hourly unit commitment in electricity grids," *IEEE Transactions on Power Systems*, vol. 33, no. 5, pp. 5604–5614, Sep. 2018.

[3] X. Zhang, Y. Liu, H. Gao, L. Wang, and J. Liu, "Bi-level corrective line switching model for urban power grid congestion mitigation," *IEEE Transactions on Power Systems*, pp. 1–11, 2019.

[4] Y. Wang, L. Huang, M. Shahidehpour, L. L. Lai, and Y. Zhou, "Impact of cascading and common-cause outages on resilience-constrained optimal economic operation of power systems," *IEEE Transactions on Smart Grid*, vol. 11, no. 1, pp. 590–601, 2020.

[5] C. Liu, M. Zhou, J. Wu, C. Long, and D. Kundur, "Financially motivated fdi on sced in real-time electricity markets: Attacks and mitigation," *IEEE Transactions on Smart Grid*, vol. 10, no. 2, pp. 1949–1959, 2019.

[6] A. A. Jahromi, A. Kemmeugne, D. Kundur, and A. Haddadi, "Cyber-physical attacks targeting communication-assisted protection schemes," *IEEE Transactions on Power Systems*, vol. 35, no. 1, pp. 440–450, 2020.

[7] R. M. Lee, M. J. Assante, and T. Conway, "Analysis of the cyber attack on the ukrainian power grid," https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf, Mar. 2016.

[8] J. Yan, Y. Zhu, H. He, and Y. Sun, "Multi-contingency cascading analysis of smart grid based on self-organizing map," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 4, pp. 646–656, April 2013.

[9] J. Yan, H. He, and Y. Sun, "Integrated security analysis on cascading failure in complex networks," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 3, pp. 451–463, March 2014.

[10] Y. Zhu, J. Yan, Y. Tang, Y. L. Sun, and H. He, "Resilience analysis of power grids under the sequential attack," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 12, pp. 2340–2354, 2014.

[11] L. Che, X. Liu, Z. Li, and Y. Wen, "False data injection attacks induced sequential outages in power systems," *IEEE Transactions on Power Systems*, vol. 34, no. 2, pp. 1513–1523, March 2019.

[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, June 2011.

[13] ——, "Quantitative analysis of load redistribution attacks in power systems," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 9, pp. 1731–1738, Sep. 2012.

[14] Y. Xiang, L. Wang, and N. Liu, "Coordinated attacks on electric power systems in a cyber-physical environment," *Electric Power Systems Research*, vol. 149, pp. 156–168, 2017.

[15] 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.

[16] 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, pp. 2016–2025, 2016.

[17] 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, 2016.

[18] ——, "Analyzing locally coordinated cyber-physical attacks for undetectable line outages," *IEEE Transactions on Smart Grid*, vol. 9, no. 1, pp. 35–47, 2018.

[19] H. Chung, W. Li, C. Yuen, W. Chung, Y. Zhang, and C. 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, 2019.

[20] Z. Chu, J. Zhang, O. Kosut, and L. Sankar, "N-1 reliability makes it difficult for false data injection attacks to cause physical consequences," *IEEE Transactions on Power Systems*, vol. 36, no. 5, pp. 3897–3906, 2021.

[21] A. J. Wood, B. F. Wollenberg, and G. B. Sheblé, *Power generation, operation, and control*. New York, NY, USA: Wiley, 1996.

[22] R. D. Zimmerman, C. E. Murillo-Sánchez, and R. J. Thomas, "Matpower: Steady-state operations, planning, and analysis tools for power systems research and education," *IEEE Transactions on Power Systems*, vol. 26, no. 1, pp. 12–19, Feb 2011.

[23] "Ieee standard for calculating the current-temperature relationship of bare overhead conductors," *IEEE Std 738-2012*, pp. 1–72, 2013.

[24] S. Karimi, P. Musilek, and A. M. Knight, "Dynamic thermal rating of transmission lines: A review," *Renewable and Sustainable Energy Reviews*, vol. 91, pp. 600–612, 2018.

[25] *NERC Reliability Guideline: Methods for Establishing IROLs*. [Online]. Available: https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Reliability_Guideline_Methods_for_Establishing_IROLs.pdf

[26] C. Liu, J. Wu, C. Long, and Y. Wang, "Dynamic state recovery for cyber-physical systems under switching location attacks," *IEEE Transactions on Control of Network Systems*, vol. 4, no. 1, pp. 14–22, 2017.

[27] J. Zhang, Z. Chu, L. Sankar, and O. Kosut, "Can attackers with limited information exploit historical data to mount successful false data injection attacks on power systems?" *IEEE Transactions on Power Systems*, vol. 33, no. 5, pp. 4775–4786, 2018.

[28] T. Huang, B. Satchidanandan, P. R. Kumar, and L. Xie, "An online detection framework for cyber attacks on automatic generation control," *IEEE Transactions on Power Systems*, vol. 33, no. 6, pp. 6816–6827, 2018.

[29] P. Kundur, J. Paserba, V. Ajjarapu, G. Andersson, A. Bose, C. Canizares, N. Hatziargyriou, D. Hill, A. Stankovi, C. Taylor, T. Van Cutsem, and V. Vittal, "Definition and classification of power system stability ieee/cigre joint task force on stability terms and definitions," *IEEE Transactions on Power Systems*, vol. 19, no. 3, pp. 1387–1401, 2004.

[30] J. Chen, J. S. Thorp, and I. Dobson, "Cascading dynamics and mitigation assessment in power system disturbances via a hidden failure model," *International Journal of Electrical Power & Energy Systems*, vol. 27, no. 4, pp. 318 – 326, 2005.

[31] M. ApS, *The MOSEK optimization toolbox for MATLAB manual. Version 9.0.*, 2019. [Online]. Available: http://docs.mosek.com/9.0/toolbox/index.html

[32] J. Lavaei and S. H. Low, "Zero duality gap in optimal power flow problem," *IEEE Transactions on Power Systems*, vol. 27, no. 1, pp. 92–107, 2012.

[33] X. Liu and Z. Li, "Trilevel modeling of cyber attacks on transmission lines," *IEEE Transactions on Smart Grid*, vol. 8, no. 2, pp. 720–729, 2017.

[34] G. P. McCormick, "Computability of global solutions to factorable nonconvex programs: Part i — convex underestimating problems," *Mathematical Programming*, vol. 10, no. 1, pp. 147–175, 1976.

[35] Z. Chu, J. Zhang, O. Kosut, and L. Sankar, "Vulnerability assessment of large-scale power systems to false data injection attacks," in *2020 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, 2020, pp. 1–6.

[36] *NERC Standard PRC-023-1–Transmission Relay Loadability*. [Online]. Available: https://www.nerc.com/files/prc-023-1.pdf

[37] J. Löfberg, "Yalmip : A toolbox for modeling and optimization in matlab," in *In Proceedings of the CACSD Conference*, Taipei, Taiwan, 2004.

[38] R. D. Zimmerman and C. E. M.-S. (2020)., "Matpower (version 7.1) [software]," https://matpower.org.

Min Zhou received the B.Eng. degree in Information Science and Engineering from East China University of Science and Technology, Shanghai, China, in 2015. She is currently pursuing the Ph.D. degree with the School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai, China. Her current research interests include cyber-physical security analysis, robust defense, and dispatch optimization for smart grid.

Chensheng Liu (Member, IEEE) received the Ph.D. degree in Control Science and Engineering from Shanghai Jiao Tong University, Shanghai, China, in 2018.

He was a Postdoctoral Research Fellow with the University of Alberta, Edmonton, AB, Canada, from 2018 to 2019. From 2019 to 2021, he was a Postdoctoral Research Fellow (supported by the Initiative Postdocs Supporting Program) with East China University of Science and Technology, Shanghai, where he is currently a Distinguished Research Fellow with the School of Information Science and Engineering. His research interests include machine learning in smart grid, security of cyber-physical systems, control and optimization of smart grid.

Amir Abiri Jahromi (Senior Member, IEEE) received the Ph.D. degree in Electrical and Computer Engineering from McGill University, Montreal, QC, Canada, in 2016. From January 2018 to December 2019, he was a Postdoctoral Fellow at the University of Toronto. In 2020, he was a Research Associate at the University of Toronto.

Currently, Amir Abiri Jahromi is a Lecturer at the School of Electronic and Electrical Engineering, University of Leeds. His research interests are in the fields of power system modeling, cyber-physical security, reliability, economics and optimization of power systems.

Deepa Kundur (Fellow, IEEE) is Professor & Chair of The Edward S. Rogers Sr. Department of Electrical & Computer Engineering at the University of Toronto. She received the B.A.Sc., M.A.Sc., and Ph.D. degrees all in Electrical and Computer Engineering in 1993, 1995, and 1999, respectively, from the University of Toronto.

Professor Kundur's research interests lie at the interface of cybersecurity, signal processing and complex dynamical networks. She is an author of over 200 journal and conference papers and is a recognized authority on cybersecurity issues. She has served in executive roles at numerous international conferences and has participated on several editorial boards and funding panels.

Professor Kundur's research has received best paper recognitions at numerous venues including the 2015 IEEE Smart Grid Communications Conference, the 2015 IEEE Electrical Power and Energy Conference, the 2012 IEEE Canadian Conference on Electrical & Computer Engineering, the 2011 Cyber Security and Information Intelligence Research Workshop and the 2008 IEEE INFOCOM Workshop on Mission Critical Networks. She has also been the recipient of teaching awards at both the University of Toronto and Texas A&M University. She is a Fellow of the IEEE, a Fellow of the Canadian Academy of Engineering, and a Senior Fellow of Massey College.

Jing Wu (Senior Member, IEEE) received the B.S. degree from Nanchang University, Nanchang, China, in 2000, the M.S. degree from Yanshan University, Hebei, China, in 2002, and the Ph.D. degree from the University of Alberta, Edmonton, AB, Canada, in 2008, all in electrical engineering.

Since 2011, she has been with Shanghai Jiao Tong University, Shanghai, China, and is currently a Professor. She is a registered Professional Engineer in Alberta, Canada. Her current research interests include robust model predictive control, security control, and stability analysis and estimations for cyber-physical systems.

Chengnian Long (Senior Member, IEEE) received the B.S., M.S., and Ph.D. degrees in control theory and engineering from Yanshan University, Hebei, China, in 1999, 2001, and 2004, respectively.

He was a Research Associate with the Department of Computer Science and Engineering, Hong Kong University of Science and Technology, Hong Kong, and a Killam Postdoctoral Fellow with the University of Alberta, Edmonton, AB, Canada. Since 2009, he has been with Shanghai Jiao Tong University, Shanghai, China, where he has been currently a Full Professor since 2011. His current research interests include artificial intelligence of things, blockchain technology, deep learning, and cyber–physical system security.