Research Article

An Optimal DoS Attack Strategy Disturbing the Distributed Economic Dispatch of Microgrid

Yihe Wang,1 Mingli Zhang,2 Kun Song,2 Tie Li,3 and Na Zhang2

1School of Information Science and Engineering, Northeastern University, Shenyang 110819, China
2State Grid Liaoning Electric Power Company Limited Economic Research Institute, Shenyang 110015, China
3State Grid Liaoning Electric Power Supply Co. Ltd., Shenyang 110004, China

Correspondence should be addressed to Yihe Wang; 1710247@stu.neu.edu.cn

Received 20 January 2021; Revised 15 February 2021; Accepted 6 March 2021; Published 2 April 2021

Academic Editor: Rui Wang

Copyright © 2021 Yihe Wang et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

As a promising method with excellent characteristics in terms of resilience and dependability, distributed methods are gradually used in the field of energy management of microgrid. However, these methods have more stringent requirements on the working conditions, which will make the system more sensitive to communication failures and cyberattacks. As a result, it is both theoretical merits and practical values to investigate the malicious effect of cyber attacks on microgrid. This paper studies the distributed economic dispatch problem (EDP) under denial-of-service (DoS) attacks for the microgrid, in which each generator can communicate with its neighbors and has the computational capability to implement local operation. Firstly, a DoS attack model is proposed, in which the DoS attacker intentionally jams the communication channel to deteriorate the performance of the microgrid. Then, the evolution mechanism of the dispatch system of the microgrid under different attack scenarios is adequately discussed. On this basis, an optimal attack strategy based on enumerating-search algorithm is presented to allocate the limited attack resources reasonably, so as to maximize the effect of DoS attacks. Finally, the validity of the theoretical studies about the attack effect under different scenarios and the effectiveness of the proposed enumerating-search-based optimal attack strategy are illustrated through the simulation examples on the IEEE 57-bus system and IEEE 39-bus system, respectively.

1. Introduction

The intelligent microgrid integrates various renewable generators and energy storage systems within a distributed system to achieve the goal of energy-saving and efficient operation and has been widely recognized as the future of power system. As a multidimensional complex system, the microgrid includes widely distributed sensors, capacity of control and optimization computation, and well-developed communication networks [1]. Now, it has been widely recognized as a typical cyber-physical system (CPS), and various fundamental problems of the microgrid have been reinvestigated in the perspective of CPS in the last few years, such as droop control [2], economic dispatch [3], and zero-sequence current suppression control [4].

Like the traditional power system, economic dispatch is one of the most concerned issues in the operation of the microgrid. Economic dispatch of the microgrid with the goal of minimizing operating costs can realize the collaborative optimization and energy distribution among units. Generally speaking, the methods to solve the economic dispatch problem (EDP) of the microgrid can be classified into centralized methods and distributed methods. Although the centralized methods are efficient, they need central authorities to collect global information of all the controlled units. These methods are sensitive to single-point failure and increase the communication burden of system [5]. On the opposite, the distributed methods without central authorities can carry out the economic dispatch with less communication burden and better scalability and privacy [6]. As a consequence, scholars have investigated the EDP for the microgrid based on various distributed methods in the past few years [7–10]. For example, a fully distributed algorithm proposed in [7] can fit well with arbitrary initializations. Moreover, it enabled generators to collectively obtain the mismatch between demand and total power output as a feedback mechanism to adjust actual power...
generation. In order to maximize the social welfare, a distributed consensus algorithm based on augmented Lagrangian and projection penalty function was proposed in [8]. Literature [9] presented a distributed double-Newton descent algorithm for cooperative energy management with faster convergence speed in a fully distributed fashion. In [10], a novel distributed primal-dual augmented subgradient algorithm was investigated, which can solve a class of distributed constrained optimization problems over a general unbalanced directed communication network. However, the above literature assumes that these algorithms are executed under ideal communication conditions and the possible cyberattacks in the communication network are not considered. In practice, once the malicious cyberattacks occur in the communication network of the microgrid, the data transmission will be disturbed, and the execution of those algorithms will be affected. Consequently, the optimal operation points of the system will move, and the execution of those algorithms will be affected. Therefore, it is of theoretical and practical significance to investigate the EDP under various cyberattacks.

Until now, two types of cyberattacks have received the most attention: denial-of-service (DoS) attacks and deception attacks [12]. As a common type of cyberattacks in CPS, DoS attacks attempt to make the network resource unavailable for its intended users. This kind of attack blocks real traffic by sending a mass of invalid information that takes up all the communication bandwidth. Currently, research on DoS attacks has two main perspectives as follows. (1) From the perspective of system defense, in order to mitigate the vulnerability of system under attacks, many robust methods have been investigated in recent years [13–15], such as event/self-triggered control [13], the confidence-level-based resilient strategy [14], and intensity-dependent consensus protocol [15]. (2) From the perspective of DoS attacker, in order to increase the probability of successful attacks and enhance the effect of attacks, the attacker tends to formulate various optimal attack strategies. For example, literature [16] proposed an optimal attack strategy under limited attack resources, and this strategy can damage the estimation performance of the system by deciding which sensor to attack. And, on this basis, the optimal attack time and attack mode are determined in [17] to maximum the impact of DoS attacks on the remote state estimation of the power system. However, the above research on the optimal attack strategies only discusses the DoS attacks against the state estimation, and the goal of it is to undermine the security and stability of systems. Until now, there are few literatures on designing the optimal DoS attacks strategies to damage the economic performance of the power system. However, the degradation caused by DoS attacks to the economic performance of the power system cannot be ignored, which may have a great impact on the national economy. As a result, it is necessary to study under what strategy the attack will cause the maximum degree of economic performance degradation, i.e., the optimal attack strategy disturbing the distributed economic dispatch of the microgrid.

Based on the above analysis, the motivation of the current work is in the following three aspects:

(1) As a common type of cyberattacks, DoS attacks are highly destructive, which may cause severe consequences for the power system.

(2) As far as we know, there are few literatures about the impact of DoS attacks on the economic dispatch of the power system. However, it is essential to analyze potential consequences of these attacks on the economic performance of the system.

(3) Research on optimal attack strategies can guide the formulation of defense measures for energy systems, and one needs to understand what the worst effect of attacks might be.

In this paper, we investigate the economic dispatch problem of the microgrid under DoS attacks. Firstly, the model of DoS attacks is established according to their working mechanism. Then, the impact of DoS attacks on the economic dispatch of the microgrid under different scenarios is investigated. On this basis, an optimal attack strategy that can maximize the effect of attacks with limited attack resources is proposed. The main contributions of this paper are summarized as follows:

(1) In this paper, the EDP of the microgrid under DoS attacks is investigated, which further enriches the theoretical research on DoS attacks in the power system.

(2) The time-varying communication network caused by DoS attacks can be divided into two types, i.e., connected and disconnected. How the two scenarios of attacks affect economic dispatch is analyzed in this paper (Theorems 1 and 2).

(3) Different from the existing literatures, where optimal attack strategies were always put forward to increase the state estimation error of the power system, the optimal attack strategy proposed in this paper aims at damaging economic performance of the microgrid.

(4) An enumerating-search algorithm is proposed to find out the optimal attack strategy for DoS attacker (Algorithm 1).

The rest of the paper is organized as follows. Section 2 revisits some preliminaries, and the problems of interest are summarized. Section 3 illustrates the degradation of system economic performance under the different scenarios of attacks through complete theoretical analysis. Section 4 derives the optimization model of attack strategy and its corresponding algorithm to find out the solution. The simulation examples and conclusion are appeared in Sections 5 and 6, respectively.

2. Preliminaries

2.1. Graph Theory. A graph $G$ is always used to model the network topology of a system. A graph can be denoted as...
2.2. Stochastic Matrix. A nonnegative square matrix \( M \) is defined as row stochastic matrix if \( \sum_{j} M_{ij} = 1 \), where \( 1 \) is a column vector with all the elements equal to 1. Similarly, a nonnegative square matrix \( N \) is defined as column stochastic matrix if \( \sum_{i} N_{ij} = 1 \), and a nonnegative square matrix \( H \) is double stochastic matrix if it satisfies both \( H1 = 1 \) and \( 1^TH = 1^T \).

Moreover, based on the Perron–Frobenius theorem [18], for a row stochastic matrix \( M \), there exists such an identity column vector \( \mu \) satisfying \( \mu^TM = \mu^T \). Similarly, for a column stochastic matrix \( N \), there also exists an identity column vector \( \xi \) satisfying \( N^T \xi = \xi \).

2.3. Analytic Solution to EDP. The microgrid is essentially a typical multiagent system, in which each generator can be regarded as an agent. The operation cost function of the \( i \)th generation is given by the following quadratic form [19]:

\[
C_i(P_i) = \alpha_i P_i^2 + \beta_i P_i + \gamma_i,
\]

where \( P_i \) is the power generated by generator \( i \) and \( \beta_i, \gamma_i \) and \( \alpha_i > 0 \) are the operation cost parameters of generator \( i \).

Assume there is a microgrid system with \( n \) generators, the objective of the economic dispatch of the microgrid is to minimize the total operation cost, which is given by

\[
\min \sum_{i=1}^{n} C_i(P_i).
\]

The EDP of the microgrid needs to be solved under the power balance constraint and power generation constraint as follows:

\[
\sum_{i=1}^{n} P_i = P_D,
\]

\[
P_i^\text{min} \leq P_i \leq P_i^\text{max}, \quad \text{for } i = 1, 2, 3 \ldots n,
\]

where \( P_i^\text{min} \) and \( P_i^\text{max} \) are the lower bound and upper bound of the output power associated with the \( i \)th generation, respectively. \( P_D \) denotes the total power demand satisfying \( \sum_{i=1}^{n} P_i^\text{min} \leq P_D \leq \sum_{i=1}^{n} P_i^\text{max} \), i.e., the problem is solvable.

The above optimization problem can be solved by the Lagrange multiplier method [20]. The Lagrange multiplier can be expressed as follows:

\[
\lambda_i = \frac{\text{tial} C_i(P_i)}{\text{tial} P_i} = 2\alpha_i P_i + \beta_i.
\]

Because the Lagrange multiplier \( \lambda_i \) is equal to the incremental cost (\( \text{tial} C_i(P_i)/\text{tial} P_i \)), we directly use \( \lambda_i \) to...
represent the incremental cost of units in the following paragraphs.

With the consideration of generation constraint in (4), the power generated by generator $i$ is given by

$$
\begin{align*}
2\alpha_iP_i + \beta_i = \lambda^*, & \quad \text{for } P_i^{\min} \leq P_i \leq P_i^{\max}, \\
2\alpha_iP_i + \beta_i < \lambda^*, & \quad \text{for } P_i = P_i^{\max}, \\
2\alpha_iP_i + \beta_i > \lambda^*, & \quad \text{for } P_i = P_i^{\min},
\end{align*}
$$

(6)

where $\lambda^*$ is the incremental cost corresponding to the optimal solution of the EDP.

2.4. Problems of Interest. Based on a well-developed distributed algorithm to solve the EDP of the smart grid, the main problems we are interested in consist of the following:

1. What is the possible effect of DoS attacks on EDP when the attacker can be detected hardly by the monitor in the smart grid?
2. How to quantify the degradation of economic performance caused by DoS attacks?
3. Does there exist an optimal attack strategy that renders maximum degradation of economic performance caused by the attacker?

3. Performance Analysis of Dispatch System under DoS Attacks

3.1. DoS Attacks’ Model. Assume the DoS attacker is a single source of attacks in the communication network environment of the microgrid, and the DoS attacker sends the invalid requests to occupy the network resources. The DoS attacks target various components including smart meters and communication links, resulting in limited availability of these components. In this paper, the objectives of DoS attacks are to hinder the transmission of information on the communication links, thereby degrading the economic performance of the microgrid.

Stochastic DoS attacks can occur at any communication moment and any communication link. To clearly describe the effect of DoS attacks on the economic dispatch of the microgrid, the model of DoS attacks needs to be established. Define an edge set $U^c(k) \subseteq E$ to represent the communication links attacked at iteration $k$, $k \in \{0, 1, \ldots\}$. The information transmission over the compromised communication links is impeded. The effect of DoS attacks on the communication network is equal to packet dropout, which fails the information transmission among agents. Actually, the communication path $(i, j) \in E$ can be regarded as unconnected if the information transmission on the edge is failed. It is reasonable to assume that the network topology could be time-varying and possibly disconnected when the communication network is attacked by the DoS attacker. In this paper, EDP over unreliable network with DoS attacks is regarded as the EDP under time-varying communication topology. Moreover, we assume that once DoS attacks disappear, any disconnected links caused by attacks will be recovered into the connected state by communication restoration mechanism.

$$
A(k) = [a_{ij}(k)] \in \mathbb{H}^{nn} \text{ is the adjacency matrix corresponding to the communication network topology under DoS attacks at iteration } k. \text{ It can be defined as the following form:}
$$

$$
a_{ij}(k + 1) = \begin{cases} 
0, & (i, j) \in U^c(k + 1), \\
1, & (i, j) \notin U^c(k + 1).
\end{cases}
$$

(7)

The updating matrices $M(k) = [m_{ij}(k)]$, $N(k) = [n_{ij}(k)] \in \mathbb{R}^{nn}$ can be defined according to $A(k)$ as follows:

$$
m_{ij}(k) = \begin{cases} 
\frac{1}{d_i^+(k)}, & j \in N_i^+, \\
0, & \text{otherwise}
\end{cases}, \quad \forall i, j \in V,
$$

(8)

$$
n_{ij}(k) = \begin{cases} 
\frac{1}{d_j^-(k)}, & i \in N_j^-, \\
0, & \text{otherwise},
\end{cases}, \quad \forall i, j \in V.
$$

(9)

It can be deduced that $M(k)$ is a row stochastic matrix and $N(k)$ is a column stochastic matrix.

Lemma 1. Based on the definition, row stochastic matrix $M$ and column stochastic matrix $N$ both have the eigenvalues $1$, and the rest eigenvalues are within the unit circle on the complex plane.

In this paper, a fully distributed algorithm proposed in [20] to solve the EDP of power system can be transformed into the following form with the consideration of DoS attacks:

$$\lambda_i(k + 1) = \sum_{j=1}^{n} m_{ij}(k) \lambda_j(k) + \varepsilon y_i(k), \quad \lambda_i^* > \lambda_i^{\max},
$$

(9)

$$P_i(k + 1) = \begin{cases} 
P_i^{\max}, & \lambda_i^* > \lambda_i^{\max}, \\
\frac{\lambda_i(k + 1) - \beta_i}{2\alpha_i}, & \lambda_i^{\min} \leq \lambda_i^* \leq \lambda_i^{\max}, \\
P_i^{\min}, & \lambda_i^* < \lambda_i^{\min},
\end{cases}
$$

(10)

$$y_i(k + 1) = \sum_{j=1}^{n} n_{ij}(k) y_j(k) - (P_i(k + 1) - P_i(k)), \quad \lambda_i^* > \lambda_i^{\max},
$$

(11)

where $y_i$ is an auxiliary variable which denotes the estimated local power mismatch and $\varepsilon$ is a sufficiently small positive constant named learning gain. $\lambda_i^{\max} = ((P_i^{\max} - \beta_i)/2\alpha_i)$ and $\lambda_i^{\min} = ((P_i^{\min} - \beta_i)/2\alpha_i)$. The distributed algorithms (9)–(11) can solve the economic dispatch problem (2) under constraints (3)–(4). Moreover, the following formula can be derived from (11):
\[ \sum_{i=1}^{n} y_i(k+1) = \sum_{i=1}^{n} \sum_{j=1}^{n} n_{ij}(k) y_i(k) - (P_i(k+1) - P_i(k)) \Longrightarrow \sum_{i=1}^{n} (y_i(k+1) + P_i(k+1)) = \sum_{i=1}^{n} (y_i(k) + P_i(0)) \]

(12)

It is easy to deduce that \( \sum_{i=1}^{n} (P_i(k+1) + y_i(k+1)) = P_D \) will be guaranteed if \( \sum_{i=1}^{n} (P_i(0) + y_i(0)) = P_D \). In other words, the equilibrium between power supply and demand can be guaranteed when the algorithm converges only if the selection of initial value satisfies certain conditions.

Most of the existing literature analyzes the impact of attacks based on the assumption of known attack probabilities [17]. In fact, the probability of an attack is generally not fully grasped by the system [21]. In this paper, we explore the effect of DoS attacks without the knowledge of probability distribution information. To this end, a communication network attacked by the DoS attacker is classified into two types:

1. The communication network topologies keep strongly connected
2. There exist communication network topologies disconnected, i.e., some units are isolated from the communication network

3.2. Strongly Connected Scenario under DoS Attacks. This section investigates the performance analysis of the dispatch system in the scenario which communication topology graphs of the microgrid keep strongly connected under DoS attacks.

Under this attack, the communication topology graphs of the microgrid are time-varying, as shown in Figure 1(a), where the solid line represents the normal connected communication links and the dotted line represents compromised communication links caused by DoS attacks. Although the communication network topology no longer maintains a fixed form under DoS attacks, it still keeps strongly connected. In this case, the distributed economic dispatch algorithm (9)–(11) can be carried out to solve the EDP of the microgrid.

**Theorem 1.** In the scenario of attacks that the communication network topologies keep strongly connected, if the positive constant \( \epsilon \) in algorithm (9)–(11) is sufficiently small and the variables satisfy the initial condition \( \sum_{i=1}^{n} (P_i(0) + y_i(0)) = P_D \), then the distributed algorithm is stable, and all the variables converge to the solution of the EDP, i.e.,

\[ \begin{align*}
\lambda_i(k) & \longrightarrow \lambda^*, \\
P_i(k) & \longrightarrow P^*, \\
y_i(k) & \longrightarrow 0, \quad k \longrightarrow \infty, \forall i \in V.
\end{align*} \]

(13)

**Proof.** Use the eigenvalue perturbation approach [18] to analyze the convergence performance of algorithms (9)–(11). Substituting (9) and (10) into (11), we can obtain

\[ \lambda(k+1) = M(k)\lambda(k) + \epsilon y(k), \]

(14)

\[ y(k+1) = (N(k) - \epsilon B) y(k) + B(I - M(k))\lambda(k), \]

(15)

where \( \lambda \) and \( y \) are the column stack vectors of \( \lambda_i \) and \( y_i \), respectively, \( I \) is an identity matrix, and \( B = \text{diag} \left( \frac{1}{2\alpha_1} \frac{1}{2\alpha_2} \ldots \frac{1}{2\alpha_N} \right) \). Algorithms (14)–(15) can be written in the following form:

\[ \begin{bmatrix}
\lambda(k+1) \\
y(k+1)
\end{bmatrix} = \begin{bmatrix}
M(k) & \epsilon I \\
B(I - M(k)) & N(k) - \epsilon B
\end{bmatrix} \begin{bmatrix}
\lambda(k) \\
y(k)
\end{bmatrix}. \]

(16)

Define \( C(k) = \begin{bmatrix}
M(k) & 0 \\
B(I - M(k)) & N(k)
\end{bmatrix}, \Delta = \begin{bmatrix}
0 & I \\
0 & -B
\end{bmatrix} \)

and updating matrix \( D(k) = \begin{bmatrix}
M(k) & \epsilon I \\
B(I - M(k)) & N(k) - \epsilon B
\end{bmatrix} \)

\[ = C(k) + \epsilon \Delta. \]

The updating matrix \( D(k) \) in (16) can be regarded as \( C(k) \) perturbed by \( \epsilon \Delta \). It is easy to deduce that \( C(k) \) is a lower triangular block matrix with the matrices \( M(k) \) and \( N(k) \) in its diagonal line. As a result, the eigenvalues of \( C(k) \) include that of matrices \( M(k) \) and \( N(k) \). According to Lemma 1, it can be obtained that \( C(k) \) has two eigenvalues \( \eta_1 = \eta_2 = 1 \) at any iteration \( k \).

Assume \( z_1(k) \) and \( x_1(k) \) are left and right eigenvectors of matrix \( C(k) \) with respect to eigenvalues \( \eta_1 \) and \( \eta_2 \), and they satisfy the following conditions:

\[ z_i^T C(k) = z_i^T \eta_i(k), \]

\[ C(k)x_i(k) = \eta_i(k)x_i(k), \]

(17)

\[ z_i^T x_i(k) = 1, \]

\[ z_i^T x_j(k) = 0. \]

According to formula (17), it is not hard to find that \( z_1^T(k) = \begin{bmatrix} 1^T \ B \end{bmatrix} \) and \( z_2^T(k) = \begin{bmatrix} u^T(k) \ 0 \end{bmatrix} \) both are the left eigenvectors of \( C(k) \): \( x_1(k) = \begin{bmatrix} 0^T \ \xi(k)^T \end{bmatrix} \) and \( x_2(k) = \begin{bmatrix} 1^T - \eta \xi(k)^T \end{bmatrix} \) both are the right eigenvectors of \( C(k) \) associated with eigenvalues \( \eta_1 = \eta_2 = 1 \), where \( \eta = \sum_{i=1}^{N} (1/2\alpha_i) \) is defined. If \( \epsilon \neq 0 \), the eigenvalues of \( C(k) \) is perturbed by \( \epsilon \Delta \). According to the eigenvalue derivation theory, the partial derivative of \( \eta_i \) corresponding to \( \epsilon \) can be expressed as follows:

\[ \frac{\partial \eta_i}{\partial \epsilon} = z_i^T(k) D(k) x_i(k). \]

(18)

Thus, it can be deduced that
That means $\nu_1(k) = 1$ does not change with $\varepsilon$, and as $\varepsilon$ goes up, $\nu_2(k)$ goes down from 1. Therefore, there is a small constant $\sigma_1$ satisfying $0 < \varepsilon < \sigma_1$, and $\nu_2(k)$ is restricted to less than 1. Based on the Bauer–Fike theorem [22], there exists an upper bound $\sigma_2$ such that $0 < \varepsilon < \sigma_2$, then $\nu_i(k) < 1$, $i = 3, 4 \ldots 2n$, i.e., other eigenvalues of $C(k)$ lie in the open unit disk. Because the eigenvalues of $D(k)$ = $C(k) + \varepsilon \Delta$ depend on $\varepsilon$, given a constant $\sigma = \min \{\sigma_1, \sigma_2\}$, if $0 < \varepsilon < \sigma$, all the eigenvalues of $D(k)$ are less than 1, except for one eigenvalue equal to 1.

It is not hard to deduce that $[1^T \ 0^T]^T \in \mathbb{H}^{2n}$ is the right eigenvector of $D(k)$ corresponding to $\nu_1(k) = 1$ at any time $k$, i.e., $D(k) \begin{bmatrix} 1 \\ 0 \end{bmatrix}^T = \begin{bmatrix} 1 \\ 0 \end{bmatrix}^T$. The rest of the eigenvalues are within the open unit disk, and matrix $D(k)$ has $2n$ independent eigenvectors.

It is reasonable to assume that the initial value can be expressed as a linear combination of all the eigenvectors as shown in the following:

\[
\begin{bmatrix}
\lambda(0) \\
y(0)
\end{bmatrix} = c_1 \theta_1 + c_2 \theta_2 + \cdots + c_{2n} \theta_{2n},
\]

where $\{c_1, c_2, \ldots c_{2n}\}$ is a set of constants and $\{\theta_1, \theta_2, \ldots \theta_{2n}\}$ is a set of eigenvectors of $D(k)$. According to formula (16), we can obtain

\[
\begin{bmatrix}
\lambda(1) \\
y(1)
\end{bmatrix} = D(0) \begin{bmatrix}
\lambda(0) \\
y(0)
\end{bmatrix} = \nu_1 c_1 \theta_1 + \nu_2 c_2 \theta_2 + \cdots + \nu_{2n} c_{2n} \theta_{2n}.
\]

Thus, it can be deduced that

\[
\begin{bmatrix}
\lambda(k) \\
y(k)
\end{bmatrix} = \prod_{p=1}^{k} D(k-p) \begin{bmatrix}
\lambda(0) \\
y(0)
\end{bmatrix}.
\]

According to the above analysis, because all the eigenvalues of $D(k)$ are less than 1, except for one eigenvalue equal to 1, and the vector $[1^T \ 0^T]^T$ corresponds to the eigenvalue 1. It can be conducted that
3.3. Disconnected Scenario under DoS Attacks. This section investigates the performance analysis of the dispatch system in the scenario that communication topology graphs of the microgrid are disconnected under DoS attacks.

If the DoS attacker concentrates on disconnecting all the communication links of a generator, it will briefly prevent the generator from communicating with its neighbors. Under these attacks, at least one generator is isolated from the communication network. It means the time-varying matrix $A(k)$ has the rows and columns in which all the elements are zero, i.e., the in-degree and out-degree of some vertexes in the communication topology graph are zero. For the convenience of analysis, it is necessary to reduce the dimension of $A(k)$ to obtain $A'(k)$ by removing the rows and columns whose elements are all equal to 0. The corresponding matrices $M(k)$ and $N(k)$ are transformed to $M'(k)$ and $N'(k)$, respectively.

In this scenario, all the generators can be divided into two types, misbehaving generators and well-behaving generators, respectively. Define $A^n(k) \subseteq V$ as the set of misbehaving generators at iteration $k$, i.e., the units isolated from communication network, and $N_n(k) = |A^n(k)|$ is the number of misbehaving generators. It is worth noting that $A^n(k)$ presents isolated generators only due to DoS attacks in unreliable communication network, and isolation of units caused by other abnormal factors is beyond the scope of this paper. If $i \notin A^n(k)$, the generator $i$ is involved in economic dispatch as a well-behaving generator, which updates its output power and incremental cost normally; otherwise, the generator $i$ is a misbehaving generator, which maintains its output power and incremental cost until it is reconnected to the communication network after the disappearance of DoS attacks on it.

Under these attacks, algorithms (9)–(11) can be rewritten as the following dynamics (24)–(26):

\[
\lambda_i(k+1) = \left\{ \begin{array}{ll}
\sum_{j \notin A^n(k)} m^i_{ij}(k) \lambda_j(k) + \varepsilon y_i(k), & i \notin A^n(k), \\
\lambda_i^{\max}, & i \in A^n(k)
\end{array} \right.
\]

\[
P_i(k+1) = \left\{ \begin{array}{ll}
\frac{\lambda_i(k+1) - \beta_i}{2\alpha_i}, & \lambda_i^{\min} \leq \lambda_i \leq \lambda_i^{\max}, \\
P_i^{\min}, & \lambda_i < \lambda_i^{\min}, \lambda_i^{\max}
\end{array} \right.
\]

\[
y_i(k+1) = \left\{ \begin{array}{ll}
\sum_{j \notin A^n(k)} n^i_{ij}(k) y_j(k) - (P_i(k+1) - P_i(k)), & i \notin A^n(k), i \in A^n(k), \\
0, & i \in A^n(k)
\end{array} \right.
\]

\[
\sum_{j \notin A^n(k)} P_i^{\min} \leq P_D - \sum_{j \notin A^n(k)} P_i(k) \leq \sum_{j \notin A^n(k)} P_i^{\max}.
\]
where $\lambda' \neq \lambda^*$ and $P' \neq P^*$ denote the suboptimal incremental cost vector and output power vector of well-behaving generators, respectively, and $\lambda_i$ and $P_i$ denote the incremental cost and output power of the misbehaving generator $i$, respectively. Note that convergence results shown in (28) depend on the attack strategies chosen by the DoS attacker.

Proof. The proof is similar with Theorem 1. The process is omitted here for convenience.

Remark 1. The attacker deliberately causes algorithms (24)–(26) to be executed on the premise that formula (27) is satisfied in the microgrid. As a result, the algorithm converges to a stable but not optimal point as shown in Theorem 2, the attacks will be considered online stealthily [23].

4. Attack Strategy Formulation

4.1. Attack Capacity Formulation. According to the analysis in Section 3.1, DoS attacks can occur at any communication moment and communication link. In practice, the launch of DoS attacks cannot be unrestrained, which is reflected in the constrained attack frequency and attack duration [24]. On the one hand, it is due to the inherent characteristics of DoS attacks, and on the other hand, several technologies of the power system can effectively resist jamming attacks [25]. As a consequence, the DoS attacker needs to formulate an optimal attack strategy on the premise of satisfying its own resource constraints to maximize the attack efficiency and attack effect.

We define the total attack resource as $\Lambda$, and $\delta_n(k)$ is the attack level at iteration $k$, which represents the proportion of isolated units to the total number of units, i.e., $\delta_n(k) = (N_u(k)/n)$, $0 \leq \delta_n(k) \leq 1$. It implies that the more generators that are isolated due to DoS attacks, the higher the attack level the attacks have. Define $\phi = [\phi_k]$, $k \in \{0, 1, \ldots\}$ as the attack decision vector in which $\phi_k$ is the decision of the attacker at iteration $k$, and $\phi_k$ indicates that the attacker decides to jam the wireless channel; otherwise, $\phi_k = 0$. Define $\rho_k(\phi_k, \delta_n(k))$ as the indicator function to represent whether the attacker implements DoS attacks successfully, and the indicator function can be formulated as follows:

$$\rho_k(\phi_k, \delta_n(k)) = \begin{cases} 1, & \phi_k = 1, \delta_n(k) \neq 0, \\ 0, & \text{otherwise}. \end{cases}$$

4.2. Optimal Attack Strategy. The definition of the incremental cost in (5) implies that incremental cost is the value of the operation cost changing with the generated power. The incremental cost can be regarded as an indicator of economic performance for the power system:

$$P_D - \frac{\sum_{i \in A^e(k)} P_i(k) + \sum_{i \in A^m(k)} (\beta / 2a_i)}{\sum_{i \in A^m(k)} (1/2a_i)} - \lambda^*.$$

Thus, the change of incremental cost in the attacks’ situation compared to the ideal situation can be used for a metric to quantify the effect of attacks. On this basis, the problem of designing an optimal attack strategy can be formulated as an optimization problem, for which the optimal solution can be obtained mathematically. This optimization problem aims to maximize the incremental cost deviation. At the same time, in order to ensure the DoS
attacks are online stealthy, the attacker should ensure that all the units can meet the power balance requirement after some units are isolated. Furthermore, the DoS attacker needs to formulate an optimal attack strategy on the premise of satisfying its own resource constraints. In the iteration interval $k \in [k_1, k_2]$, the formulation of an optimal DoS attacks’ strategy can be transformed to the optimization problem as follows:

$$\text{s.t. } \sum_{k=k_1}^{k_2} \phi_k \delta_{\ast,n}(k) \leq \Lambda,$$

(31)

and (27).

The design of optimal strategy is completely reasonable because the purpose of the DoS attacks against economic dispatch process is to violate the economy principle and result in the largest degradation of the economic performance of the microgrid. As shown in previous analysis, $\lambda'$ corresponds to the optimal economic dispatch results without DoS attacks and $\lambda'\ast$ reflects the solution of the EDP under DoS attacks, and the value of $\lambda'$ is related to the attack strategies chosen by the attacker. Therefore, the more $\lambda'$ deviates from $\lambda'\ast$, the worse economic performance of the system can be obtained, and the objective function can be formulated as (30). Moreover, if the attack strategy selected violates the power supply-demand principle in (27), the attacks will be detected easily by the monitoring mechanism in the system, which goes against the intention of the attacker to hide its behaviors. Formula (31) considers the constraint of the attack resources from the practical point of view, and the formulation of attack strategy must be limited by it.

In this paper, the static attack problem is investigated, and the optimal attack strategy is decided before the attack actions begin. However, the solution of the above objective function is inaccessible because the output power of isolated generators is unknown at that time. There are only some static parameters available for the attacker to formulate the attack strategies; thus, we put forward the following assumptions about DoS attacks and reformulate the optimization model according to them.

**Assumption 1.** Attacker can collect pivotal information of the microgrid such as operation cost parameters of generators, power upper and lower limits, and the total power demand. The information can be obtained by monitoring normal process of economic dispatch and collecting the relevant information published by authoritative organizations or manufacturers.

**Assumption 2.** For the objective to maximize the change of incremental cost in the attacks’ situation compared to the ideal situation, the attacker tends to attack the unit when its incremental cost in the attacks’ situation compared to the ideal situation is the highest. Therefore, the more $\lambda'$ deviates from $\lambda'\ast$, the worse economic performance of the microgrid such as operation cost parameters of generators, power upper and lower limits, and the total power demand. The information can be obtained by monitoring normal process of economic dispatch and collecting the relevant information published by authoritative organizations or manufacturers.

**Remark 2.** According to the above analysis, in the nonideal communication environment with DoS attacks, the incremental cost $\lambda'$ obtained by the calculation is related to the selected attack strategy. Because the EDP of the microgrid (2)–(4) is a convex optimization problem, the incremental cost is positively correlated with its corresponding output of the generator, which means that the larger the deviation of $\lambda'$ and $\lambda'\ast$ obtained under different attack strategies, the higher the operation cost of the system is. The above optimal attack strategy models (31)–(33) are essential to increase the operating cost of the system, thereby destroying the economic performance of the microgrid.

Based on the assumption of attack pattern and objective shown above, the attacker pursues an expression of the optimal attack strategy $X\ast$. Reformulate (27) and (30), $\sum_{i \in A''(k)} P_i$ can be replaced by $\sum_{i \in A''(k)} P_{i_{\min}}$, and the optimization problem can be reformulated as follows:

$$X\ast = \arg \max_{A''(k)} \sum_{k=k_1}^{k_2} \rho_k |\lambda' - \lambda'\ast| = \arg \max_{A''(k)} \sum_{k=k_1}^{k_2} \rho_k \left(\frac{P_D - \sum_{i \in A''(k)} P_{i_{\min}} + \sum_{i \in A''(k)} (\beta_i/2\alpha_i) - \lambda'\ast}{\sum_{i \in A''(k)} (1/2\alpha_i)}\right),$$

(32)

$$\text{s.t. } \sum_{i \in A''(k)} P_{i_{\min}} \leq P_D - \sum_{i \in A''(k)} P_{i_{\max}} \leq \sum_{i \in A''(k)} P_{i_{\min}},$$

(33)

where the parameters’ information of (31)–(33) is available in advance, and it means the optimal attack strategy can be decided before the attack actions begin.

4.3. Algorithm to Obtain the Optimal Attack Strategy. The above optimization problem is not a simple convex optimization problem, and it cannot be directly solved by analytical methods or CVX toolbox in MATLAB [26]. As a result, this paper proposes an enumerating-search algorithm to solve the above optimization problem, which is described in Algorithm 1.

The essence of Algorithm 1 is to use the recursive process to exhaustively search for the optimal solution, i.e., the optimal attack strategy which damages the economic performance of the microgrid to the greatest extent. Firstly, enumerate all the possible attack schemes satisfying constraints (31) and (33), where the attack
schemes are represented by the sequence number of the isolated units caused by each attack action. Then, we compute the deviation value of incremental cost corresponding to each attack scheme. By comparing all the deviation value, the attack scheme corresponding to the maximum deviation value is pursued by the DoS attacker. Finally, combine this optimal attack scheme with the attack decision vector $\phi$ [17]. This part is not the focus of the EDP for the microgrid, so it will not be detailed here.

### 5. Simulation Examples

Numerical simulation is a common method to verify theoretical analysis results as well as the effectiveness of the algorithm proposed. In this section, we firstly chose the IEEE 57-bus system to simulate the microgrid to compare the EDP under the different communication situations. Then, on the IEEE 39-bus system, we discuss the effect of DoS attacks adopting various attack strategies on economic performance of the microgrid.

#### Table 1: Parameters of generators.

| $\alpha_i$ | $\beta_i$ | $\gamma_i$ | $P_{i}^{\text{min}}$ (MW) | $P_{i}^{\text{max}}$ (MW) |
|------------|----------|------------|--------------------------|--------------------------|
| 0.001562   | 7.92     | 561        | 150                      | 600                      |
| 0.00194    | 7.85     | 310        | 100                      | 400                      |
| 0.00482    | 7.8      | 300        | 50                       | 200                      |
| 0.00234    | 7.85     | 100        | 100                      | 300                      |
| 0.00312    | 7.88     | 100        | 50                       | 300                      |

#### Table 2: Initialization.

| $\lambda_i(0)$ ($$/\text{MWh}$) | $P_i(0)$ (MW) | $y_i(0)$ (MW) |
|-------------------------------|--------------|--------------|
| 8.8572                        | 300          | 100          |
| 8.82                          | 250          | -100         |
| 8.764                         | 100          | 50           |
| 7.85468                       | 200          | -50          |
| 7.88624                       | 100          | 50           |
5.1. Case 1: The EDP under Ideal Communication Conditions.

There is an IEEE 57-bus system for simulation, and the communication network corresponding to the physical power network is shown in Figure 2. This test system includes five generators, whose parameters and initial state values are listed in Tables 1 and 2, respectively. The total power demand of the system is set to 1000 MW.

In this case, under the ideal communication conditions without DoS attacks, the EDP can be solved with the algorithm proposed in [20]. In the iteration interval $k \in [0, 350]$, the evolution of the output power $P_i$, incremental cost $\lambda_i$, the total power generated $\sum P$, and power demand $P_D$ is shown in Figure 3. Ultimately, the incremental cost $\lambda_i$, $i = 1, \ldots, 5$, converges to a common value $\lambda^* = 8.8183 \$/MWh; meanwhile, the output power $P_1^* = 287.5440$ MW, $P_2^* = 249.5587$ MW, $P_3^* = 105.6315$ MW, $P_4^* = 206.8991$ MW, and $P_5^* = 150.3666$ MW, all the generators are operating within their generation constraints, and also the total power demand is satisfied by these power output. The convergence results of the distributed algorithm are the same as that calculated by the centralized algorithm in [27]. The total operation cost is 9692.8 $$/h, which is the minimum operation cost of the system.

According to the above analysis, the optimal solution of the EDP can be solved through the distributed economic dispatch algorithm under ideal communication conditions. This case can be used as a comparison of the subsequent simulation cases.
5.2. Case 2: The EDP with Strongly Connected Communication Topology under DoS Attacks. Simulation case is performed with the same system model and parameters as those in Section 5.1. In this case, we consider the scenario that communication topology graphs keep strongly connected under DoS attacks. Assuming the communication topology changes two times resulted by DoS attacks, the attacker launches DoS attacks firstly in the communication link (1,3) at iteration \( k \in [50, 100] \); then, the attacker launches DoS attacks in the communication link (1,4) at iteration \( k \in [100, 350] \).

In this case, the EDP can be solved with algorithms (9)–(11). In the iteration interval \( k \in [0, 350] \), the evolution of the output power \( P_i \), incremental cost \( \lambda_i \), the total power generated \( \sum P \), and power demand \( P_D \) is shown in Figure 4.

Ultimately, the incremental cost \( \lambda_i, i = 1, \ldots, 5 \), converges to a common value \( \lambda^* = 8.8183 \$/MWh \) and the output power \( P_1^* = 287.5440 \text{ MW}, P_2^* = 249.5587 \text{ MW}, P_3^* = 105.6315 \text{ MW}, P_4^* = 206.8991 \text{ MW}, \text{ and } P_5^* = 150.3666 \text{ MW} \). It can be concluded that the final convergence results in this case are the same as the results of Case 1.

According to Figure 4, it can be observed that the distributed algorithms (9)–(11) can finally converge to the optimal solution of EDP, although the existences of DoS attacks interfere with the convergence process of the algorithm. As a result, the correctness of the conclusion in Section 3.2 is verified, i.e., this attack scenario where the communication network still keeps strongly connected shows little benefit to the degradation of economic performance of the microgrid.
5.3. Case 3: The EDP with Disconnected Communication Topology under DoS Attacks. Simulation is performed with the same system model and parameters as those in Section 5.1. In this case, we consider the scenario that there exist communication topology graphs disconnected under DoS attacks. If all the communication paths of a generator are attacked for a certain period of time, the generator is briefly isolated from the communication network. It is important to note that the generator will reconnect to the communication network when the attacks disappear.

Assuming the communication topology changes two times because of DoS attacks, the attacker launches DoS attacks on generator 5, firstly, at iteration $k = 50$ until $k = 100$; then, the attacker launches DoS attacks on generator 4 and 5 at iteration $k = 100$ until $k = 350$. In this scenario, these two generators are misbehaving generators because of the DoS attacks on them, which lead to the disconnected communication topology graphs.

In this case, algorithms (24)–(26) are carried out to solve the EDP. The evolution of the output power $P_i$, incremental cost $\lambda_i$, the total power generated $\sum P$, and power demand $P_D$ is shown in Figure 5. Under these DoS attacks, misbehaving generator 5 is isolated from the communication network at the iteration interval $k \in [50, 350]$, and misbehaving generator 4 is isolated at the iteration interval $k \in [100, 350]$, while the output power of the well-behaving generators can still satisfy the power demand remained. The incremental cost $\lambda_i, i = 1, 2, 3$, converge to a common value $\lambda' = 8.8562 \$/MWh, $\lambda_4$ converges to $\lambda_4 = 8.7934 \$/MWh, and $\lambda_5$...
converges to $\lambda_5 = 8.6893 \$/MW. The ultimate generators' output $P_1' = 299.6912$ MW, $P_2' = 259.3390$ MW, $P_3' = 109.5680$ MW, $P_4' = 201.5769$ MW, and $P_5' = 129.6879$ MW. All the generations are operating within their generation constraints, and the total load requirement is satisfied ultimately by generators participating in economic dispatch and the generators isolated. The total operation cost of the system is $9693.5 \$/h$, which is higher than that of Case 1, the economic performance of the system declines.

According to Figure 5 and the total operation cost, it can be observed that the distributed algorithms (24)–(26) cannot finally converge to the optimal solution of the EDP, and the economic dispatch process is disrupted by malicious attacks. It implies the correctness of conclusion in Section 3.3 is verified, i.e., the attack scenario that makes the communication network disconnected leads to the suboptimal solution of the EDP, which degrades the economic performance of the microgrid.

5.4. Case 4: The Optimal Attack Strategy. In this case, we discuss the different attack strategies, which can cause varying degrees of damage to economic performance of the microgrid. We chose the IEEE 39-bus system to simulate the microgrid, and its communication network corresponding to the physical power network is shown in Figure 6. This system includes four generators, whose parameters can be chosen in Table 1. The total power load in the microgrid is set to 500 MW. Assuming the total attack energy $\Lambda = 1$ and attack decision vector $\phi = \{0 \ldots 0 \ 1 \ 0 \ldots 0 \ 1 \ 0 \ldots 0\}$, it is easy to deduce that $\delta_n(k)$ must be smaller than 1/2, which means the number of generators isolated caused by each attack action cannot exceed two for the communication network in Figure 6. Then, the set of attack strategies can be obtained according to constraints (31) and (33).

For the communication network in this case, we can enumerate the set of all attack schemes.

![IEEE 39-bus system](image)
\( X = \{X_1, X_2, \ldots, X_{10}\} \), which include \( X_1 = [1], X_2 = [2], X_3 = [3], X_4 = [4], X_5 = [1, 2], X_6 = [1, 3], X_7 = [1, 4], X_8 = [2, 3], X_9 = [2, 4], \) and \( X_{10} = [3, 4] \); an attack scheme is represented by the serial numbers of the misbehaving generators caused by each attack action. Establishing the objective function and constraints as (31)–(33), the optimization problem can be solved by Algorithm 1, and the calculation results are shown in Figure 7(a). According to Figure 7(a), if \( X_2 = [1, 2] \) is adopted, the deviation of incremental cost will be maximized. It means the execution of the optimal attack strategy \( X^* \) is to repeat the attack scheme \( X_5 = [1, 2] \) at each attack moment. Combining the attack decision vector \( \phi \) and attack schemes, different attack strategies can be obtained. The comparison of different attack strategies is shown in Figure 7(b), from which we can easily sum up that optimal attack strategy obtained by using Algorithm 1 indeed causes the most degradation of economic performance compared with other attack strategies. As a result, it is feasible to carry out the proposed enumerating-search algorithm to obtain the optimal attack strategy.

6. Conclusion

This paper considers an optimal attack strategy against the economic dispatch for the microgrid. Firstly, according to the operating principle of DoS attacks, the unreliable communication network under DoS attacks can be classified into two scenarios, i.e., disconnected and strongly connected scenarios. The theoretical analysis results show that economy performance of the microgrid is damaged in the former case. On this basis, the optimal DoS attack strategy considering the resource constraints of the attacker is formulated to maximize the effect of attacks, which can be obtained by using the enumerating-search algorithm. Finally, the correctness of the theoretical analysis results with respect to the effect of attacks is verified by the simulations on the IEEE 57-bus system, and the effectiveness of the proposed enumerating-search-based optimal attack strategy is illustrated through the simulations on the IEEE 39-bus system. This paper delivers the message that, besides the efforts of designing novel distributed economic dispatch algorithms to guarantee the economic operation for the microgrid, it is equally important to protect the economic dispatch process from malicious attacks and evade potential economic losses.

For the future work, how to build the rational model of DoS attacks is the key to solving the EDP of the energy system under DoS attacks. Furthermore, we will synthetically consider the impact of other attacks on the EDP, such as false data injection attacks and replay attacks. Moreover, research on the dynamic optimal attack strategy disrupting the economic dispatch of the energy system is also the focus of our future work.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.
Acknowledgments

This work was supported partly by the National Key R&D Program of China under Grant 2018YFA0702200, Fundamental Research Funds for the Central Universities (N2004005), and Science and Technology Project of State Grid Corporation of China (2020YF-19).

References

[1] B. Huang, L. Liu, H. Zhang, Y. Li, and Q. Sun, “Distributed optimal economic dispatch for microgrids considering communication delays,” IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 49, no. 8, pp. 1634–1642, 2019.

[2] R. Wang, Q. Sun, W. Hu, Y. Li, D. Ma, and P. Wang, “SoC-based droop coefficients stability region analysis of the battery for stand-alone supply systems with constant power loads,” IEEE Transactions on Power Electronics, vol. 36, no. 7, p. 7866, 2021.

[3] H. Li, Z. Wang, G. Chen, and Z. Y. Dong, “Distributed robust algorithm for economic dispatch in smart grids over general unbalanced directed networks,” IEEE Transactions on Industrial Informatics, vol. 16, no. 7, pp. 4322–4332, 2020.

[4] W. Hu, C. Ruan, H. Nian, and D. Sun, “Zero-sequence current suppression strategy with common-mode voltage control for open-end winding PMSM drives with common DC bus,” IEEE Transactions on Industrial Electronics, vol. 68, no. 6, p. 4691, 2021.

[5] J. Zhang, J. Zhang, F. Zhang, M. Chi, and L. Wan, “An improved symbiosis particle swarm optimization for solving economic load dispatch problem,” Journal of Electrical and Computer Engineering, vol. 2021, Article ID 8869477, 11 pages, 2021.

[6] J. B. Park, Y. W. Jeong, and J. R. Shin, “An improved particle swarm optimization for nonconvex economic dispatch problems,” IEEE Transactions on Power Systems, vol. 25, no. 1, pp. 156–166, 2020.

[7] A. Cherukuri and J. Cortés, “Initialization-free distributed coordination for economic dispatch under varying loads and generator commitment,” Automatica, vol. 74, pp. 183–193, 2016.

[8] Z. Fu, X. He, T. Huang, and H. Abu-Rub, “A distributed continuous time consensus algorithm for maximizing social welfare in micro grid,” Journal of the Franklin Institute, vol. 353, no. 15, pp. 3966–3984, 2016.

[9] Y. Li, W. Gao, G. Wei, H. Zhang, and J. Zhou, “A distributed doublenewton descent algorithm for cooperative energy management of multiple energy bodies in energy internet,” IEEE Transactions on Industrial Informatics, vol. 1, p. 1, 2020.

[10] H. Li and T. Huang, “Convergence analysis of a distributed optimization algorithm with a general unbalanced directed communication network,” IEEE Transactions on Network Science and Engineering, vol. 6, no. 3, pp. 237–248, 2018.

[11] D. Ding, Q.-L. Han, Y. Xiang, X. Ge, and X.-M. Zhang, “A survey on security control and attack detection for industrial cyber-physical systems,” Neurocomputing, vol. 275, no. 10, pp. 1674–1683, 2018.

[12] E. Hammad, A. Farraj, and D. Kundur, “On cyber-physical coupling and distributed control in smart grids,” IEEE Transactions on Industrial Informatics, vol. 15, no. 8, pp. 4418–4429, 2019.

[13] W. Xu, D. W. C. Ho, J. Zhong, and B. Chen, “Event/self-triggered control for leader-following consensus over unreliable network with DoS attacks,” IEEE Transactions on Neural Networks and Learning Systems, vol. 30, no. 10, pp. 3137–3149, 2019.

[14] P. Li, Y. Liu, H. Xin, and X. Jiang, “A robust distributed economic dispatch strategy of virtual power plant under cyber-attacks,” IEEE Transactions on Industrial Informatics, vol. 14, no. 10, pp. 4343–4352, 2018.

[15] D. Zhang and G. Feng, “A new switched system approach to leader-F follower consensus of heterogeneous linear multiagent systems with DoS attack,” IEEE Transactions on Systems, Man and Cybernetics, vol. 99, pp. 1–9, 2019.

[16] C. Yang, X. Ren, W. Yang, H. Shi, and L. Shi, “Jamming attack in centralized state estimation,” in Proceedings of the 2015 34th Chinese Control Conference (CCC), pp. 6530–6535, Hangzhou, Zhejiang, China, July 2015.

[17] H. Zhang, Y. Qi, J. Wu, L. Fu, and L. He, “DoS attack energy management against remote state estimation,” IEEE Transactions on Control of Network Systems, vol. 5, no. 1, pp. 383–394, 2018.

[18] Z. Zhang and M.-Y. Chow, “Convergence analysis of the incremental cost consensus algorithm under different communication network topologies in a smart grid,” IEEE Transactions on Power Systems, vol. 27, no. 4, pp. 1761–1768, 2012.

[19] B. Huang, L. Liu, Y. Li, and H. Zhang, “Distributed optimal energy management for microgrids in the presence of time-varying communication delays,” IEEE Access, vol. 7, pp. 83702–83712, 2019.

[20] S. Yang, S. Tan, and J.-X. Xu, “Consensus based approach for economic dispatch problem in a smart grid,” IEEE Transactions on Power Systems, vol. 28, no. 4, pp. 4416–4426, 2013.

[21] S. Liu, Z. Hu, X. Wang, and L. Wu, “Stochastic stability analysis and control of secondary frequency regulation for islanded microgrids under Random denial of service attacks,” IEEE Transactions on Industrial Informatics, vol. 15, no. 7, pp. 4066–4075, 2019.

[22] F. L. Bauer and C. T. Fike, “Norms and exclusion theorems,” Numerische Mathematik, vol. 2, no. 1, pp. 137–141, 1960.

[23] C. Zhao, J. He, P. Cheng, and J. Chen, “Analysis of consensus-based distributed economic dispatch under stealthy attacks,” IEEE Transactions on Industrial Electronics, vol. 64, no. 6, pp. 5107–5117, 2017.

[24] C. De Persis and P. Tesi, “Input-to-state stabilizing control under denial-of-service,” IEEE Transactions on Automatic Control, vol. 60, no. 11, pp. 2930–2944, 2015.

[25] W. Xu, K. Ma, W. Trappe, and Y. Zhang, “Jamming sensor networks: attack and defense strategies,” Network IEEE, vol. 20, no. 3, pp. 41–47, 2006.

[26] D. A. Guimarães, G. H. F. Floriano, and L. S. Chaves, “A tutorial on the CVX system for modeling and solving convex optimization problems,” IEEE Latin America Transactions, vol. 13, no. 5, pp. 1228–1257, 2015.

[27] A. J. Wood and B. F. Wollenberg, Power Generation, Operation, and Control, Wiley-Interscience, New York, NY, USA, 1996.