IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received May 24, 2019, accepted June 3, 2019, date of publication June 7, 2019, date of current version June 21, 2019.

*Digital Object Identifier 10.1109/ACCESS.2019.2921603*

# Optimal Strategy of Attack-Defense Interaction Over Load Frequency Control Considering Incomplete Information

**WENJUN BI, CHUNYU CHEN, AND KAIFENG ZHANG, (Member, IEEE)**
Key Laboratory of Measurement and Control of CSE, School of Automation, Southeast University, Nanjing 210096, China

Corresponding author: Kaifeng Zhang (kaifengzhang@seu.edu.cn)

This work was supported by National Natural Science Foundation of China under Grant 51577031 and Grant 61473083, and Research Program of State Grid Corporation of China (Dynamic Demand Response Control of Large-scale Diverse Demand Side Resources).

**ABSTRACT** Studying cyber attack-defense interaction over load frequency control (LFC) had become critical for guaranteeing the frequency quality and safety operation of power systems. It was revealed that both the attacker and the defender have multiple alternatives from strategy pools, which results in optimal strategy selection in pursuit of optimal payoff. In this paper, game theory model is introduced to analyze optimal strategy of attack-defense interaction over LFC. As to payoff calculation, we consider the comprehensive evaluating metric containing both the application effect and implementation cost of specific strategies, and propose a fuzzy logic-based calculation method. Considering the incomplete information in the attack-defense interaction game, we propose a mixed strategy method to obtain the optimal strategy. The simulation results show the effectiveness of the proposed optimal strategies.

**INDEX TERMS** Load frequency control, attack-defense interaction, optimal strategy, zero-sum game, incomplete information.

## I. INTRODUCTION

The electric power system is among the most fundamental critical infrastructures (CIs), and begins to face hacking risks [1], [2]. As one of the most essential operational functions in power systems, load frequency control (LFC) becomes the potential target of cyber attacks. By manipulating the interested signals or variables in LFC, hackers can destabilize the balance of active power and cause cascading failures. Therefore, the principles of counterattacks must be established to mitigate the attack damage.

Previous studies of cyber attacks on power systems mainly focus on the vulnerability analysis of the supervisory control and data acquisition (SCADA) [3], [4], topology [5], [6] and power system state estimation (PSSE) attack [7]–[12]. In recent literature, deceptive attack schemes of PSSE attack, which can disable the commonly used measurement residual-based detection methods under different scenarios, began to capture researchers' interests [7]–[9]. And a growing body of research investigates countermeasures against these more deceptive intrusions in turn [10]–[12].

In this paper, research on cyber attacks and defense strategies on LFC is focused. The scope of investigations of LFC oriented attacks mainly contains attack and counterattack measure design. As to attack schemes, reachability-based data injection attack for uncertain model scenario is studied by using feedback linearization [13]. An optimal attack minimizing the remaining time until the onset of disruption is presented in [14]. As to countermeasure design, a bad data alarm-based detection method is proposed using area control error (ACE) forecasting [15]. In [16], a new dynamic state estimator that can provide real-time models of the system is proposed to detect cyber attacks on power systems. A countermeasure to denial of service attack is proposed by reconfiguring routing topology using game tree [17]. As to attack-defense measure, Law [18] lays the groundwork for unified studies of attack and defense scheme of LFC by using game technique. In our prior literatures, attack strategies are systematically analyzed from aspects of attack influence and concealment, and detection schemes are designed with the aid of machine learning algorithm [19], [20].

With the increase of the types of attack and counterattack strategies, the attacker and defender have many alternatives

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

for attack and defense scheme design. Different joint actions (cartesian product of strategy pools of the attacker and the defender), could produce different payoffs. Hence, it is very essential to investigate the optimal countermeasure in attack-defense interaction over LFC considering this strategy pool scenario. Game-based model could effectively characterize the multi-strategy scenario, and optimal strategy selection is thus transformed into solving Nash equilibrium of the game. Groundbreaking work adopting game technique is proposed in [18]; and further refinement could be made considering more complex game conditions and payoff calculation. Notice that the incomplete information in the attack-defense game can lead to flexible payoffs under the same joint actions, i.e., the attacker and defender would make different gains when the level of knowledge varies, thus influencing the optimal strategy.

In order to study the optimal strategy of the attack-defense interaction over LFC systems, we propose a game-based interaction model considering incomplete information. The main contributions of the paper are twofold.

(1) To calculate the payoff of the attack-defense game in LFC systems, both the application effect and implementation cost are quantified with the aid of fuzzy logical-based method.

(2) For the first time the incomplete information game model is introduced to analyze optimal strategy of attack-defense interaction over LFC systems. A mixed strategy method is proposed to maximize the guaranteed payoff when the defender has incomplete information of the choice of the attack strategies.

The remaining of the paper is organized as follows. Section II presents the basic framework of game-based LFC attack-defense interaction model. Optimal strategy of attack-defense interaction over LFC is discussed in Section III. Simulations and analysis are addressed in Section IV. Finally, conclusions and discussions are drawn in Section V.

## II. BASICS OF ATTACK-DEFENSE GAME-BASED LOAD FREQUENCY CONTROL SYSTEM

### A. BASICS OF LOAD FREQUENCY CONTROL SYSTEM

The diagram of LFC of a normal multi-area interconnected system is represented in Fig. 1. Notice that the areas are divided into compromised area and other normal areas.

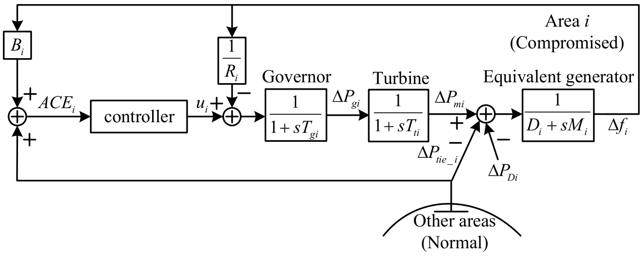

**FIGURE 1. Schematic of LFC of a multi-area system.**

The commands of LFC system for Area *i* are based on Area Control Error (ACE) signals, which can be expressed as

$$ACE_i = \beta_i \Delta f_i + \Delta P_{tie\_i} \tag{1}$$

where $\beta_i$ is the area frequency bias coefficient for Area *i*; $\Delta f_i$ and $\Delta P_{tie\_i}$ denote the frequency deviation and tie-line power, respectively. The LFC commands are dispatched down to the generating units, which mitigate power imbalance and guarantee frequency stability. The two main attack objectives in respect to LFC are frequency and tie-line interchange power measurement in (1). The latter is much more susceptible to cyber attacks compared with the former (falsification of frequency measurement can be easily detected by comparing with other normal readings); hence, only cyber attacks on tie-line interchange power measurement are considered. Moreover, since cyber attacks on tie-line interchange power measurement of both areas will not trigger the long-term instability [15], only one area (Area *i*) is assumed to be compromised. Based on our prior work [15], we model the compromised tie-line power signals as

$$\Delta P^*_{tie\_i} = \Delta P_{tie\_i} + D \tag{2}$$

where $\Delta P^*_{tie\_i}$ represents the tie-line power signals that the LFC center accepts; $D$ represents the compromised signals.

### B. HYPOTHESIS OF ATTACK-DEFENSE GAME

In this subsection, we assume that the attack-defense game on LFC systems has the following characteristics.

#### 1) ZERO-SUM GAME

Since the relation between the attacker and the defender is completely conflicting, we assume that the game discussed in this paper is a zero-sum game. The game is described by a triplet $(S_A, S_D, P)$, where

- $S_A = \{a_1, a_2, \ldots, a_m\}$ is the strategy pool for the attacker, in which multiple alternatives are available for the attacker. The attack strategy $a_i$ can be one attack or a combination of attacks at the same time.
- $S_D = \{d_1, d_2, \ldots, d_n\}$ is the strategy pool for the defender, in which multiple alternatives are available for the defender.
- $P(d_i, a_j) = (p^d_{ij}, p^a_{ij})$ gives real values on specific joint action of the defender and the attacker, where $p^d_{ij}$ and $p^a_{ij}$ are the payoff for the defender and attacker under joint action $(d_i, a_j)$. In the zero-sum game, the following formula is established

$$p^d_{ij} = -p^a_{ij} \tag{3}$$

#### 2) ATTACKERS HAVE TWO ATTACKING TENDENCIES

The attacker considers two attacking tendencies of FDI strategies: 1) damage oriented FDI; 2) deception oriented FDI.

- Damage oriented FDI attack scheme
In this case, the attacker does not consider his potential exposure by the alarm. He would inject false data

$D$ as much as possible to cause damages, which also increases the possibility of being detected by the alarm. Based on (2), we model the damage oriented FDI attack scheme as

$$\begin{aligned} \Delta P^{*}_{tie\_i} &= \Delta P_{tie\_i} + D \\ s.t.\, f_i &\geq f_u \; or \; f_i \leq f_l \end{aligned} \tag{4}$$

where $f_l$ and $f_u$ are the threshold frequency values which could trigger emergency control. That is, the magnitude of $D$ should be large enough to trigger frequency emergency control. In this paper, we assume that there are no large load variations during the cyber attacks on LFC systems. In fact, large load variations do not occur frequently, which means that normal large load variations and cyber attacks are unlikely to occur at the same time. As to small load variations, we assume that small load variations conform to the standard normal distribution.

- Deception oriented FDI attack scheme
  In this case, the attacker tries to make the compromised value of the monitoring variable below the alarm value, thus eluding detection by the alarm [15]. We model the damage oriented FDI attack scheme as

$$\begin{aligned} \Delta P^{*}_{tie\_i} &= \Delta P_{tie\_i} + D \\ s.t.\, x_{mc} &\leq x_{m0} \end{aligned} \tag{5}$$

  where $x_{mc}$ is the value of ACE signals. $x_0$ is the alarm value set by the defender.
  It can be seen the main differences between (4) and (5) are the inequality constraints: the constraint in (4) aims at the production of attack damage, while the constraint in (5) aims at detection elusion. These two criteria are the main goals of the attacker. In this paper, we use different values of $D$ to represent different strategies of attackers.

#### 3) DEFENDERS HAVE TWO KINDS OF DETECTION SCHEMES

The defender considers two kinds of detection schemes: 1) alarm-based detection scheme; 2) threshold-based detection scheme.

- Alarm-based detection scheme
  In this case, the defender uses false data alarm to distinguish between compromised and normal signals. If $x_{mc}$ surpasses $x_0$, then attack detection is achieved; otherwise, the attacker eludes the detection.
- Threshold-based detection scheme
  The core of threshold-based detection lies in the anomaly of transient behaviors of compromised variables. Specifically, a metric $m$ evaluating the transient behaviors is expressed by an accumulation of the change of the variable during certain time period [18]

$$m = \sum_{T_0} |x_{mea}(t) - x_{mea}(t-1)| \tag{6}$$

  where $m_0$ is the threshold value set by the defender. If $m \geq m_0$, then the compromised variable can be screened out; otherwise, the variable is regarded as normal.

In this paper, we use different values of $x_0$ and $m_0$ to represent different strategies of defenders.

#### 4) INCOMPLETE INFORMATION GAME

In this paper, we specify the incomplete information as the incomplete knowledge of opponent's strategy. The attacker and defender, during attack-defense interaction over LFC, would have incomplete information about specific conditions: The attacker has incentives to mimic the normal ACE to elude detection. Hence, the defender would protect normal ACE signals and the alarm from the outsiders, causing the attacker information incompleteness. The incomplete information could change the payoff of the game, thus influencing the decision-making of attacker and defender.

As to attacker, the alarm value or the threshold value set by the defender cannot be obtained, which makes it difficult for attacker to accurately calculate the payoff of attack strategies in specific situations. Based on the attacking tendencies, attackers can launch attack by randomly selecting attack strategy from the attack strategy pool.

As to defender, the compromised value $D$ set by attacker cannot be obtained. Defender should choose appropriate alarm value or threshold value to cope with possible attack strategy.

## III. OPTIMAL STRATEGY OF ATTACK-DEFENSE INTERACTION OVER LFC

In this section, optimal strategy is discussed based on the attack-defense game-based LFC system model in Section II. Firstly, fuzzy logic-based model of payoff is established. Then, from the perspective of defender, optimal strategy is designed by mixing the strategies from the strategy pool with certain probability to maximize the payoff.

### A. FUZZY LOGIC-BASED PAYOFF IN ATTACK-DEFENSE INTERACTION OVER LFC

In order to calculate payoff, the following evaluation indexes are considered from the perspective of attackers. Notice that what the attacker gains is the opposite of what the defender gains.

- Application effect
  Application effect $ae(d_i, a_j)$ reflects the extent to which an attacker achieves his goal. $ae(d_i, a_j)$ is defined by cumulative frequency deviation $F_{ae}$.

$$F_{ae} = \sum_{T=0}^{T=T_1} |\Delta f(T+1) - \Delta f(T)| \tag{7}$$

  where $\Delta f(T)$ represents the system frequency deviation at time $T$. $\Delta f$ can be expressed as

$$\Delta f = \sum_{j=1}^{n} H_i f_i / \sum_{i=1}^{n} H_i - f_s \tag{8}$$

where $f_i$ and $H_i$ are the frequency and the inertia of Area $i$; $f_s$ is the nominal frequency.

- Implementation cost
  Implementation cost $ic(d_i, a_j)$ evaluate the cost of using specific strategy for attacker. $ic(d_i, a_j)$ is defined by the possibility of being detected.

$$ic(d_i, a_j) = \frac{TP}{TP + FN} \tag{9}$$

where TP stands for true positives (samples correctly identified as anomalies); FN represents false negatives (samples inaccurately identified as the normal).

The payoff can be represented by the weighted difference of the utility of $ae(d_i, a_j)$ and $ic(d_i, a_j)$:

$$p^a_{ij} = -p^d_{ij} = \alpha_1 U_1(ae(d_i, a_j) - \alpha_2 U_2(ic(d_i, a_j)) \tag{10}$$

where $\alpha_1, \alpha_2 = [0, 1]$ represent the weighting coefficients; the minus sign indicates that implementation cost is the loss to the attacker; $U_1$ and $U_2$ are the utility function. The weights $\alpha_1$ and $\alpha_2$ reflect how the attacker weighs each objective. As can be seen, $ae(d_i, a_j)$ and $ic(d_i, a_j)$ are of different magnitudes, and normalization is required to make utility consistent with the weights the decision maker assigns. Therefore, we select $U_1$ and $U_2$ as the following min-max functions [22]:

$$U_{1,2} = \frac{p - p_{min}}{p_{max} - p_{min}} \tag{11}$$

where $p_{min}$ and $p_{max}$ are the minimum and maximum of payoff $p$.

Let $p_{ae}$ and $p_{ic}$ are the normalized application effect and implementation cost in the sense of utility, utility in (11) can be expressed by the weighted sum of $p_{ae}$ and $p_{ic}$ :

$$p^a_{ij} = -p^d_{ij} = \alpha_1 p_{ae} - \alpha_2 p_{ic} \tag{12}$$

The weighting coefficients $\alpha_1$ and $\alpha_2$ should be dependent on $p_{ae}$ and $p_{ic}$. Ideally, the attacker desires to maximize $p_{ae}$ and minimize $p_{ic}$ simultaneously. However, these two objectives are usually conflicting. For example, if $p_{ae}$ achieves high scores, which means the attacker is prone to use $a_1$ to increase $F_{ae}$. It will lead to high implementation cost, which is equivalent to the high scores of $p_{ic}$, and vice versa.

From the perspective of the attacker, it is assumed that the attacker prioritizes $p_{ae}$ promotion over $p_{ic}$ reduction. The attacker would not pay more attention to control of implementation cost until he achieves sufficient level of application effect. That is, the highest priority is given to $p_{ae}$; when certain $p_{ae}$ is achieved, $p_{ic}$ is then considered. For example, when $p_{ae}$ is of little but $p_{ic}$ is of high score, the attacker has no incentives to weigh more implementation cost, thus assigning small value to $\alpha_2$. When both $p_{ae}$ and $p_{ic}$ achieve high scores, the attacker begins to weigh more the implementation cost by assigning big value to $\alpha_2$. Furthermore, In order to make the payoff variation between different $p_{ae}$ explicit, $\alpha_1$ is assumed to be positively correlated to $p_{ae}$. Based on the aforementioned analysis, the weighting coefficients can be calculated as

$$\alpha_1 = p_{ae} \tag{13}$$

$$\alpha_2 = \min\{p_{ae}, p_{ic}\} \tag{14}$$

The analysis above present a fuzzy conception of computation of $\alpha_1$ and $\alpha_2$, and thus fuzzy logic method is adopted to quantify $\alpha_{1,2}$. Through fuzzification and defuzzification, the fuzzy logic component can generate crisp weighting coefficients $\alpha_1$ and $\alpha_2$ based on decision maker's fuzzy preferences to $p_{ae}$ and $p_{ic}$ The fuzzy sets for the inputs $p_{ae}$ and $p_{ic}$ are both {S M B}, where **S** - small; **M** - medium; **M** - big. Similarly, the fuzzy sets for the outputs $\alpha_1$ and $\alpha_2$ are the same as those for the inputs.

The core of weighting coefficient calculation is the design of fuzzy logic rules. Based on (13) and (14), the fuzzy rules are given in Table 1 and 2.

**TABLE 1.** Rules base for $\alpha_1$.

| $p_{ae}$<br>$p_{ic}$ | S | M | B |
|---|---|---|---|
| S | S | M | B |
| M | S | M | B |
| B | S | M | B |

**TABLE 2.** Rules base for $\alpha_2$.

| $p_{ae}$<br>$p_{ic}$ | S | M | B |
|---|---|---|---|
| S | S | S | S |
| M | S | M | M |
| B | S | M | B |

The membership functions for both the inputs and outputs are a string of symmetric triangles with equal base.

### B. OPTIMAL STRATEGY CONSIDERING INCOMPLETE INFORMATION

As is mentioned in Section II. B, defender has incomplete information of the compromised signals D since attacker launches attack by randomly selecting attack strategy from the strategy pool. The optimal strategy for the defender is to maximize the minimum payoff when faced with all attack strategies from the strategy pool.

*Remark 1:* Considering that it is not suitable to discuss the optimal attack strategy publicly, we only discuss the optimal strategy of the defender in this subsection.

If the attacker has $m$ alternatives and the defender has $n$ alternatives, the normal form game can be expressed in a matrix form:

$$\begin{array}{ccccc} & a_1 & a_2 & \cdots & a_m \\ d_1 & (p^d_{11}, p^a_{11}) & (p^d_{12}, p^a_{12}) & \cdots & (p^d_{1m}, p^a_{1m}) \\ d_2 & (p^d_{21}, p^a_{21}) & (p^d_{22}, p^a_{22}) & \cdots & (p^d_{2m}, p^a_{2m}) \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ d_n & (p^d_{n1}, p^a_{n1}) & (p^d_{n2}, p^a_{n2}) & \cdots & (p^d_{nm}, p^a_{nm}) \end{array} \tag{15}$$

For a specific strategy $d_i$, the minimum payoff can be expressed as

$$p_i^{min} = \min\{p_{i1}^d, p_{i2}^d, \ldots, p_{im}^d\} \tag{16}$$

The goal of the defender is to find the optimal strategy to maximize his payoff $p^{max}$. $p^{max}$ can be expressed as

$$p^{max} = \max\{p_1^{min}, p_2^{min}, \ldots, p_n^{min}\} \tag{17}$$

Therefore, the optimal strategy for the defender can thus be described by

$$d_{op} = \arg \max_{d_i \in S_D} \min_{a_j \in S_A} p_{ij}^d \tag{18}$$

In this paper, the mixed defense strategy, which means that defender can choose multiple defense strategies based on certain probability, is used to further enhance the payoff to defender. The mixed strategy for defender may be represented by $\Gamma = [\gamma_1, \gamma_2, \ldots, \gamma_n]^T$ of probabilities that add to 1. If defender chooses column $j$ in (15), the payoff to defender can be described by

$$p_j^d = \sum_{i=1}^{n} \gamma_i p_{ij}^d \tag{19}$$

Based on (18) and (19), the optimal mixed defense strategy can be described by

$$d_m = \arg \max_{\{\gamma_1, \ldots, \gamma_n\}} \min_{a_j \in S_A} p_j^d \tag{20}$$

The optimal mixed defense strategy is formulated as the linear programming (LP) problem (21).

$$\max \sum_{i=1}^{n} \gamma_i p_{ij}^d \tag{21}$$

$$\text{subject to} \sum_{i=1}^{n} (p_{ij}^d - p_{ik}^d)\gamma_i \leq 0 \ \ \forall k = 1, 2, \ldots m \tag{22}$$

$$0 \leq \gamma_i \leq 1 \ \ \forall \gamma_i \in \Gamma \tag{23}$$

$$\sum_{i=1}^{n} \gamma_i = 1 \tag{24}$$

Notice that this LP model needs to run $m$ times to find the optimal defense strategy. There are two situations in the solution process. The first situation is that there exists an optimal solution to the current linear programming problem. As to the attack strategy in this situation, it can be regarded as an attack strategy that affects the defender's decision-making. The second situation is that there is no optimal solution to the current linear programming problem. It can be learned that the attack strategy in this situation plays no role in the minimum envelop, which means that this attack strategy is dominated by other attack strategies. Defender does not need to consider this attack strategy when choosing defense strategy. This enables defender to effectively reduce the number of attack strategies they need to consider when facing a larger attack strategy pool.

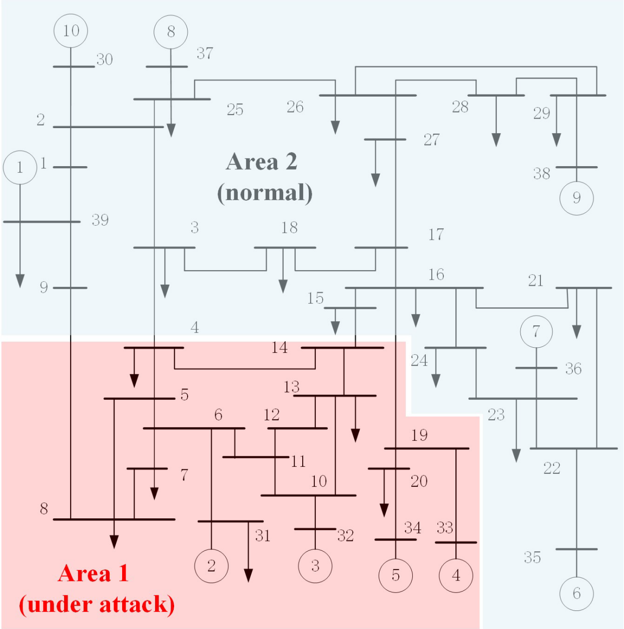

**FIGURE 2.** Diagram of 10-unit-39-bus-based two-area system.

## IV. CASE STUDIES

In this section, case studies are presented with regards to the optimal strategy selection discussed in Section III. Notice that the real data about power grid attacks are confidential at present, which means that the detailed data can be hardly accessed. In this section, the IEEE standard system is used to verify the proposed method. In Section IV.A, the simulation model is briefly discussed. In Section IV.B, through numerical analyses, performances of different joint of actions on application effects and implementation costs are studied. In Section IV.C, optimal strategies are discussed in different situations.

### A. MODELING OF CYBER ATTACKS ON LFC

LFC model is built upon a 10-unit-39-bus two-area system as shown in Fig. 3. The system is modelled in the MATLAB/SIMULINK environments. The parameters of the elements, e.g., ten generating units $G_i$, the primer mover

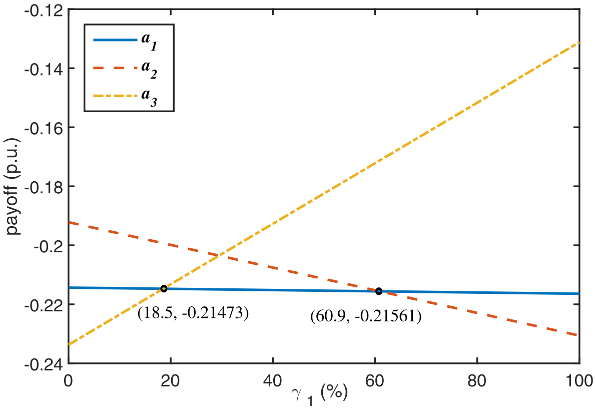

**FIGURE 3.** Payoff of mixed strategy in case 1.

and governing system and the transmission network, are given in [25]. Based on the analysis in [15], the upper frequency threshold value $f_u$ is 1.0117 p.u. and the lower frequency threshold value $f_l$ is 0.9883 p.u.. As to the attack strategies, 1000 samples are randomly generated considering the two attacking tendencies. As to the detection scheme, the defender can choose either alarm-based detection scheme or threshold-based detection scheme. Defender can mix several different defense strategies in all of the alarm-based detection schemes or the threshold-based detection schemes. Defender can also mix defense strategies in both alarm-based detection schemes and threshold-based detection schemes. Without loss of generality, the set of the alarm value is assumed to be $\{1.9, 2.0, 2.1\}$ and the set of the threshold value is assumed to be $\{3.4, 3.5, 3.6\}$.

### *B. NUMERICAL ANALYSIS OF APPLICATION EFFECT/IMPLEMENTATION COST*

In this subsection, model-based application effect and implementation cost in Section III under different joint of actions are studied.

#### 1) SCENARIO 1: DECEPTION ORIENTED FDI ATTACK SCHEME AND ALARM-BASED DETECTION SCHEME

Without loss of generality, let parameter $D$ in (4) be: $D_i = 1 + 0.1i$ $(0 \leq i \leq 4)$. Application effect and implementation cost are shown in TABLE 3 and TABLE 4.

**TABLE 3.** Application effect in scenario 1.

| $D_i$ | 1 | 1.1 | 1.2 | 1.3 | 1.4 |
|---|---|---|---|---|---|
| min. freq. | 0.9922 | 0.9915 | 0.9907 | 0.9899 | 0.9891 |
| application effect | 0.0111 | 0.0122 | 0.0133 | 0.0144 | 0.0154 |

**TABLE 4.** Implementation cost in scenario 1.

| $D_i$<br>$x_0$ | 1 | 1.1 | 1.2 | 1.3 | 1.4 |
|---|---|---|---|---|---|
| 1.9 | 0.03 | 0.05 | 0.08 | 0.06 | 0.07 |
| 2.0 | 0.02 | 0.05 | 0.06 | 0.06 | 0.03 |
| 2.1 | 0.02 | 0.02 | 0.05 | 0.04 | 0.03 |

From TABLE 3, it can be learned that application effect of the deception oriented FDI attack scheme is positively associated with the value of parameter $D$, which makes the attacker more inclined to choose a larger $D$. Notice that none of the minimum frequency under deception attack is lower than $f_l$, which can not trigger emergency control to cause greater damage. From TABLE 4, it can be learned that implementation cost of the deception oriented FDI attack scheme is at a low level and not positively associated with the value of parameter $D$.

#### 2) SCENARIO 2: DECEPTION ORIENTED FDI ATTACK SCHEME AND THRESHOLD-BASED DETECTION SCHEME

Values of $D$ are the same as those in Scenario 1, and all the *ae* have the same scores as those in Scenario 1. Implementation cost is shown in TABLE 5. It can be learned that the deception-oriented FDI attack can also maintain a low implementation cost in this case.

**TABLE 5.** Implementation cost in scenario 2.

| $D$<br>$m_0$ | 1 | 1.1 | 1.2 | 1.3 | 1.4 |
|---|---|---|---|---|---|
| 3.4 | 0.1 | 0.09 | 0.13 | 0.13 | 0.12 |
| 3.5 | 0.1 | 0.09 | 0.13 | 0.13 | 0.11 |
| 3.6 | 0.1 | 0.08 | 0.12 | 0.09 | 0.07 |

#### 3) SCENARIO 3: DAMAGE ORIENTED FDI ATTACK SCHEME AND ALARM-BASED DETECTION SCHEME

Without loss of generality, let parameter $D$ in (4) be: $D_i = 1 + 0.1i$ $(0 \leq i \leq 4)$. Application effect and implementation cost are shown in TABLE 6 and TABLE 7.

**TABLE 6.** Application effect in scenario 3.

| $D_i$ | 1.5 | 1.6 | 1.7 | 1.8 | 1.9 |
|---|---|---|---|---|---|
| min. freq. | 0.9883 | 0.9876 | 0.9868 | 0.9861 | 0.9853 |
| application effect | 0.0165 | 0.0176 | 0.0188 | 0.0198 | 0.0209 |

**TABLE 7.** Implementation cost in scenario 3.

| $D_i$<br>$x_0$ | 1.5 | 1.6 | 1.7 | 1.8 | 1.9 |
|---|---|---|---|---|---|
| 1.9 | 0.1 | 0.18 | 0.27 | 0.38 | 0.45 |
| 2.0 | 0.06 | 0.13 | 0.21 | 0.27 | 0.26 |
| 2.1 | 0.06 | 0.07 | 0.14 | 0.20 | 0.17 |

From TABLE 6, it can be learned that the minimum frequency under damage oriented FDI attack is lower than $f_l$, which can trigger emergency control to cause severe damage. Based on the data shown in TABLE 6 and TABLE 7, it can be learned that application effect and implementation cost are positively correlated with the value of parameter $D$.

#### 4) SCENARIO 4: DAMAGE ORIENTED FDI ATTACK SCHEME AND THRESHOLD-BASED DETECTION SCHEME

$D$ are the same as those in Scenario 3, and all the *ae* have the same scores as those in Scenario 3. Implementation cost is shown in TABLE 8

**TABLE 8.** Implementation cost in scenario 2.

| $D_i$<br>$m_0$ | 1.5 | 1.6 | 1.7 | 1.8 | 1.9 |
|---|---|---|---|---|---|
| 3.4 | 16 | 22 | 28 | 31 | 35 |
| 3.5 | 14 | 22 | 26 | 28 | 30 |
| 3.6 | 10 | 17 | 24 | 24 | 27 |

### *C. NUMERICAL ANALYSIS OF OPTIMAL STRATEGY IN ATTACK-DEFENSE INTERACTION OVER LFC*

In this subsection, optimal mixed defense strategy is discussed in the following three cases.

- Case 1: By comparing with other method, the advantages of mixed defense strategy are illustrated in this case.
- Case 2: The optimal mixed strategy is discussed when there are multiple strategies in each type of detection schemes.

#### 1) CASE 1

In this case, three attack strategies $\{a_1, a_2, a_3\}$ and two defense strategies $\{d_1, d_2\}$ are selected. Without loss of generality, let the parameter $D$ in $a_1$, $a_2$ and $a_3$ be 1.3, 1.4 and 1.5. Let the parameter $x_0$ in $d_1$ and $d_2$ be 2.0 and 2.1. Based on the payoff calculation method in III. A, the payoff can be calculated as:

$$\begin{array}{cccc} & a_1 & a_2 & a_3 \\ d_1 & -0.21641 & -0.23061 & -0.13119 \\ d_2 & -0.21435 & -0.19218 & -0.23371 \end{array} \tag{25}$$

As to the traditional pure strategy, it can be learned that defense strategy $d_1$ can be chosen to ensure at least $-0.23061$ payoff in the face of all the attack strategies. When defender uses the proposed mixed strategy, he can choose the defense strategy with probability $\gamma_1$ and the defense strategy with probability $1 - \gamma_1$. The payoff of the proposed mixed strategy is shown in Fig. 3.

Based on the intersection of the lines shown in Fig. 3, it can be learned that defender can maximize his guaranteed payoff, which equals to $-0.21473$, by choosing strategy $a_1$ with probability 18.5%. Notice that when $\gamma_1$ equals 100% or 0%, the defense strategy is the traditional pure strategy. The payoff of the proposed mixed strategy can be 6.8% higher than the payoff of the traditional pure strategy.

#### 2) CASE 2

In this case, three attack strategies $\{a_1, a_2, a_3\}$ and three defense strategies $\{d_1, d_2, d_3\}$ are selected. Without loss of generality, let the parameter $D$ in $a_1$, $a_2$ and $a_3$ be 1.4, 1.5 and 1.6. Values of $x_0$ and $m_0$ are introduced in Section IV. A. As to the strategies in alarm-based detection scheme, the payoff $p_{ij}^d$ can be calculated as:

$$\begin{array}{cccc} & a_1 & a_2 & a_3 \\ d_1 & -0.2087 & -0.2267 & -0.1788 \\ d_2 & -0.2164 & -0.2306 & -0.1312 \\ d_3 & -0.2144 & -0.1922 & -0.2337 \end{array} \tag{26}$$

The results of the LP problem (21) are shown in TABLE 9.

**TABLE 9. Results of the LP problem considering alarm-based detection schemes.**

| | $\max p_j^d$ | $\gamma_1$ | $\gamma_2$ | $\gamma_3$ |
|---|---|---|---|---|
| $j$=1 | -0.2112 | 55.27% | 0 | 44.73% |
| $j$=2 | -0.2112 | 55.27% | 0 | 44.73% |
| $j$=3 | -0.2121 | 39.31% | 0 | 60.69% |

From (26), It can be learned that the maximum guaranteed payoff equals to -0.2267 with the aid of traditional pure strategy. From TABLE 9, it can be learned that the optimal defense strategy is to set $x_0 = 1.9$ with probability 55.27% and set $x_0 = 2.1$ with probability 44.73%. The defender can get at least $-0.2112$ payoff with the aid of the proposed mixed defense strategy. By comparison, the proposed mixed strategy can also perform well in the case considering alarm-based detection scheme.

As to the defense strategies in threshold-based detection scheme, the payoff $p_{ij}^d$ can be calculated as:

$$\begin{array}{cccc} & a_1 & a_2 & a_3 \\ d_1 & -0.2003 & -0.1618 & -0.1012 \\ d_2 & -0.2087 & -0.1820 & -0.0372 \\ d_3 & -0.2217 & -0.2365 & -0.1012 \end{array} \tag{27}$$

The results of the LP problem (21) are shown in TABLE 10.

**TABLE 10. Results of the LP problem considering threshold-based detection schemes.**

| | $\max p_j^d$ | $\gamma_1$ | $\gamma_2$ | $\gamma_3$ |
|---|---|---|---|---|
| $j$=1 | -0.2003 | 100% | 0 | 0 |
| $j$=2 | -0.2158 | 27.71% | 0 | 72.29% |
| $j$=3 | N/A | N/A | N/A | N/A |

Notice that the maximum guaranteed payoff of the traditional pure strategy equals to the one of the proposed mixed strategy. It can be learned that the proposed mixed strategies contain traditional pure strategies in special cases, which means that the proposed mixed strategy has wider applicability.

## V. CONCLUSIONS AND DISCUSSIONS

### A. CONCLUSIONS

In this paper, optimal strategy selection is studied for attack-defense interaction over load frequency control (LFC). The attack-defense interaction is modelled by a incomplete information game, thus searching for the optimal strategy is equivalent to computation of maximum guaranteed payoff. Through case studies, it can be learned that the proposed mixed strategy method enables the defender to choose optimal defense strategies.

### B. DISCUSSIONS

As to practical implementation, the challenge is to accurately calculate the payoff of both attackers and defenders. Reasonable payoff can help defenders make the right decisions. The next step of the study could be to optimize the existing payoff calculation model based on the actual scenario data.

## Acknowledgment

*(Wenjun Bi and Chunyu Chen contributed equally to this work.)*

## REFERENCES

[1] C.-W. Ten, G. Manimaran, and C.-C. Liu, "Cybersecurity for critical infrastructures: Attack and defense modeling," *IEEE Trans. Syst., Man, Cybern. A, Syst. Humans*, vol. 40, no. 4, pp. 853–865, Jul. 2010.

[2] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber-physical system security for the electric power grid," *Proc. IEEE*, vol. 100, no. 1, pp. 210–224, Jan. 2012.

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

[4] A. Nicholson, S. Webber, S. Dyer, T. Patel, and H. Janicke, "SCADA security in the light of cyber-warfare," *Comput. Secur.*, vol. 31, no. 4, pp. 418–436, Jun. 2012.

[5] J. Yan, H. He, X. Zhong, and Y. Tang, "Q-learning-based vulnerability analysis of smart grid against sequential topology attacks," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 1, pp. 200–210, Jan. 2017.

[6] X. Liu, Z. Li, X. Liu, and Z. Li, "Masking transmission line outages via false data injection attacks," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 7, pp. 1592–1602, Jul. 2016.

[7] 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, pp. 1–13, Jan. 2011.

[8] A. Teixeira, G. Dán, H. Sandberg, and K. H. Johansson, "A cyber security study of a SCADA energy management system: Stealthy deception attacks on the state estimator," *IFAC Proc. Vol.*, vol. 44, no. 1, pp. 11271–11277, Jan. 2011.

[9] 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.

[10] O. Vukovic, K. C. Sou, G. Dan, and H. Sandberg, "Network-aware mitigation of data integrity attacks on power system state estimation," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 6, pp. 1108–1118, Jul. 2012.

[11] 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.

[12] H. Fawzi, P. Tabuada, and S. Diggavi, "Secure estimation and control for cyber-physical systems under adversarial attacks," *IEEE Trans. Autom. Control*, vol. 59, no. 6, pp. 1454–1467, Jun. 2014.

[13] P. M. Esfahani, M. Vrakopoulou, K. Margellos, J. Lygeros, and G. Andersson, "A robust policy for automatic generation control cyber attack in two area power network," in *Proc. 49th IEEE Conf. Decis. Control (CDC)*, Atlanta, GA, USA, Dec. 2010, pp. 5973–5978.

[14] R. Tan, H. H. Nguyen, E. Y. S. Foo, D. K. Y. Yau, Z. Kalbarczyk, R. K. Iyer, and H. B. Gooi, "Modeling and mitigating impact of false data injection attacks on automatic generation control," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 7, pp. 1609–1624, Jul. 2017.

[15] S. Sridhar and M. Govindarasu, "Model-based attack detection and mitigation for automatic generation control," *IEEE Trans. Smart Grid*, vol. 5, no. 2, pp. 580–591, Mar. 2014.

[16] A. P. S. Meliopoulos, G. Cokkinides, R. Fan, and L. Sun, "Data attack detection and command authentication via cyber-physical comodeling," *IEEE Des. Test*, vol. 34, no. 4, pp. 34–43, Aug. 2017.

[17] P. Srikantha and D. Kundur, "Denial of service attacks and mitigation for stability in cyber-enabled power grid," in *Proc. IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf. (ISGT)*, Washington, DC, USA, Feb. 2015, pp. 1–5.

[18] Y. W. Law, T. Alpcan, and M. Palaniswami, "Security games for risk minimization in automatic generation control," *IEEE Trans. Power Syst.*, vol. 30, no. 1, pp. 223–232, Jan. 2015.

[19] C. Chen, K. Zhang, K. Yuan, L. Zhu, and M. Qian, "Novel detection scheme design considering cyber attacks on load frequency control," *IEEE Trans. Ind. Informat.*, vol. 14, no. 5, pp. 1932–1941, May 2018.

[20] W. Bi, K. Zhang, Y. Li, K. Yuan, and Y. Wang, "Detection scheme against cyber-physical attacks on load frequency control based on dynamic characteristics analysis," *IEEE Syst. J.*, to be published. doi: 10.1109/JSYST.2019.2911869.

[21] M. J. Osborne, *An Introduction to Game Theory*, vol. 3. New York, NY, USA: Oxford Univ. Press, 2004.

[22] O. Grodzevich and O. Romanko, "Normalization and other topics in multi-objective optimization," in *Proc. Fields-MITACS Ind. Problems Workshop*, 2006, pp. 87–101.

[23] E. Rasmusen, *Games and Information*, vol. 15. Hoboken, NJ, USA: Blackwell, 1994.

[24] R. Gibbons, *A Primer in Game Theory*. New York, NY, USA: Wheatsheaf Harvester, 1992.

[25] C. Huang, K. Zhang, X. Dai, and Q. Zang, "Robust load frequency controller design based on a new strict model," *Electr. Power Compon. Syst.*, vol. 41, no. 11, pp. 1075–1099, Jul. 2013.

**WENJUN BI** received the B.S. degree in electrical engineering from Southwest Jiaotong University, Chengdu, China, in 2013 and he is pursuing the Ph.D. degree with Southeast University, Nanjing, China.

**CHUNYU CHEN** received the B.S. degree in electrical engineering from the China University of Mining and Technology, Xuzhou, China, in 2012 and he is pursuing the Ph.D. degree with Southeast University, Nanjing, China.

**KAIFENG ZHANG** (M'10) received the Ph.D. degree from Southeast University, Nanjing, China, in 2004. He was a Postdoctoral Fellow in Control Science and Engineering, from 2004 to 2006 and joined the Faculty of Southeast University ever since. He was a Visiting Scholar in Lehigh University, from 2013 to 2014. He was also a Visiting Scholar in Energy Systems Division, Argonne National Laboratory, in 2016. His research interests include in the areas of power systems dispatch and control, wind power, electricity market, and nonlinear control.