A Hybrid Cyber Attack Model for Cyber-Physical Power Systems

TU, Haicheng; XIA, Yongxiang; TSE, Chi K.; CHEN, Xi

Published in:
IEEE Access

Published: 01/01/2020

Document Version:
Final Published version, also known as Publisher's PDF, Publisher's Final version or Version of Record

Published version (DOI):
10.1109/ACCESS.2020.3003323

Publication details:
TU, H., XIA, Y., TSE, C. K., & CHEN, X. (2020). A Hybrid Cyber Attack Model for Cyber-Physical Power Systems. *IEEE Access*, *8*, 114876-114883. [9120058]. https://doi.org/10.1109/ACCESS.2020.3003323

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received June 1, 2020, accepted June 15, 2020, date of publication June 18, 2020, date of current version July 1, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3003323

A Hybrid Cyber Attack Model for Cyber-Physical Power Systems

HAICHENG TU[1], YONGXIANG XIA[2], (Senior Member, IEEE), CHI K. TSE[3], (Fellow, IEEE), AND XI CHEN[4], (Senior Member, IEEE)

[1]College of Information Science and Electronic Engineering, Zhejiang University, Hangzhou 310027, China
[2]School of Communication Engineering, Hangzhou Dianzi University, Hangzhou 310018, China
[3]Department of Electrical Engineering, City University of Hong Kong, Hong Kong
[4]GEIRI North America, San Jose, CA 95134, USA

Corresponding author: Yongxiang Xia (xiayx@hdu.edu.cn)

ABSTRACT Over the past decade, the cyber security of power systems has been widely studied. Most previous studies have focused on cyber physical attacks, and barely considered one typical cyber attack: availability attack. We propose a hybrid attack model and apply conventional state estimation processes to study cyber attacks on power grids in this paper. The proposed model considers both integrity attack and availability attack simultaneously. Compared with the particular attack, namely, false data injected attack, we analyze their consequences to power systems in the events of false negatives attack and false alarm attack. The results show that the hybrid attack can confuse the control center by manipulating the integrity and availability of measurements. More importantly, we evaluate the hybrid attack with different values of the cost ratio between integrity and availability attacks, and then verify that the hybrid attack can achieve the same goal with a reduced cost.

INDEX TERMS Cyber-physical power system, cyber security, attack cost, differential evolution algorithm.

I. INTRODUCTION

The advent of information and communication technology has made modern power systems smarter and more efficient through deployment of computer-based control and monitoring. Modern power systems are thus cyber-physical power systems (CPPS). Although the coupling of these two networks brings some convenience, the power system is more vulnerable to intricate cyber environment, which puts the CPPS at the risk of cyber attacks [1], [2]. In general, external attacks on CPPS can be divided into physical attacks, cyber attacks and cyber-physical attacks (also called coordinated attacks).

Physical attacks, such as disrupting power substations and cutting the transmission lines, always cause massive damage to infrastructure. The physical attack is also called a terrorist threat problem and has subsequently been the subject of a lot of research [3]–[5]. Cyber attacks always target the supervisory control and data acquisition (SCADA) system, and perturb the data transmission process or even garble the data. For example, in 2015, the Ukraine blackout, initiated by the planting of a computer malware (called BlackEnergy), caused inconvenience to many people and incurred considerable economic losses [6]. Thus, to ensure that a CPPS operates safely and reliably in cyber environment, according to the basic attributes of information security [7], there are three requirements for the handling of data in CPPS: 1) *Integrity* is to ensure that the data is reliable and authentic; 2) *availability* is to ensure that the data can be delivered safely and in a timely way; and 3) *confidentiality* is to ensure that the contents of the data are not illegally leaked. According to these three requirements, three kinds of cyber attacks can be conducted.

- *Integrity* includes maintaining trustworthiness of data and prevents data from being tampered illegally throughout the process [8]–[10]. From this view, a classic integrity data attack, called *false data injection attack* (FDIA), has become a recent research hotspot. FDIA was initially intended to disrupt state estimation (SE) in the SCADA system. It has been pointed out [11] that the attackers can successfully inject specific data to original measurements, and at the same time pass the Bad Data Detector (BDD). Moreover, the analysis of estimation errors due to FDIA attacks has illustrated

The associate editor coordinating the review of this manuscript and approving it for publication was Zhiyi Li.

that the damages caused by FDIA could be large even when very few measurements have been compromised [12], [13]. FDIA can also perturb the electricity market by affecting power dispatching, resulting in making a huge profit or bringing a bigger burden to power systems [14], [15]. Furthermore, some studies of the physical impact of FDIA have shown that the attackers aim to cause line overloading in the power system [16].

- *Availability* ensures data to be timely accessed by the control center. Availability attacks, also called denial-of-service (DoS) attacks, are attacks that try to block or delay the data delivery in CPPS. Liu *et al.* [17] studied the influences of DoS attacks on load frequency control of smart grids. The delay of these critical messages can also result in catastrophes for power systems. For example, in the case of substation trip protection, if an attacker successfully delays the transmission of a protection message, it will cause serious damage to other power equipment [18]. Thus, the goals of DoS attacks are not only to interrupt resource access, but also to violate the timing requirements of critical messages exchange.
- Compared with the above two requirements, attackers targeting to compromise *confidentiality* have no intention to modify or delay the transmitting data. Instead, they eavesdrop on communication channels to get the information they need, such as a customer's account or electricity consumption. Typical methods include wiretappers [19] and traffic analyzers [20].

In reality, the attackers may combine physical and cyber attacks to realize coordinated attacks. Li *et al.* formulated the coordinated attacks as a bilevel model [21], and extended this idea with incomplete network information [22]. Deng *et al.* proposed replay and optimized coordinated attacks [23]. In these works, coordinate attacks considering physical lines disconnection and false data were considered to evaluate the attack influences. Also, load frequency control was studied by a coordinated attack model in [24]. In response to the huge threat of cyber-physical attacks, many researchers have proposed corresponding countermeasures [25], [26].

However, the above coordinated attacks do not consider the availability attacks. In fact, the availability attacks seriously threaten the operation of CPPS. The main reason is that SCADA systems are always more vulnerable to availability attacks, and attackers may prefer to perform availability attacks with limited resource. In order to further enrich the diversity of cyber attacks, the attacker will consider not only the cooperation between the cyber attack and the physical attack but also the cooperation between the availability attack and the integrity attack. Inspired by the above ideas, as shown in Fig. 1, the hybrid attack model considers both integrity and availability attacks. Furthermore, compared with FDIA, the consequences of the hybrid attack on CPPS are analyzed in terms of the attack cost. The key contributions of this paper are as follows. First, the model of hybrid cyber attack is proposed. Unlike previous studies where only one

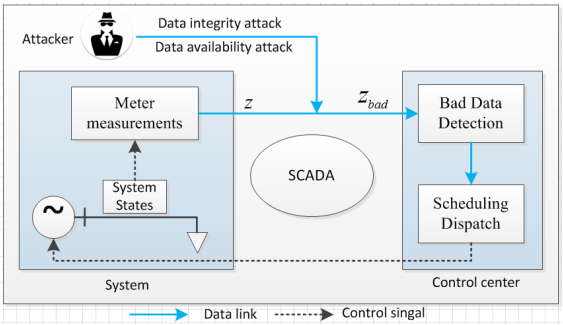


FIGURE 1. The schematic diagram of the hybrid cyber attack.

kind of attack is considered, the hybrid attack model considers both integrity and availability attacks simultaneously. The model thus extends the application of cyber attacks significantly, and promotes the analysis of different attack situations under a unified model rather than multiple cyber attack models. Then, based on the proposed model, we examine the consequences of hybrid attack in two common scenarios. By injecting a valid attack vector, attackers can mislead the control center and develop a serious threat or damage to power system operations. Finally, a metric is proposed to quantify the cost of attacks, and found that the proposed attack model can do the same harm to the power system with less resource.

The rest of this paper is as follows. Section II gives the model of cyber attacks, including the mechanism of SE, BDD, FDIA, availability attack, and the hybrid attack model. In Section III, a simple and efficient heuristic *differential evolution* algorithm is used to find all parameters of the attack model. Then, the consequences of hybrid attack under two scenarios and the attack cost are studied in Section VI. Finally, Section V concludes the paper.

II. THE MODEL DESCRIPTION

In this section, the mechanisms of state estimation and bad data detection are introduced firstly. Then the mathematical model of attack models is given, including the FDIA model, the availability attack model and the hybrid attack model.

A. STATE ESTIMATION

According to a series of meter measurements, the SE process estimates the state variables, such as the voltage on each bus or power flow on each line. Such estimated variables are those parameters that show the running conditions of the power system in a period of time [27]. In this paper, we consider a power system with n buses and m transmission lines. Each transmission line is equipped with a meter to measure its power flow. The SE problem is to estimate the state variable $\mathbf{x} = (x_1, x_2, \ldots, x_n)^T$ based on the meter measurements $\mathbf{z} = (z_1, z_2, \ldots, z_m)^T$, under the measurement noise $\mathbf{n} = (n_1, n_2, \ldots, n_m)^T$ which follows the Gaussian distribution $N(\mathbf{0}, \sigma^2)$. Thus, the linear state estimation is based on the

following approximation model [11].

$$\mathbf{z} = \mathbf{H}\mathbf{x} + \mathbf{n}, \tag{1}$$

where $\mathbf{H}$ is the Jacobian matrix. Then, the estimated system state $\bar{\mathbf{x}}$ is given by

$$\bar{\mathbf{x}} = (\mathbf{H}^T\mathbf{W}\mathbf{H})^{-1}\mathbf{H}^T\mathbf{W}\mathbf{z}. \tag{2}$$

where $\mathbf{W} = diag\{\sigma_1^{-2}, \sigma_2^{-2}, \ldots, \sigma_m^{-2}\}$.

B. BAD DATA DETECTION

Bad data detection (BDD) can detect measurement errors and prevent bad data from passing through the whole system. To achieve this in the DC power model, when $\mathbf{W} = \mathbf{I}$, the error between estimations and measurements should satisfy

$$\frac{1}{2}\|\mathbf{z} - \mathbf{H}\bar{\mathbf{x}}\|^2 < \tau, \tag{3}$$

where τ is a pre-determined significance level.

In order to make the symbol in the rest of this paper simple, the *largest normalized residual* (LNR) is used to denote the error residual, i.e., $\text{LNR} = \|\mathbf{z} - \mathbf{H}\bar{\mathbf{x}}\|$.

C. FALSE DATA INJECTION ATTACK MODEL

In the false data injection attack (FDIA) model, attackers can enable bad data to evade detection by injecting a set of altered measurement data with the satisfaction of eq. (3). With this in mind, attackers should carefully design the attack strategy to deceive the BDD to avoid being detected. A non-zero vector $\triangle\mathbf{z}$ is defined as an attack vector that is injected into the original measurement data $\mathbf{z}$. Thus, the new LNR value can be represented as

$$LNR_{bad} = \|\mathbf{z} - \mathbf{H}\bar{\mathbf{x}} + (\triangle\mathbf{z} - \mathbf{H}\triangle\mathbf{x})\|. \tag{4}$$

If the FDIA vector follows $\triangle\mathbf{z} = \mathbf{H}\triangle\mathbf{x}$, attackers can keep the LNR unchanged by injecting bad data into meter measurements.

Theoretically, if attackers can fully acquire the information of the whole system configuration (i.e., the topology of grid, running states, mechanism of state estimation algorithm and bad data detection method, etc.) and has the ability to manipulate all meter measurements, it can be conceptually capable of launching a valid attack strategy by injecting a conditional vector. Thus, the mathematical model of FDIA can represent as following [11]

$$\min \ \|\triangle\mathbf{z}\|_0 \tag{5}$$
$$s.t.\ \mathbf{z}_{bad} = \mathbf{z} + \triangle\mathbf{z} \tag{6}$$
$$\triangle\mathbf{z} = \mathbf{H}\triangle\mathbf{x} \tag{7}$$
$$\triangle\mathbf{z} \neq \mathbf{0} \tag{8}$$
$$(\mathbf{z}_{bad} - \mathbf{H}\mathbf{x})^T\mathbf{W}(\mathbf{z}_{bad} - \mathbf{H}\mathbf{x}) < \tau \tag{9}$$

Here, the goal is design an attack strategy with the lowest cost. In other words, the number of non-zeros in $\triangle\mathbf{z}$ is as small as possible, indicating the fewest meters has been manipulated. Constraint (6) shows that the vector of received measurement is changed as $\mathbf{z}_{bad}$ by injecting the attack vector $\triangle\mathbf{z}$. Constraint (7) guarantees that malicious data will not be detected by BDD. Constraint (8) guarantees that the injected vector is non-zero. Finally, constraint (9) means that the estimated error on manipulated measurements should be within the preset thresholds.

D. AVAILABILITY ATTACK MODEL

For a large SCADA system, missing data and failing remote terminal units are common [29]. When certain measurements are missing, a traditional solution in SCADA is to use the rest of data or predictive data before the system becomes ''unobservable''. In this paper, it is assume that the SE uses the rest of data to estimate the state of power system when the availability attacks happen. The availability attack vector is denoted as $\mathbf{d} \in \{0, 1\}^m$ in which $\mathbf{d}(i) = 1$ corresponds to measurement i being unavailable. Similar to FDIA, the model for the rest of measurements and the variable of system states can be represented as

$$\mathbf{z}_d = \mathbf{H}_d\mathbf{x} + \mathbf{n}_d, \tag{10}$$

where $\mathbf{z}_d$ and $\mathbf{n}_d$ are measurement vector and noise vector, respectively. If measurement i is unavailable, the values of corresponding component i are zeros. Similarly, matrix $\mathbf{H}_d \in \mathbb{R}^{m\times n}$ denotes the attribute of the rest of measurements. Due to the availability attack on some measurements, $\mathbf{H}_d$ can obtain from $\mathbf{H}$ by replacing corresponding rows with zeros, i.e., $\mathbf{H}_d := (\mathbf{I} - diag(\mathbf{d}))\mathbf{H}$.

E. HYBRID ATTACK MODEL

As mentioned above, there are two main kinds of cyber attacks, namely, integrity attack and availability attack. Previous studies have rarely considered these two kinds of cyber attacks simultaneously. However, the rapid development of CPPS has posed security threats from both of these two attack methods, which can be launched individually or cooperatively. Here, the proposed hybrid model considers both integrity and availability attacks. The goal of the hybrid attack is to modify some measurements and to make some of other sets of measurements unavailable to SE so that the received bad data can pass through BDD.

Similar to FDIA, if the attack vector satisfies $\triangle\mathbf{z} = \mathbf{H_d}\triangle\mathbf{x}$, the hybrid attack can also be launched with stealth. The minimum number of measurements that need to be modified or blocked by attackers is adopted as objective of the hybrid attack as, i.e.,

$$\min \ \|\triangle\mathbf{z}\|_0 + \|\mathbf{d}\|_0 \tag{11}$$
$$s.t.\ \mathbf{z}_{bad} = \mathbf{z_d} + \triangle\mathbf{z_d} \tag{12}$$
$$\triangle\mathbf{z_d} = \mathbf{H_d}\triangle\mathbf{x_d} \tag{13}$$
$$\mathbf{H_d} = (\mathbf{I} - \mathbf{diag}(\mathbf{d}))\mathbf{H} \tag{14}$$
$$\triangle\mathbf{z} \neq \mathbf{0} \tag{15}$$
$$(\mathbf{z}_{bad} - \mathbf{H_d}\mathbf{x_d})^T\mathbf{W}(\mathbf{z}_{bad} - \mathbf{H_d}\mathbf{x_d}) < \tau \tag{16}$$

This hybrid attack model can be considered as being based on the FDIA model with the availability attack incorporated at the same time.

III. SOLUTION ALGORITHM

Intelligent algorithms are usually used to solve the non-convex optimization problems. In this paper, the differential evolution (DE) [30] is adopted to find the solution of the hybrid attack model. In the population of NP m-dimensional vectors, i.e., $\mathbf{X}_{i,t} = \{x_{i,t}^1, \ldots, x_{i,t}^m\}$, $i = 1, \ldots, NP$, the DE algorithm can achieve the optimal solution through the mutation, crossover and selection operation. The detailed algorithm steps are described below.

A. INITIALIZATION

In order to make the initial population cover all possible solutions as much as possible, each value of individual should be within the range of the given minimum and maximum parameter bounds $\mathbf{X}_{\min} = \{x_{\min}^1, \ldots, x_{\min}^m\}$ and $\mathbf{X}_{\max} = \{x_{\max}^1, \ldots, x_{\max}^m\}$. For example, the initial value of the jth parameter in the ith individual at generation $t = 0$ is generated by

$$x_{i,0}^j = x_{\min}^j + rand(0, 1) \cdot (x_{\max}^j - x_{\min}^j), \tag{17}$$

where $j = 1, 2 \ldots, m$ and rand(0,1) represents a uniformly distributed random variable within the range [0, 1].

B. MUTATION OPERATION

After the population is initialized, for each individual $\mathbf{X}_{i,t}$, also called the target vector, DE randomly selects the other three individuals to generate the mutation vector $\mathbf{Y}_{i,t} = \{y_{i,t}^1, y_{i,t}^2, \ldots, y_{i,t}^m\}$ by the mutation strategy, i.e.,

$$\mathbf{Y}_{i,t} = \mathbf{X}_{r_1^i,t} + F \cdot (\mathbf{X}_{r_2^i,t} - \mathbf{X}_{r_3^i,t}). \tag{18}$$

The indicators r_1^i, r_2^i and r_3^i are three integers randomly generated within the interval [1, NP], which are also different from index i. These indicators are randomly generated once for each mutant vector. The scaling factor F is a positive control parameter for scaling the difference vector.

C. CROSSOVER OPERATION

After the mutation, each pair of the target vector $\mathbf{X}_{i,t}$ and its corresponding mutant vector $\mathbf{Y}_{i,t}$ is cross-processed to generate a trial vector: $\mathbf{U}_{i,t} = \{u_{i,t}^1, u_{i,t}^2, \ldots, u_{i,t}^m\}$. In the basic version, DE employs a uniform crossover defined by

$$u_{i,t}^j = \begin{cases} y_{i,t}^j, & \text{if } rand_j[0, 1) \le C_r \text{ or } j = j_{rand} \\ x_{i,t}^j, & \text{otherwise} \end{cases} \tag{19}$$

In the above equation, the crossover rate C_r is a user-specified constant that controls the proportion of parameter values copied from the mutation vector in the range [0, 1). j_{rand} is an integer randomly selected within the range $[1, m]$. if $rand_j[0, 1) \le C_r$ or $j = j_{rand}$, the binomial crossover operator copies the jth parameter of the mutant vector to the corresponding element in the trial vector $\mathbf{U}_{i,t}$. Otherwise, it will be copied from the corresponding target vector $\mathbf{X}_{i,t}$.

D. SELECTION OPERATION

If a value exceeds its bound in the newly generated trial individual resulting from the mutation and crossover operations, a new trial individual needs to be re-generated until all the values are within the upper and lower bounds. The algorithm then calculates the objective function values of all the trial individual and its corresponding target individual, i.e., $\mathbf{O}(\mathbf{U}_{i,t})$ and $\mathbf{O}(\mathbf{X}_{i,t})$, in the current population. If the objective function value of the trial individual is greater than the corresponding target individual, the target individual will retain to the next generation population. Otherwise, the trail individual will replace the corresponding target individual and enter the operation of the next generation population. Thus, the selection operation can be expressed as

$$\mathbf{X}_{i,t+1} = \begin{cases} \mathbf{U}_{i,t}, & \text{if } \mathbf{O}(\mathbf{U}_{i,t}) \le \mathbf{O}(\mathbf{X}_{i,t}) \\ \mathbf{X}_{i,t}, & \text{otherwise} \end{cases} \tag{20}$$

The above 3 steps (from step B to step D) are iterated generation after generation until the objective value is unchanged or the total number of generations reaches a preset number.

IV. SIMULATION RESULTS AND DISCUSSIONS

In this section, we study how the hybrid attack affects the modified IEEE tested systems [31]. In a power system, each transmission line is equipped with a meter to measure its real power flow. The SE problem estimates the variable $\overline{\mathbf{x}} = [\overline{\theta}, \overline{V}]$ with $\overline{\theta}$ and $\overline{V}$ representing the phase angle and voltage magnitude of bus. In order to compare with the FDIA model in [11], the threshold $\tau = 70.993$ used in [11] is also adopted in this paper. The maximum power allowed through the transmission lines is set as 2 p.u.. It is worth noting that once the transmission capacities are fixed, the appropriate attack vector can always be found to meet the specific attack scenario. The different setting of the maximum power of transmission lines only affects which lines are overloaded, but the qualitative results drawn in this paper do not change. All simulations are implemented on MATLAB using MatPower [32]. Table 1 gives the DE parameter setting for simulations.

TABLE 1. Differential evolution parameter setting.

Population size NP	100
Number of iterations	5000
F	0.9
C_r	0.1

In this paper, the target of attackers is to confuse the control center. In the static security assessment (SSA) module, if the power flow of a transmission line exceeds its corresponding capacity, the SSA will immediately show an insecure signal. The system dispatcher will take corresponding emergency protection operation, such as generator rescheduling or load shedding. If there are no overloaded lines, the SSA will show a secure situation. In this case, the system dispatcher does

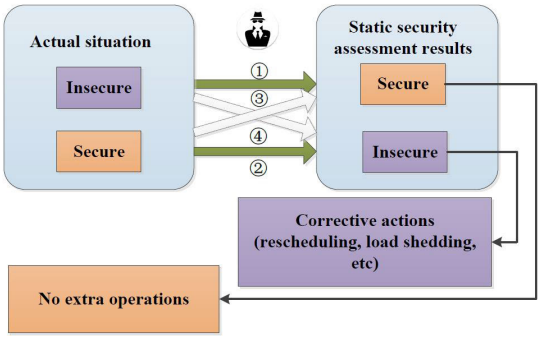


FIGURE 2. Overview of the objectives of cyber attack in CPPS.

not need to take any protection. Since there are two possible actual running states and two possible assessment results, there are totally four scenarios for SSA when applying the hybrid attack to SE, as shown in Fig. 2:

1) The SSA reports a secure situation, while the actual situation is insecure;
2) The SSA reports an insecure situation, while the actual situation is secure;
3) The SSA reports an insecure situation, while the actual situation is insecure;
4) The SSA reports a secure situation, while the actual situation is secure;

Obviously, scenarios 3 and 4 are the correct ones we want. However, if an attack takes place, the scenario 1 or 2 may happen. They are called false negatives attack (FNA) and false alarm attack (FAA), respectively. Specific scenarios are described as follows.

A. FALSE NEGATIVES ATTACK

We assume that an open circuit fault takes place as an initial disruption and causes an overload situation. Under this condition, the SSA should report an insecure signal. However, if a valid attack vector is injected at this time, it is possible that BDD will not detect the measurement modified, and SSA will show a secure signal based on false data. As a result, the system will not take any necessary action, which may lead to widespread power outage. The mathematical model of this scenario is

$$\min \ \|\triangle \mathbf{z}\|_0 + \|\mathbf{d}\|_0 \tag{21}$$

$$s.t. \ constraints \quad (12)-(16) \tag{22}$$

$$P_{ij} = V_i^2 G_{ij} - V_i V_j (G_{ij}\cos\theta_{ij} + B_{ij}\sin\theta_{ij}) \tag{23}$$

$$P_i = V_i \sum_{j=1}^{n} V_j (G_{ij}\cos\theta_{ij} + B_{ij}\sin\theta_{ij}) \tag{24}$$

$$P_{ij\min} \le P_{ij} \le P_{ij\max} \tag{25}$$

$$P_{i\min} \le P_i \le P_{i\max} \tag{26}$$

where constraints (23) and (24) are the network equations with P_{ij} and P_i representing the power flows on transmission line (i, j) and bus i, respectively; θ_i and θ_j are the phase angles on nodes i and j; $\theta_{ij} = \theta_i - \theta_j$. V_i and V_j are voltage magnitudes on nodes i and j; G_{ij} and B_{ij} are the real and imaginary parts of admittance matrix on line (i, j). Constraints (25) and (26) give the upper and lower bounds of transmission lines and buses, respectively.

The situation results for IEEE 39-bus and IEEE 57-bus systems are shown in Figs. 3 and 4, respectively. Taking IEEE 39-bus for example, we assume that the initial open circuit fault takes place at the 30th transmission line. Due to the fault, the power flow will be redistributed, causing the actual power flows on transmission lines 3 and 25 overloaded, shown as red bars in Fig. 3. When the system is not being attacked, the system has the same power distribution due to an initial open circuit fault (causing the certain transmission lines overloaded), and the SSA will immediately inform the power dispatcher of this insecure situation and take corresponding emergency action timely. However, by applying the integrity attack (FDIA in Fig. 3(a) or hybrid attack in Fig. 3(b)) to the measurements, the overloading situation can be manipulated to be within the bounds, shown as green bars in Fig. 3. It looks like that no line is overloaded anymore. Consequently, the control center will not detect the overloading. The same qualitative results can also be found in IEEE 57-bus, as shown in Fig. 4.

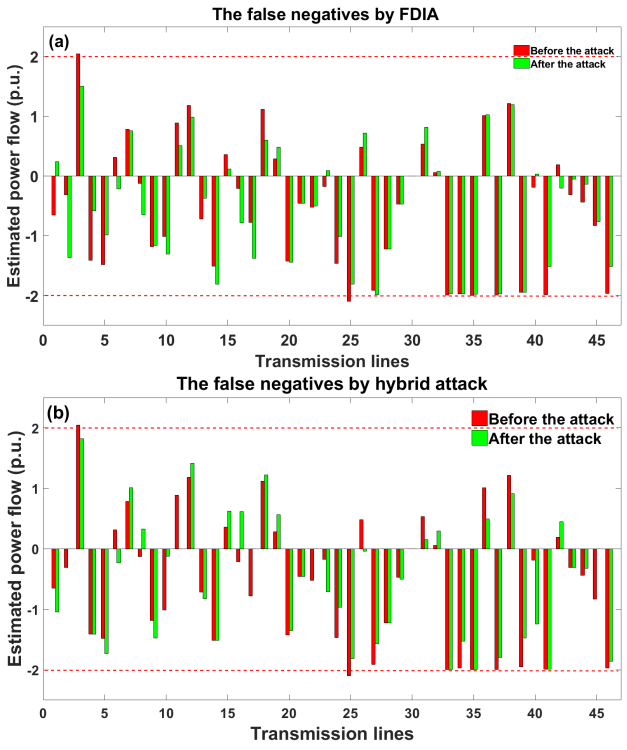


FIGURE 3. False negatives attack on IEEE 39 bus. Results with and without (a) FDIA attack and (b) hybrid attack. Red bars and green bars represent the power flows of transmission lines before and after the attack, respectively. Dotted lines show upper and lower bounds.

B. FALSE ALARM ATTACK

For false alarm attack, the normal situation is maliciously reported as a transmission line overload case. Attackers inject an appropriate fake data that deceives BDD and confuses

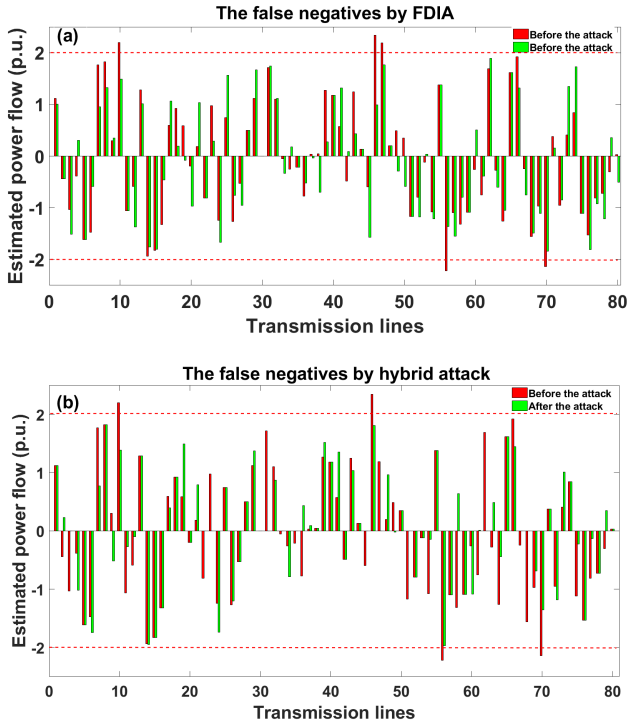


FIGURE 4. False negatives attack on IEEE 57 bus. Results with and without (a) FDIA attack and (b) hybrid attack. Red bars and green bars represent the power flows of transmission lines before and after the attack, respectively. Dotted lines show upper and lower bounds.

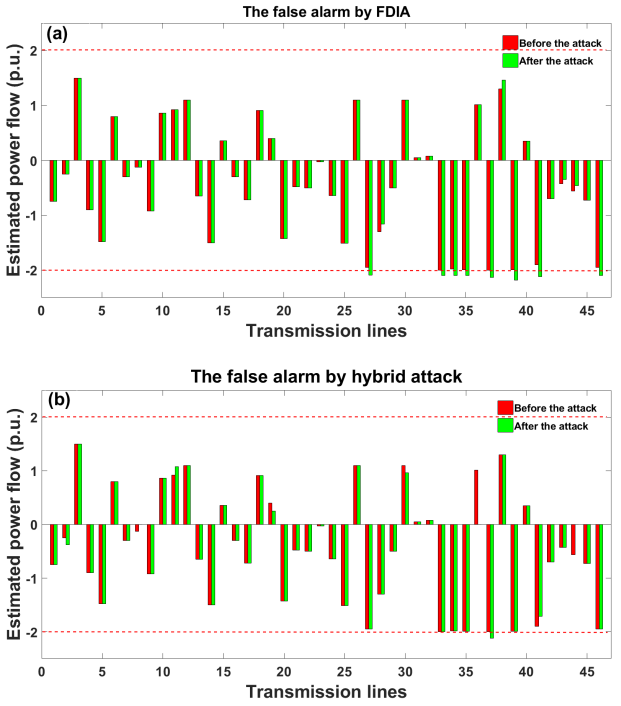


FIGURE 5. Fake alarm attack on IEEE 39 bus. Results with and without (a) FDIA attack and (b) hybrid attack. Red bars and green bars represent the power flows of transmission lines before and after the attack, respectively. Dotted lines are their upper and lower bounds.

SSA that there is an overloading. The mathematical model is formulated as

$$\min \ \|\triangle \mathbf{z}\|_0 + \|\mathbf{d}\|_0 \tag{27}$$

$$s.t.\ constraints \quad (12)-(16) \tag{28}$$

$$P_{ij} = V_i^2 G_{ij} - V_i V_j (G_{ij}\cos\theta_{ij} + B_{ij}\sin\theta_{ij}) \tag{29}$$

$$P_i = V_i \sum_{j=1}^{n} V_j (G_{ij}\cos\theta_{ij} + B_{ij}\sin\theta_{ij}) \tag{30}$$

$$\exists P_{ij} > P_{ij\max} \tag{31}$$

where constraint (31) indicates that the SSA mistakenly concludes based on the modified measurement data that there is overloading on at least one transmission line.

As for simulation, as shown as in Figs. 5 and 6, we study how FAA affects the power system in both IEEE 39-bus and IEEE 57-bus systems. We take IEEE 39-bus for example, the red bars in Fig. 5 represent as the estimated power flow measurements of transmission lines before the attack. Then, by launching the cyber attack (FDIA in Fig. 5(a) or hybrid attack in Fig. 5(b)) to the measurements, attackers create fake overloading situations, shown as the green bars in Fig. 5. We can find that the SSA will show an insecure situation, even if there is no transmission line actually overloaded.

Upon receiving the insecure signal sent by SSA, the control center will act unnecessarily, such as rescheduling and performing load shedding. Such actions incur extra cost and do not make meaningful contributions.

C. COST OF CYBER ATTACKS

In this section, the costs of integrity and availability attacks are introduced into the above models. Suppose C_I and C_A are the costs of the integrity and availability attacks required to manipulate one measurement, respectively. Then, the total cost of hybrid attack is

$$Cost' = C_I \|\triangle \mathbf{z}\|_0 + C_A \|\triangle \mathbf{d}\|_0. \tag{32}$$

In order to compare the costs of integrity and availability attacks, we use a normalization method to quantify the relative sizes of C_I and C_A.

$$Cost = \|\triangle \mathbf{z}\|_0 + \lambda \|\triangle \mathbf{d}\|_0, \tag{33}$$

where λ is the cost ratio between the availability attack and integrity attack, namely, $\lambda = C_A/C_I$. Thus, with the consideration of cost, the objective function of hybrid attack becomes

$$\min \ \|\triangle \mathbf{z}\|_0 + \lambda \|\mathbf{d}\|_0. \tag{34}$$

It is worth noting that the cost of the hybrid attack is related not only to the number of manipulated meters, but also to the cost of each meter. Taking Table 2 as an example, $\lambda = 1$ indicates that the cost of the integrity and availability attacks are the same. It can be seen that the hybrid attack requires less manipulated meters to achieve the same attack purpose than FDIA does under different attack scenarios.

Finally, we study how the optimal cost changes as a function of λ in a power system. From Fig. 7, whatever the case is, the cost of the hybrid attack increases with an increase

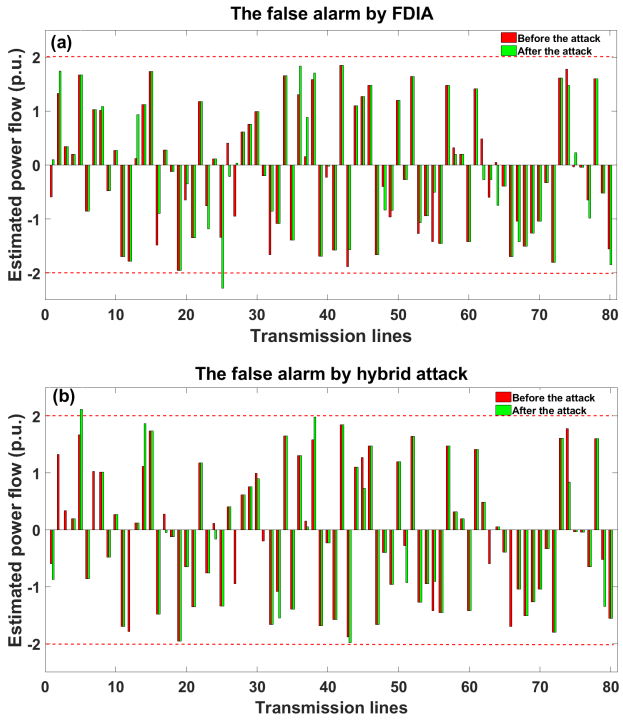


FIGURE 6. Fake alarm attack on IEEE 57 bus. Results with and without (a) FDIA attack and (b) hybrid attack. Red bars and green bars represent the power flows of transmission lines before and after the attack, respectively. Dotted lines are their upper and lower bounds.

TABLE 2. Compromised measurements of FDIA and the hybrid attack when $\lambda = 1$ under two specific scenarios in two IEEE benchmark system.

Network	Attack scenario	Attack method	$\|\triangle \mathbf{z}\|_0$	$\|\mathbf{d}\|_0$	Cost
IEEE 39-bus	FNA	FDIA	40	0	40
		Hybrid	32	5	37
	FAA	FDIA	11	0	11
		Hybrid	6	3	9
IEEE 57-bus	FNA	FDIA	65	0	65
		Hybrid	40	12	52
	FAA	FDIA	29	0	29
		Hybrid	13	8	21

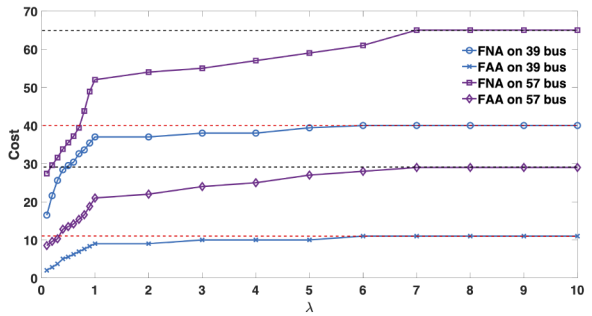


FIGURE 7. Optimal attack cost versus the cost ratio λ under hybrid attack. Dotted lines are the cost of FDIA under corresponding attack situations.

of λ. However, when λ is large enough, the cost becomes constant. This trend can be explained as following. When λ is small, availability attack takes a relatively smaller share of the total cost. Therefore, the availability attack will be the main approach in the hybrid attack framework, and the total cost is lower than that of FDIA. However, as λ increases, the cost of availability attack begins to dominating. Thus, a hybrid attack tends to use less availability attack to save cost. When λ is large enough, the most efficient way to conduct hybrid attack is thus to utilize FDIA solely. As a result, the cost of the hybrid attack will be the same as that of FDIA. It is worth mentioning that, no matter what value λ is, the cost of hybrid attacks is always lower than or equal to that of FDIA. In other words, from the perspective of attackers, the attackers can achieve the same goal with less cost.

V. CONCLUSION

In this paper, we constructed a hybrid cyber attack model, which combines integrity attack and availability attack. Deploying hybrid attack can effectively avoid being detected by the control center, and hence cause confusion that incurs potential damages to the system. We analyze two serious attack scenarios, namely, false negative attack (FNA) and fake alarm attack (FAA). The proposed model effectively captures the enhanced effectiveness and reduced cost of the hybrid attack, providing an effective tool to study more intricate cyber-physical power systems, and to evaluate different attack strategies with limited sources. In addition, the model also reveals the design requirements for more effective detection mechanisms and resource allocation schemes for future cyber-physical power systems.

REFERENCES

[1] S. Li, K. Xue, Q. Yang, and P. Hong, "PPMA: Privacy-preserving multi-subset data aggregation in smart grid," *IEEE Trans. Ind. Informat.*, vol. 14, no. 2, pp. 462–471, Feb. 2018.

[2] H. Tu, Y. Xia, J. Wu, and X. Zhou, "Robustness assessment of cyber-physical systems with weak interdependency," *Phys. A, Stat. Mech. Appl.*, vol. 522, pp. 9–17, May 2019.

[3] J. M. Arroyo and F. D. Galiana, "On the solution of the bilevel programming formulation of the terrorist threat problem," *IEEE Trans. Power Syst.*, vol. 20, no. 2, pp. 789–797, May 2005.

[4] N. Romero, N. Xu, L. K. Nozick, I. Dobson, and D. Jones, "Investment planning for electric power systems under terrorist threat," *IEEE Trans. Power Syst.*, vol. 27, no. 1, pp. 108–116, Feb. 2012.

[5] E. I. Bilis, W. Kroger, and C. Nan, "Performance of electric power systems under physical malicious attacks," *IEEE Syst. J.*, vol. 7, no. 4, pp. 854–865, Dec. 2013.

[6] J. Kollmer, R. Irwin, and S. Biswas, "Analysis of the cyber attack on the Ukrainian power grid," Electr. Inf. Sharing Anal. Center Rep., 2016.

[7] D. Ding, Z. Wang, Q.-L. Han, and G. Wei, "Security control for discrete-time stochastic nonlinear systems subject to deception attacks," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 48, no. 5, pp. 779–789, May 2018.

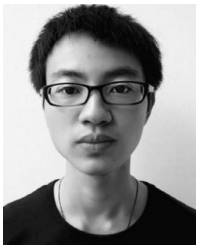
[8] L. Che, X. Liu, Z. Shuai, Z. Li, and Y. Wen, "Cyber cascades screening considering the impacts of false data injection attacks," *IEEE Trans. Power Syst.*, vol. 33, no. 6, pp. 6545–6556, Nov. 2018.

[9] Y. Fan, J. Li, and D. Zhang, "A method for identifying critical elements of a cyber-physical system under data attack," *IEEE Access*, vol. 6, pp. 16972–16984, 2018.

[10] O. A. Beg, T. T. Johnson, and A. Davoudi, "Detection of false-data injection attacks in cyber-physical DC microgrids," *IEEE Trans. Ind. Informat.*, vol. 13, no. 5, pp. 2693–2703, Oct. 2017.

[11] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inf. Syst. Secur.*, vol. 14, no. 1, p. 13, 2011.

[12] Q. Yang, J. Yang, W. Yu, D. An, N. Zhang, and W. Zhao, "On false data-injection attacks against power system state estimation: Modeling and countermeasures," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 3, pp. 717–729, Mar. 2014.
[13] L. Liu, M. Esmalifalak, Q. Ding, V. A. Emesih, and Z. Han, "Detecting false data injection attacks on power grid by sparse optimization," *IEEE Trans. Smart Grid*, vol. 5, no. 2, pp. 612–621, Mar. 2014.
[14] 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.
[15] L. Jia, J. Kim, R. J. Thomas, and L. Tong, "Impact of data quality on real-time locational marginal price," *IEEE Trans. Power Syst.*, vol. 29, no. 2, pp. 627–636, Mar. 2014.
[16] Y. Tan, Y. Li, Y. Cao, and M. Shahidehpour, "Cyber-attack on overloading multiple lines: A bilevel mixed-integer linear programming model," *IEEE Trans. Smart Grid*, vol. 9, no. 2, pp. 1534–1536, Mar. 2018.
[17] S. Liu, X. P. Liu, and A. El Saddik, "Denial-of-service (DoS) attacks on load frequency control in smart grids," in *Proc. IEEE PES Innov. Smart Grid Technol. Conf.*, Feb. 2013, pp. 1–6.
[18] A. R. Metke and R. L. Ekl, "Smart grid security technology," in *Proc. Innov. Smart Grid Technol. (ISGT)*, Jan. 2010, pp. 1–7.
[19] K. Jain, "Security based on network topology against the wiretapping attack," *IEEE Wireless Commun.*, vol. 11, no. 1, pp. 68–71, Feb. 2004.
[20] C. V. Wright, S. E. Coull, and F. Monrose, "Traffic morphing: An efficient defense against statistical traffic analysis," in *Proc. NDSS*, vol. 9, 2009, pp. 1–14.
[21] Z. Li, M. Shahidehpour, A. Alabdulwahab, and A. Abusorrah, "Bilevel model for analyzing coordinated cyber-physical attacks on power systems," *IEEE Trans. Smart Grid*, vol. 7, no. 5, pp. 2260–2272, Sep. 2016.
[22] 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.
[23] R. Deng, P. Zhuang, and H. Liang, "CCPA: Coordinated cyber-physical attacks and countermeasures in smart grid," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2420–2430, Sep. 2017.
[24] C. Chen, M. Cui, X. Wang, K. Zhang, and S. Yin, "An investigation of coordinated attack on load frequency control," *IEEE Access*, vol. 6, pp. 30414–30423, 2018.
[25] 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.
[26] J. Tian, B. Wang, T. Li, F. Shang, and K. Cao, "Coordinated cyber physical attacks considering DoS attacks in power systems," *Int. J. Robust Nonlinear Control*, vol. 5, no. 3, pp. 121–131, Nov. 2019.
[27] Y. Yuan, Z. Li, and K. Ren, "Quantitative analysis of load redistribution attacks in power systems," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 9, pp. 1731–1738, Sep. 2012.
[28] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, "A review of false data injection attacks against modern power systems," *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1630–1638, Jul. 2017.
[29] H. Sandberg, A. Teixeira, and K. H. Johansson, "On security indices for state estimators in power networks," in *Proc. 1st Workshop Secure Cont. Syst.*, 2010, pp. 1–6.
[30] R. Storn and K. Price, "Differential evolution—A simple and efficient heuristic for global optimization over continuous spaces," *J. Global Optim.*, vol. 11, no. 4, pp. 341–359, 1997.
[31] R. D. Christie. (1999). *Power Systems Test Case Archive*. University of Washington. Accessed: Nov. 25, 2013. [Online]. Available: https://www.ee.washington.edu/research/pstca/
[32] R. D. Zimmerman, "AC power flows, generalized OPF costs and their derivatives using complex matrix notation," MATPOWER Tech. Note 2, Feb. 2010.



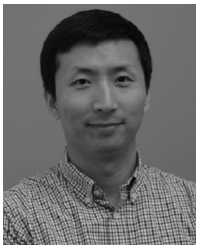
HAICHENG TU received the B.Eng. degree in communication engineering from Zhejiang Sci-Tech University, Hangzhou, China, in 2016. He is currently pursuing the Ph.D. degree with the College of Information Science and Electronic Engineering, Zhejiang University, Hangzhou.

His research interests include the applications of network science in the assessment and improvement of power systems and cyber physical systems.

YONGXIANG XIA (Senior Member, IEEE) received the B.Eng. and Ph.D. degrees in electronic engineering from Tsinghua University, Beijing, China, in 1998 and 2004, respectively.

He is currently a Distinguished Professor with Hangzhou Dianzi University. His research interest includes network science and its applications in engineering networks, where he has published more than 40 articles. He is a member of the IEEE Technical Committee on Nonlinear Circuits and Systems, an Editorial Board Member of *Scientific Reports*, and an Associate Editor of the IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS—II: EXPRESS BRIEFS.

CHI K. TSE (Fellow, IEEE) received the B.Eng. degree (Hons.) in electrical engineering and the Ph.D. degree from The University of Melbourne, Australia, in 1987 and 1991, respectively. He is currently the Chair Professor with The Hong Kong Polytechnic University, Hong Kong, where he was the Head of the Department of Electronic and Information Engineering, from 2005 to 2012. His research interests include power electronics, nonlinear circuits, and complex network applications.



XI CHEN (Senior Member, IEEE) received the B.Eng. degree in information engineering from Beijing Technology and Business University, Beijing, China, in 2003, the M.Sc. degree in digital signal processing from King's College London, University of London, London, U.K., in 2005, and the Ph.D. degree in electronic and information engineering from The Hong Kong Polytechnic University, Hong Kong, in 2009.

He was a Postdoctoral Research Fellow with the Institute of Software, Chinese Academy of Sciences, Beijing, from 2011 to 2013, and a Research Associate with The Hong Kong Polytechnic University, in 2009. He was a Visiting Student with the University of Florida, Gainesville, FL, USA, in 2008. In 2014, he joined GEIRI North America, San Jose, CA, USA, where he currently is the Chief Information Officer. From 2009 to 2014, he was with State Grid Corporation of China, Beijing. His research interests include the Internet of Things, smart grids, electric vehicle charging, and computer networks, and complex network analysis and its applications.