Analysis of Consensus-Based Distributed Economic Dispatch Under Stealthy Attacks

Chengcheng Zhao, *Student Member, IEEE*, Jianping He, *Member, IEEE*, Peng Cheng, *Member, IEEE*, and Jiming Chen, *Senior Member, IEEE*

***Abstract*—In a smart grid, distributed energy management (DEM) is a promising approach to realize reliable and efficient operation. Since cyberattack is one of the crucial threats faced by smart grid, the investigation of the effect of cyberattacks on DEM is both a theoretical merit and a practical value. This paper considers the typical DEM problem, i.e., distributed economic dispatch (ED) problem, under attacks. Under a well-developed consensus-based ED protocol, we first define the stealthy attack through false data injection for offline and online cases, respectively. The necessary and sufficient conditions are provided to guarantee convergence of the algorithm when the attacker only injects false data into the broadcast information. And the offline stealthy attack can be realized under this kind of attack. Then, we prove that there exists no stealthy attack injecting false data into the broadcast information for the online case. Further, we provide the stealthy attack by merely injecting constant false data into generation cost parameters for the online case. We also prove that for every node, there exists false data injection into generation cost parameters, which reduces the generation efficiency. Simulation studies validate the theoretical results.**

***Index Terms*—Consensus, distributed energy management (DEM), economic dispatch (ED), smart grid, stealthy attacks.**

I. Introduction

INTEGRATED with smart infrastructures, communication architectures, advanced control technologies, etc., a smart grid is expected to be much more efficient and reliable [1], [2] compared with the traditional power grid. Due to the existence of intelligent controllable electrical devices and advanced communication networks [3], distributed control and optimization [4] become possible and also desirable in a smart grid [5], [6]. Compared with the conventional centralized approach, the distributed one will be more scalable and robust, which is more applicable for smart grid. Especially, distributed energy management (DEM) is a critical and notable problem in the operation of a smart grid [7].

Owing to the high integration of communication constructions [8], cyberattack [9] is becoming one of the most challenging problems faced by a smart grid [10]. The existing control and optimization algorithms without considering cyberattacks may admit the attacker penetrating the power grid and then attaining access to the control software, which can destabilize the grid in unforeseeable ways [11]. A great amount of work has been done for the state estimation under cyberattacks in electric power grids and most of these analysis and designs are given from the perspective of distributed controls [12], [13]. For DEM problems, which rely on distributed optimizations, only few efforts regarding cyberattacks have been accomplished. In [14], the vulnerability of the incremental cost consensus (ICC) algorithm, which is designed to solve the Economic Dispatch (ED) problem, was investigated under attacks and a reputation-based detection algorithm was provided. However, the ICC algorithm needs a centralized unit and is only effective for undirected topologies. Duan *et al.* analyzed how the distributed DC optimal power flow (DC-OPF) algorithm behaves under integrity attacks [15], where equality constraints are decentralized naturally.

In state estimation, false data injection means that by manipulating the measurements, the attacker knowing the system configuration information can introduce errors into certain state variables without being detected by existing algorithms [16]. Stealthy false data injection attacks have been widely studied for the networked control system [17], [18]. Considering the attacker has the property of stealthiness, we define the similar cyberattacks for DEM. Seeing that DEM optimization problems cannot be unified simply, to investigate the stealthy attack for DEM, we consider a representative and significant problem, i.e., ED. Distributed ED is used to allocate multiple generation units to meet the expected demand, while minimizing the total generation cost in a distributed way [19]. As there exists a global equality constraint for the balance between the generation and demand, which cannot be decoupled easily, distributed ED behaves differently from distributed DC-OPF under attacks.

Since high efficiency is an important feature of smart grid [1] and the attacker that makes the total generation cost larger than the optimal one in ED can decrease energy efficiency, it is meaningful and practical for the attacker to increase the

Manuscript received May 31, 2016; revised August 12, 2016 and October 15, 2016; accepted October 30, 2016. Date of publication December 9, 2016; date of current version May 10, 2017. This work was supported in part by the National Natural Science Foundation of China under Grant 61429301 and Grant 61503332 and in part by the National Key R&D Program under Grant 2016YFB0800204. *(Corresponding author: Jiming Chen.)*

C. Zhao, P. Cheng, and J. Chen are with the State Key Laboratory of Industrial Control Technology and Innovation Joint Research Center for Industrial Cyber Physical Systems, Zhejiang University, Hangzhou 310027, China (e-mail: zccsq90@gmail.com; pcheng@iipc.zju.edu.cn; jmchen@ieee.org).

J. He is with the Department of Automation, Shanghai Jiao Tong University, Shanghai 200240, China (e-mail: jianpinghe.zju@gmail.com).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIE.2016.2638400

total generation cost. Usually, ED is realized every 5 min or longer according to the generation prediction and load condition [20], which means the ED algorithm implementation is offline. When the distributed ED algorithm is executed offline, if all agents achieve seemingly satisfactory final state under attacks but the imbalance between the generation and demand occurs, the attacker cannot be detected. Accordingly, such attacks are undetectable and the power system may become unstable in the future. Due to the volatility and intermittent of the renewable energy resources, real-time ED, i.e., the scheduling is fulfilled online, is also needed for smart grid [21]. For the online case, since the power mismatch can be estimated by frequency measurements [22], the attack causing the imbalance between the generation and demand can be detected easily. Hence, whether the attacker can make the total generation cost increase while keeping the generation and demand balanced is an interesting problem. Meanwhile, how the attacker can manipulate its state to introduce high total generation cost is also attractive.

Different distributed ED algorithms have been proposed for different performance objectives including low computation complexity, high speed, etc. Usually, these algorithms are nonlinear, which makes the performance analysis of the algorithm under cyberattacks difficult. As an efficient distributed computing method [23]–[26], consensus-based algorithms have attracted significant research interests for solving the ED problem [27]–[32]. The consensus-based ED algorithm, which can be simplified as a linear system for the iteration process, makes the analysis tractable. Considering the fully distributed consensus-based ED algorithm for directed communication topologies proposed in [29], we define stealthy attacks for the online and offline cases under attacks and then analyze influence of the stealthy attack on the algorithm. The main contributions of this paper are summarized as follows.

1) We consider how the consensus-based ED algorithm proposed in [29] behaves under stealthy attacks. To the best of our knowledge, the formulated problem is novel and practical.
2) We derive the necessary and sufficient conditions to guarantee the convergence of the algorithm under attacks only injecting false data into the broadcast information.
3) We prove that the offline stealthy attack can be realized and the online stealthy attack does not exist if the attacker only injects false data into the broadcast information.
4) We provide an online stealthy attack by merely injecting constant false data into generation cost parameters. The existence of generation cost parameters manipulation that will reduce the generation efficiency is proved.

The remainder of this paper is organized as follows. In Section II, the problem of the consensus-based ED algorithm under attacks is formulated. Section III analyzes the convergence, feasibility, and optimality of the consensus-based algorithm under attacks that only injects false data into the broadcast information. Section IV provides the stealthy attack injecting constant false data into the generation cost parameters. Simulations are presented in Section V to verify the obtained results. Finally, Section VI concludes this paper.

II. Preliminaries and Problem Formulation

Considering a power grid with $N \geq 3$ agents indexed by $1, 2, \ldots, N$, we assume that each agent owning certain amount of demand can control a generation unit locally. A directed strongly connected graph $G = \{V, E\}$ is used to represent the communication topology of the network, where V is the set of N nodes and $E \subset V \times V$ is the edge set. It is noted that $(j, i) \in E$ if and only if (iff) node i can receive information from node j, and node j is the in-neighbor of node i. The in-neighbor set of node i is defined as $N_i^+ = \{j | (j, i) \in E, j \neq i\}$ and $|N_i^+|$ is the cardinality. Meanwhile, we represent the out-neighbor set of node i as $N_i^- = \{j | (i, j) \in E, j \neq i\}$ and $|N_i^-|$ is the cardinality. Self-loop is not considered here, i.e., $(i, i) \notin E, \forall i \in V$.

A. Preliminaries of Consensus

We introduce a row stochastic matrix $W = [w_{ij}]$ and a column stochastic matrix $Q = [q_{ij}]$, whose elements are as follows:

$$w_{ij} = \begin{cases} \frac{1}{|N_i^+|+1}, j \in N_i^+ \\ 1 - \sum\limits_{j \in N_i^+} w_{ij}, j = i \\ 0, j \notin N_i^+, j \neq i \end{cases}, \quad q_{ij} = \begin{cases} \frac{1}{|N_j^-|+1}, j \in N_i^+ \\ 1 - \sum\limits_{j \in N_i^-} q_{ji}, j = i \\ 0, j \notin N_i^+, j \neq i \end{cases}.$$

Let $x(k) = [x_1(k), \ldots, x_N(k)]^{\mathrm{T}}$ denote the state vector of all nodes in G at iteration $k, k \in \{1, 2, \ldots\}$. Given any initial state $x(0)$, we can obtain the following two lemmas [24].

Lemma 1 (Consensus): If G is a strongly connected graph, under the consensus algorithm $x(k+1) = Wx(k)$, then there holds that $\lim\limits_{k \to \infty} x_i(k) = c, \forall i \in V$, where c is a constant.

Lemma 2 (Ratio consensus): If G is a strongly connected graph, under the ratio consensus algorithm $x(k+1) = Qx(k)$, then there holds that $\lim\limits_{k \to \infty} x_i(k) = \varpi_i \sum_{i=1}^{N} x_i(0), \forall i \in V$, where ϖ_i is the ith element of the normalized right eigenvector corresponding to eigenvalue 1.

Note that under Lemma 2, the state of each node will converge to a stable value and the sum of all states will not change during the iteration process. For general weight settings for all edges, which guarantee the row and column stochasticity of W and Q, respectively, the above lemmas will always hold.

B. Distributed ED

In the network-enabled distributed power grid, the aim of ED is to improve the generation efficiency by minimizing the total generation cost without considering transmission line thermal limits. The details are given as follows.

Dividing a day into T time periods, the length of each period is constant (for example, 5 min). In each period $t, t \in \{1, 2, \ldots, T\}$, the agents aim to minimize their total generation cost as well as achieving the balance between the generation and demand simultaneously through local communications. For each agent $i, i \in V$, the generating power is represented as P_i with lower (upper) bound denoted by P_i^m (P_i^M). The cost $C_i(P_i)$ of agent i can be denoted as the quadratic function of

P_i, i.e.,

$$C_i(P_i) = a_i P_i^2 + b_i P_i + c_i$$

where a_i, b_i, and c_i are the fitting parameters of generation unit i. To make the notations simple, we transform the cost function as

$$C_i(P_i) = \frac{(P_i - \alpha_i)^2}{2\beta_i} + \gamma_i, i \in V$$

where $\beta_i = \frac{1}{2a_i}$, $\alpha_i = \frac{-b_i}{2a_i}$, and $\gamma_i = c_i - \frac{b_i^2}{4a_i}$. Then ED problem is formulated as

$$\min \sum_{i\in V} C_i(P_i) \tag{1a}$$

$$\text{s.t.} \sum_{i\in V} P_i = \sum_{i\in V} d_i \tag{1b}$$

$$P_i^m \le P_i \le P_i^M, i \in V \tag{1c}$$

where $d_i, i \in V$, is the local load known by agent i. Denote the incremental cost of generation unit i by λ_i, i.e, $\lambda_i = \frac{dC_i(P_i)}{dP_i}$. We represent $\lambda_i^M = 2a_i P_i^M + b_i$ and $\lambda_i^m = 2a_i P_i^m + b_i$, which will be used in the iteration of $P_i(k)$. The consensus-based algorithm under no attack can be described as $\forall i \in V$

$$\begin{cases} \lambda_i(k+1) = \sum_{j\in V} w_{ij}\lambda_j(k) + \varepsilon\xi_i(k) \\ P_i(k+1) = \begin{cases} P_i^M, & \lambda_i(k+1) \ge \lambda_i^M \\ \beta_i\lambda_i(k+1) + \alpha_i, & \lambda_i^m < \lambda_i(k+1) < \lambda_i^M \\ P_i^m, & \lambda_i(k+1) \le \lambda_i^m \end{cases} \\ \xi_i(k+1) = \sum_{j\in V} q_{ij}\xi_j(k) - (P_i(k+1) - P_i(k)) \end{cases} \tag{2}$$

where ξ_i is the local power mismatch estimated by node $i, \forall i \in V$. As variables ξ_i and λ_i will be broadcast to neighbors of node i, we depict ξ_i's and λ_i's as the broadcast information. β_i's and α_i's are the named generation cost parameters. If each agent $i \in V$ initializes its state as follows:

$$\begin{cases} P_i(0) = \begin{cases} P_i^m, & d_i \le P_i^m \\ d_i, & P_i^m < d_i < P_i^M \\ P_i^M, & P_i^M \le d_i \end{cases} \\ \lambda_i(0) = 2a_i P_i(0) + b_i \\ \xi_i(0) = d_i - P_i(0) \end{cases} \tag{3}$$

the algorithm in (2) can achieve the optimal solution of the ED problem in (1) distributedly. Here, ε is the learning gain parameter, which is critical for convergence of the algorithm in (2), as shown in the following Lemma [29].

Lemma 3: Under the algorithm in (2) with initialization in (3), if the network is strongly connected, there exists a small $\bar{\varepsilon} > 0$, when $0 < \varepsilon < \bar{\varepsilon}$, the algorithm in (2) can achieve the optimal solution of the problem in (1), i.e.,

$$\lim_{k\to\infty} \lambda_i(k) = \lambda^*, \lim_{k\to\infty} P_i(k) = P_i^*, \lim_{k\to\infty} \xi_i(k) = 0, i \in V$$

where $P_i^*, \forall i \in V$ and λ^* are optimal power and optimal Lagrangian multiplier, respectively.

C. Distributed ED Under Attacks

The nodes manipulated by the attacker are called attack nodes and attack nodes can inject false data into state variables, i.e., $\lambda_i(k)$, $\xi_i(k)$, and $P_i(k)$, where i is an attack node. When each node i cannot know neighbors' information P_j^m and $P_j^M, \forall j \in N_i$ and attack nodes can ignore the lower and upper bound of generation power, the false data injected by the attack node j to $P_j(k)$ can be any value in R. Thus, we provide a rather general form of the attack to $P(k)$ to make the problem clear and general, i.e., the algorithm in (2) under attacks can be modeled as $\forall i \in V$

$$\begin{cases} \lambda_i(k+1) = \sum_{j\in V} w_{ij}\lambda_j(k) + \varepsilon\xi_i(k) + \bar{u}_i^{\lambda}(k) \\ P_i(k+1) = \bar{u}_i^{P}(k) \\ \xi_i(k+1) = \sum_{j\in V} q_{ij}\xi_j(k) - (P_i(k+1) - P_i(k)) + \bar{u}_i^{\xi}(k) \end{cases} \tag{4}$$

where when i is an attack node, $\bar{u}_i^{\lambda}(k)$, $\bar{u}_i^{P}(k)$, and $\bar{u}_i^{\xi}(k)$ can be any value in R. Otherwise, $\bar{u}_i^{\lambda}(k) \equiv 0$, $\bar{u}_i^{\xi}(k) \equiv 0$, and $\bar{u}_i^{P}(k)$ follows the second equation in (2).

From (4), we observe that the attacker can ruin the convergence of the algorithm easily by making Lemma 3 invalid. However, breaking the convergence or the balance between the generation and demand will make the attacker exposed to the system operator or agents. Suppose that when the algorithm in (4) is executed offline, the attack making (4) divergence can be detected. Meanwhile, when executing (4) online, the divergence or the imbalance between the generation and demand can be detected by agents through the frequency deviation. The stealthy attacks for offline and online cases are defined as follows.

Definition 1: Under the algorithm in (4), if the attack makes the algorithm converge to a stable but not optimal point, i.e.,

$$\lim_{k\to\infty} \lambda_i(k) = \lambda^a, \lim_{k\to\infty} P_i(k) = P_i^a, \lim_{k\to\infty} \xi_i(k) = 0, i \in V$$

where $\lambda^a \ne \lambda^*$ is a constant and $P_i^a, \forall i \in V$ is constant, the attack is offline stealthy.

For the offline ED problem, as long as all incremental cost $\lambda_i(k)$'s converge to a common constant and all local power mismatch $\xi_i(k)$'s converge to zero, each safe agent would think that the cooperation achieves optimality. However, there may exist some stable final point that is not optimal or even not feasible. Thereby, the imbalance between the generation and demand may occur in the future. How to guarantee the convergence of the distributed algorithm (4) is a difficult problem because there is a nonlinear iteration process for the local power $P_i(k)$ and lots of variables can be manipulated.

Definition 2: Under the algorithm in (4), if the attack can make the algorithm converge to a stable, feasible but not optimal point, i.e.,

$$\lim_{k\to\infty} \lambda_i(k) = \lambda^a, \lim_{k\to\infty} P_i(k) = P_i^a, \lim_{k\to\infty} \xi_i(k) = 0, i \in V$$

where $\lambda^a \ne \lambda^*$ is a constant and $\sum_{j\in V} P_i^a = \sum_{j\in V} d_i$, the attack is online stealthy.

For the online ED problem, the global coupling equality constraint must hold. Note that the consensus-based algorithm is designed to converge to the optimal solution starting from the infeasible point, which implies that the global coupling

constraint does not hold for the initial point. Thus, it is difficult to guarantee the feasibility of the final point by one or more attack nodes through false data injection. Hence, if there exists false data injection, whether the algorithm in (4) can achieve convergence and how to ensure the feasibility of the final point while ruin the optimality are challenging and open problems.

Therefore, whether the attack can reduce the efficiency of ED in a stealthy way for online and offline cases, respectively, is an interesting problem. If there exists the stealthy attack, how much the attack node can drag the final point from the optimal one is also noteworthy. To solve these problems, we first provide the necessary and sufficient conditions for the convergence of the algorithm in (4) and the offline stealthy attack is achieved. Then, we propose that the online stealthy attack can be fulfilled by injecting false data into generation cost function parameters.

III. Stealthy Attacks to the Broadcast Information

Considering the attacker injecting false data into the broadcast information [33], we analyze how the convergence of (4) can be guaranteed for the unbounded generation case and then generalize it to the bounded one.

A. Unbounded Generation Cases

Here, we first consider the problem in (1) without inequality constraints (1c) that is important for the analysis of the problem in (1). As attack node i only injects the false data into $\lambda_i(k)$'s and $\xi_i(k)$'s, the algorithm in (4) can be transformed as

$$\begin{bmatrix}\lambda(k+1)\\ \xi(k+1)\end{bmatrix}=\begin{bmatrix}W & \varepsilon I\\ B(I-W) & Q-\varepsilon I\end{bmatrix}\begin{bmatrix}\lambda(k)\\ \xi(k)\end{bmatrix}+\begin{bmatrix}u^{\lambda}(k)\\ u^{\xi}(k)\end{bmatrix} \tag{5}$$

where $B\in R^{N\times N}$ is a diagonal matrix with $B_{ii}=\beta_i,\forall i\in V$, and $u^{\lambda}(k)=[u_1^{\lambda}(k),\ldots,u_N^{\lambda}(k)]^{\mathrm{T}}$ and $u^{\xi}(k)=[u_1^{\xi}(k),\ldots,u_N^{\xi}(k)]^{\mathrm{T}}$ represent false data vector for $\lambda(k)$, and $\xi(k)$, respectively. At the same time, there holds $u_i^{\lambda}(k)\equiv u_i^{\xi}(k)\equiv 0$ iff node i is not an attack node.

Before providing the necessary and sufficient conditions for the convergence of the system in (5), we present the following necessary and sufficient condition for the initialization. The analysis in this paper is established on this condition and Lemma 3.

Lemma 4: Iff there holds

$$\sum_{i\in V}\xi_i(0)+\sum_{i\in V}P_i(0)=\sum_{i\in V}d_i \tag{6}$$

the algorithm in (2) can achieve a feasible point of the problem in (1).

Proof: According to the algorithm in (2), there holds

$$\sum_{i\in V}\xi_i(k+1)+\sum_{i\in V}P_i(k+1)=\sum_{i\in V}\xi_i(k)+\sum_{i\in V}P_i(k). \tag{7}$$

Since the algorithm will converge and the final point will satisfy $\lim_{k\to\infty}\xi_i(k)=0,\forall i\in V$, we have $\lim_{k\to\infty}\sum_{i\in V}P_i(k)=\sum_{i\in V}\xi_i(0)+\sum_{i\in V}P_i(0)=\sum_{i\in V}d_i$. Accordingly, the final point is feasible under condition (6) that concludes the sufficiency.

Then, we prove the necessity. As the final point is feasible and (7) holds, we have $\lim_{k\to\infty}\sum_{i\in V}P_i(k)=\sum_{i\in V}\xi_i(0)+\sum_{i\in V}P_i(0)$. Since the final point is feasible, there holds $\lim_{k\to\infty}\sum_{i\in V}P_i(k)=\sum_{i\in V}d_i$. As a result, we can obtain $\sum_{i\in V}\xi_i(0)+\sum_{i\in V}P_i(0)=\sum_{i\in V}d_i$. ■

Although the system matrix in (5) is different from that in [34] and [35], it has a simple largest eigenvalue 1 while all other eigenvalues lie in the open unit disk. As a consequence, we can generalize results in [34] and [35] and obtain the following necessary and sufficient condition for the convergence of the system in (5).

Lemma 5: If the system (5) can achieve asymptotic convergence, i.e.,

$$\lim_{k\to\infty}\lambda_i(k)=\bar{\lambda}^*,\lim_{k\to\infty}\xi_(k)=0,\forall i\in V \tag{8}$$

where $\bar{\lambda}^*$ is a constant, then there holds

$$\lim_{k\to\infty}\begin{bmatrix}u^{\lambda}(k)\\ u^{\xi}(k)\end{bmatrix}=\mathbf{0}. \tag{9}$$

Since the proof of Lemma 5 can be obtained simply through contradiction, we omit it here.

Lemma 6: If there exists a constant H such that

$$\sum_{k=0}^{\infty}|u_i^{\lambda}(k)|\le H,\sum_{k=0}^{\infty}|u_i^{\xi}(k)|\le H,i\in V \tag{10}$$

then the system in (5) achieves asymptotic convergence, i.e.,

$$\lim_{k\to\infty}\lambda_i(k)=\bar{\lambda}^*,\lim_{k\to\infty}\xi_(k)=0,\forall i\in V. \tag{11}$$

Proof: For simplification, we give the following notation, $A=\begin{bmatrix}W & \varepsilon I\\ \beta(I-W) & Q-\varepsilon I\end{bmatrix}$, $x(k)=\begin{bmatrix}\lambda(k)\\ \xi(k)\end{bmatrix}$, and $u(k)=\begin{bmatrix}u^{\lambda}(k)\\ u^{\xi}(k)\end{bmatrix}$. Then, we have

$$\begin{aligned}x(k+1)&=Ax(k)+u(k)\\&=A^{k+1}x(0)+A^ku(0)+\cdots+A^0u(k)\\&=A^{k+1}x(0)+\sum_{t=0}^{k}A^{k-t}u(t).\end{aligned} \tag{12}$$

As A has a simple eigenvalue 1 and all other eigenvalues lie in the open unit disk, by referring to Theorem 2 in [35], $\lim_{k\to\infty}\sum_{t=0}^{\infty}A^{k-t}u(t)$ will converge to the eigenvector corresponding to eigenvalue 1. As the eigenvector of A corresponding to eigenvalue 1 has the form ve, where $v>0$ is a constant, and $e=[1,\ldots,1,0,\ldots,0]^{\mathrm{T}}\in R^{2N\times 1}$ with N elements equal to 1 and N elements equal to 0, we have

$$\lim_{k\to\infty}\sum_{t=0}^{\infty}A^{k-t}u(t)=ce. \tag{13}$$

where c is a constant. Meanwhile, according to Lemma 3, there holds

$$\lim_{k\to\infty}A^{k+1}x(0)=\lambda^*e. \tag{14}$$

From (13) and (14), it can be obtained that the final value of (5) will achieve convergence, i.e.,

$$\lim_{k\to\infty} x(k) = ce + \lambda^* e.$$

■

Theorem 1: If (10) is satisfied, (5) can achieve asymptotic convergence and the final point satisfies

$$\lim_{k\to\infty} \lambda_i(k) = \frac{\sum_{i\in V} d_i + \lim_{k\to\infty} \sum_{j=0}^{k} \sum_{i\in V} u_i^{\xi}(j) - \sum_{i\in V} \alpha_i}{\sum_{i\in V} \beta_i} \quad \forall i \in V. \tag{15}$$

Proof: Due to (6), convergence of (5) can be guaranteed if (10) holds. According to the iteration rule for $\xi_i(k)$ in (5), by summing up all $\xi_i(k)$ for all $i \in V$, one obtains

$$\begin{aligned}
&\sum_{i\in V} \xi_i(k+1) + \sum_{i\in V} P_i(k+1) \\
&= \sum_{i\in V} \xi_i(k) + \sum_{i\in V} P_i(k) + \sum_{i\in V} u_i^{\xi}(k) \\
&= \sum_{i\in V} \xi_i(k-1) + \sum_{i\in V} P_i(k-1) + \sum_{i\in V} u_i^{\xi}(k-1) \\
&\quad + \sum_{i\in V} u_i^{\xi}(k) \\
&= \sum_{i\in V} \xi_i(0) + \sum_{i\in V} P_i(0) + \sum_{j=0}^{k} \sum_{i\in V} u_i^{\xi}(j).
\end{aligned} \tag{16}$$

Since $P_i(k+1) = \beta_i \lambda_i(k+1) + \alpha_i$, substituting $P_i(k+1)$ by $\lambda_i(k+1)$, we can transform (16) as

$$\begin{aligned}
&\sum_{i\in V} \xi_i(k+1) + \sum_{i\in V} (\beta_i \lambda_i(k+1) + \alpha_i) \\
&\qquad = \sum_{i\in V} \xi_i(0) + \sum_{i\in V} P_i(0) + \sum_{j=0}^{k} \sum_{i\in V} u_i^{\xi}(j).
\end{aligned} \tag{17}$$

Taking limitations on both sides of (17), as $\lim_{k\to\infty} \xi_i(k) = 0, \forall i \in V$ and (6), one infers that

$$\lim_{k\to\infty} \sum_{i\in V} (\beta_i \lambda_i(k) + \alpha_i) = \sum_{i\in V} d_i + \sum_{k=0}^{\infty} \sum_{i\in V} u_i^{\xi}(k).$$

As λ_i's will achieve consensus according to the system dynamic and $\beta_i > 0$, we obtain (15). ■

Remark 1: We see that the final state of the algorithm in (5) only depends on the total sum of false data injected into the local power mismatch $\xi_i(k)$ and the false data injected into the incremental cost cannot affect the final state. Moreover, for the first time iteration, since $P_i(0)$ is used for updating $\xi_i(k)$, $\lambda_i(0), \forall i \in V$ can be randomly chosen.

Theorem 2: The algorithm in (5) can achieve convergence and the final point is the feasible solution of the problem in (1) without inequality constraints (1c) if the condition (10) and the following equation holds:

$$\lim_{k\to\infty} \sum_{j=0}^{k} \sum_{i\in V} u_i^{\xi}(j) = 0. \tag{18}$$

The feasible solution must be the optimal one, which indicates that there is no online stealthy attack under algorithm in (5).

Proof: Seeing that (10) holds, according to Theorem 1, the algorithm in (5) will achieve convergence and the final state satisfies (15). If we have (18) hold, there holds

$$\lim_{k\to\infty} \lambda_i(k) = \frac{\sum_{i\in V} d_i - \sum_{i\in V} \alpha_i}{\sum_{i\in V} \beta_i} \forall i \in V. \tag{19}$$

As $P_i(k+1) = \beta_i \lambda_i(k) + \alpha_i$, transforming (19), one obtains $\lim_{k\to\infty} \sum_{i\in V} P_i(k) = \sum_{i\in V} d_i$. The balance between the generation and demand is achieved, which implies the final point is feasible. Without any generation bounds consideration, the optimal solution of the problem satisfies (19). The feasible final point must be the optimal one. ■

Remark 2: From Theorem 2, we note that if the attacker just injects false data into the broadcast information, it cannot make the final point to a feasible but not optimal point. Hence, the online stealthiness cannot be realized. However, if the distributed algorithm is executed offline, every node thinks that the convergence and optimality are achieved. Without any detection, such attack cannot be found timely, and instability and even blackout may be caused by such kind of attack.

B. Bounded Generation Cases

Considering generation units have limited generation power bound, we prove that the above results still hold. The algorithm in (4) with false data injection into the broadcast information can be written as

$$\begin{cases}
\lambda_i(k+1) = \sum_{j\in V} w_{ij} \lambda_j(k) + \varepsilon \xi_i(k) + u_i^{\lambda}(k) \\
P_i(k+1) = \begin{cases} P_i^M, & \lambda_i(k+1) \geq \lambda_i^M \\ \beta_i \lambda_i(k+1) + \alpha_i, & \lambda_i^m < \lambda_i(k+1) < \lambda_i^M \\ P_i^m, & \lambda_i(k+1) \leq \lambda_i^m \end{cases} \\
\xi_i(k+1) = \sum_{j\in V} q_{ij} \xi_j(k) - (P_i(k+1) - P_i(k)) + u_i^{\xi}(k).
\end{cases} \tag{20}$$

Theorem 3: If the algorithm in (20) achieves convergence, i.e.,

$$\lim_{k\to\infty} \lambda_i(k) = \lambda_c, \lim_{k\to\infty} \xi_i(k) = 0 \quad \forall i \in V \tag{21}$$

where λ_c is a constant, we have (9).

Proof: For each node i, by taking limitations on both sides of the first equation of (20), one obtains

$$\begin{aligned}
\lim_{k\to\infty} \lambda_i(k+1) &= \lim_{k\to\infty} \left(\sum_{j\in V} w_{ij} \lambda_j(k) + \varepsilon \xi_i(k) + u_i^{\lambda}(k) \right) \\
&= \sum_{j\in V} w_{ij} \lim_{k\to\infty} \lambda_j(k) + \varepsilon \lim_{k\to\infty} \xi_i(k) \\
&\quad + \lim_{k\to\infty} u_i^{\lambda}(k).
\end{aligned}$$

Due to $\lim_{k\to\infty}\lambda_i(k)=\lambda_c$, we have $\lambda_c=\sum_{j\in V}w_{ij}\lambda_c+\varepsilon\times 0+\lim_{k\to\infty}u_i^{\lambda}(k)$. Because W is row stochastic, there holds $\sum_{j\in V}w_{ij}=1$. As a result, $\lambda_c=\lambda_c+\lim_{k\to\infty}u_i^{\lambda}(k)$. We conclude $\lim_{k\to\infty}u_i^{\lambda}(k)=0,\forall i\in V$. Since $\lim_{k\to\infty}\xi_i(k)=0$, by taking limitations on both sides of the third equation of (20), one obtains $0=-\lim_{k\to\infty}P_i(k+1)+\lim_{k\to\infty}P_i(k)+\lim_{k\to\infty}u_i^{\xi}(k)$. As $\lim_{k\to\infty}\lambda_i(k)=\lambda_c$ holds and $P_i(k+1)$ satisfies the second equation of (20), $P_i(k+1)$ can achieve convergence. Accordingly, one infers that $\lim_{k\to\infty}u_i^{\xi}(k)=0$. Hence, (9) holds. ■

Theorem 4: If conditions (10) and

$$\sum_{i\in V}P_i^m\le\sum_{i\in V}d_i+\lim_{k\to\infty}\sum_{j=0}^{k}\sum_{i\in V}u_i^{\xi}(j)\le\sum_{i\in V}P_i^M \tag{22}$$

hold, there must exist integers $\mathcal{M}>0$ and N^b such that when $k>\mathcal{M}$, (20) can be modeled as the system (5) with dimension being $N^b\le N$, which means that it can achieve convergence, i.e., (21) holds. Meanwhile, if $\lim_{k\to\infty}\sum_{j=0}^{k-1}\sum_{i\in V}u_i^{\xi}(j)\neq 0$, the final value will not be a feasible point.

Proof: Owing to (22), the original problem in (1) is feasible. By summing up the first and third equation in (20) for all $i\in V$, we can obtain

$$\sum_{i\in V}\lambda_i(k+1)=\sum_{i\in V}\sum_{j\in V}w_{ij}\lambda_j(k)+\varepsilon\sum_{i\in V}\xi_i(k)+\sum_{i\in V}u_i^{\lambda}(k). \tag{23}$$

According to (16), (23) can be transformed as

$$\sum_{i\in V}\lambda_i(k+1)=\sum_{i\in V}\sum_{j\in V}w_{ij}\lambda_j(k)+\varepsilon\Big(\sum_{i\in V}-P_i(k)+\sum_{i\in V}d_i+\sum_{j=0}^{k-1}\sum_{i\in V}u_i^{\xi}(j)\Big)+\sum_{i\in V}u_i^{\lambda}(k) \tag{24}$$

Without loss of generality, suppose $\varepsilon(\sum_{i\in V}-P_i(k)+\sum_{i\in V}d_i+\sum_{j=0}^{k-1}\sum_{i\in V}u_i^{\xi}(j))+\sum_{i\in V}u_i^{\lambda}(k)>0$, $\lambda_i(k+1)$'s will become larger generally and reach consensus, which means that $P_i(k+1)$'s will be increasing. Hence, $P_i(k)$'s will make $\varepsilon(\sum_{i\in V}-P_i(k)+\sum_{i\in V}d_i+\sum_{j=0}^{k-1}\sum_{i\in V}u_i^{\xi}(j))+\sum_{i\in V}u_i^{\lambda}(k)$ approach to zero as k goes to infinity. Since (10) holds, we suppose

$$\sum_{k=0}^{\infty}u_i^{\xi}(k)=S_i^{\xi},\ \lim_{k\to\infty}u_i^{\lambda}(k)=0,i\in V$$

where S_i^{ξ}'s are constants. Accordingly, with k growing, $P_i(k)$'s will have smaller adjustable range. Therefore, there must exist a large $\mathcal{M}$ such that when $k>\mathcal{M}$, some generation units reaching their upper or lower bounds will keep saturated. Cutting these saturated generation units, when $k>\mathcal{M}$, the dynamic of the algorithm can be described as the linear system (5) with dimension N^b satisfying $N^b\le N$. As a result, according to Theorem 1, the algorithm in (4) can achieve convergence, i.e., (21) holds.

Meanwhile, from (24), we can see that due to (21), there holds $\lim_{k\to\infty}\sum_{i\in V}-P_i(k)+\sum_{i\in V}d_i+\sum_{j=0}^{k-1}\sum_{i\in V}u_i^{\xi}(j)=0$. Then, if $\lim_{k\to\infty}\sum_{j=0}^{k-1}\sum_{i\in V}u_i^{\xi}(j)$ does not equal to zero, the discrepancy occurs between the generation and demand, which means that the final value will not be a feasible point. ■

Remark 3: The theoretical results for the unbounded generation play a key role in analyzing cases considering the inequality power constraints. First, considering the unbounded generation cases, we can obtain the linear system (5), which renders the specific analytical expression of the final solution tractable. Furthermore, the inequality power constraints for generation units have very limited impact on the convergence of the algorithm in (4). If the optimal solution of problem (1) is the same as the one of the problem in (1) deleting the inequality constraints, the algorithm will have almost the same dynamic under small false data injection into the broadcast information. If not, i.e., there is at least one generation unit that will reach its upper or lower bound, the system dynamic may vary from the unbounded case, but can still attain convergence under the false data injection into the broadcast information. Further, we can see that the results of Theorems 1–4 considering the attacker injecting false data into the broadcast information are not related to the number of attack nodes.

IV. Stealthy Attacks for Generation Cost Parameters

In Section II, we formulate the problem of the consensus-based ED algorithm under attacks as (4), where the attack may not be the stealthy attack. Here, we provide a form of the online stealthy attack injecting false data into generation cost parameters for both the unbounded and bounded generation cases, which is the specified form of that in (4). Under such attack, the attacker can fulfill either the online or offline stealthy attack. First, some important notations are provided. Denote $\tilde{C}_m$ and C_m as the final generation cost under attacks and no attack, respectively. Meanwhile, λ^* (P^*) is the optimal incremental cost (generation power) under no attack and $\tilde{\lambda}^*$ ($\tilde{P}^*$) is the final incremental cost (generation power) under attacks.

A. Unbounded Generation Cases

Considering there is only one attack node $i_a, i_a\in V$ in the network, we provide how attack node i injecting constant false data into generation cost parameters can affect the final generation cost compared with the optimal one. Let the manipulated parameters satisfy $\tilde{\beta}_{i_a}=\beta_{i_a}+\Delta_{\beta_{i_a}}$ and $\tilde{\alpha}_{i_a}=\alpha_{i_a}+\Delta_{\alpha_{i_a}}$. Then, we obtain

$$\lim_{k\to\infty}\lambda_i(k)=\tilde{\lambda}^*=\frac{\sum_{i\in V}d_i-\sum_{i\in V}\alpha_i-\Delta_{\alpha_{i_a}}}{\sum_{i\in V}\beta_i+\Delta_{\beta_{i_a}}}. \tag{25}$$

Theorem 5: If one attack node i injecting constant false data $\Delta_{\beta_{i_a}}\neq 0$ and $\Delta_{\alpha_{i_a}}\neq 0$ to β_{i_a} and α_{i_a}, the algorithm in (5) can achieve convergence and the final point is feasible but

not optimal. A larger deviation of $\tilde{\lambda}^*$ introduces more growth of $\tilde{C}^m$.

Proof: From (19) and (25), one obtains

$$\tilde{\lambda}^* = \frac{\lambda^* \sum_{i\in V} \beta_i - \Delta\alpha_{i_a}}{\sum_{i\in V} \beta_i + \Delta\beta_{i_a}}$$

which means that

$$\tilde{\lambda}^* \Delta\beta_{i_a} + \Delta\alpha_{i_a} = (\lambda^* - \tilde{\lambda}^*) \sum_{i\in V} \beta_i.$$

Therefore, the cost of node i_a under attacks is denoted by

$$\begin{aligned}
&\tilde{C}_{i_a}(\tilde{P}_{i_a}) \\
&= \frac{[(\beta_{i_a} + \Delta\beta_{i_a})\tilde{\lambda}^* + \alpha_{i_a} + \Delta\alpha_{i_a} - \alpha_{i_a}]^2}{2\beta_{i_a}} + \gamma_{i_a} \\
&= \frac{(\beta_{i_a}\tilde{\lambda}^* + \Delta\beta_{i_a}\tilde{\lambda}^* + \Delta\alpha_{i_a})^2}{2\beta_{i_a}} + \gamma_{i_a} \\
&= \frac{[\beta_{i_a}\tilde{\lambda}^* + (\lambda^* - \tilde{\lambda}^*)\sum_{i\in V}\beta_i]^2}{2\beta_{i_a}} + \gamma_{i_a}.
\end{aligned}$$

Without attack, the cost of node i_a is $\tilde{C}_{i_a}(\tilde{P}_{i_a}) = \frac{(\beta_{i_a} + *\lambda^* + \alpha_{i_a} - \alpha_{i_a})^2}{2\beta_{i_a}} + \gamma_{i_a} = \frac{\beta_{i_a}^2 (\lambda^*)^2}{2\beta_{i_a}} + \gamma_{i_a}$. Thus, we have

$$\begin{aligned}
&C_{i_a}(P_{i_a}) - \tilde{C}_{i_a}(\tilde{P}_{i_a}) \\
&= \frac{\beta_{i_a}^2 (\lambda^*)2 - [\beta_{i_a}\tilde{\lambda}^* + (\lambda^* - \tilde{\lambda}^*)\sum_{i\in V}\beta_i]^2}{2\beta_{i_a}} \\
&= (\beta_{i_a}\lambda^* + \beta_{i_a}\tilde{\lambda}^* + (\lambda^* - \tilde{\lambda}^*)\sum_{i\in V}\beta_i) \\
&\quad \times \frac{(\beta_{i_a}\lambda^* - \beta_{i_a}\tilde{\lambda}^* - (\lambda^* - \tilde{\lambda}^*)\sum_{i\in V}\beta_i)}{2\beta_{i_a}} \\
&= [(\beta_{i_a} + \sum_{i\in V}\beta_i)\lambda^* + (\beta_{i_a} - \sum_{i\in V}\beta_i)\tilde{\lambda}^*] \\
&\quad \times \frac{(\beta_{i_a} + \sum_{i\in V}\beta_i)(\lambda^* - \tilde{\lambda}^*)}{2\beta_{i_a}}.
\end{aligned} \tag{26}$$

For $i \neq i_a$, there holds

$$\begin{aligned}
C_i(P_i) - \tilde{C}_i(\tilde{P}_i) &= \frac{\beta_i((\lambda^*)^2 - (\tilde{\lambda}^*)^2)}{2} \\
&= \frac{\beta_i(\lambda^* - \tilde{\lambda}^*)(\lambda^* + \tilde{\lambda}^*)}{2}.
\end{aligned} \tag{27}$$

From (26) and (27), we obtain

$$\begin{aligned}
&C_m - \tilde{C}_m \\
&= \sum_{i\in V, i\neq i_a} [C_i(P_i) - \tilde{C}_i(\tilde{P}_i)] + C_{i_a}(P_{i_a}) - \tilde{C}_{i_a}(\tilde{P}_{i_a}) \\
&= \left(\beta_{i_a} - \sum_{i\in V}\beta_i\right)(\lambda^* - \tilde{\lambda}^*) \\
&\quad \times \frac{[-\beta_{i_a}(\lambda^* + \tilde{\lambda}^*) + \beta_{i_a}\lambda^* + \sum_{i\in V}\beta_i\lambda^* + \beta_{i_a}\tilde{\lambda}^* - \sum_{i\in V}\beta_i\tilde{\lambda}^*]}{2\beta_{i_a}} \\
&= \frac{\left(\beta_{i_a} - \sum_{i\in V}\beta_i\right)\left(\sum_{i\in V}\beta_i\right)(\lambda^* - \tilde{\lambda}^*)^2}{2\beta_{i_a}}.
\end{aligned}$$

When $\lambda^* \neq \tilde{\lambda}^*$, we have $C_m - \tilde{C}_m < 0$. Iff $\lambda^* = \tilde{\lambda}^*$, there holds $C_m - \tilde{C}_m = 0$. Therefore, the final point is not optimal, which signifies that by injecting constant false data into generation cost parameters, the attack can keep stealthy and make the total generation cost increase. ■

Remark 4: From the above proof, one observes that more deviation of $\tilde{\lambda}^*$ from the optimal one λ^* can induce larger increment of generation cost. The attack can make $\tilde{\lambda}^*$ deviated from λ^* by manipulating β_{i_b} and α_{i_a}. The above analysis can be generalized for multiple attack nodes cases.

B. Bounded Generation Cases

The inequality constraints in (1) are important practical constraints. With the constant false data injection into generation cost parameters, we analyze how such attack will affect the optimality of the algorithm in (4).

Theorem 6: For the problem in (1), if attack node i_a only injects constant false data $\Delta_{\beta_{i_a}}$ or $\Delta_{\alpha_{i_a}}$ to β_{i_a} or α_{i_a}, there exists $\Delta_{\beta_{i_a}}$ or $\Delta_{\alpha_{i_a}}$ such that the algorithm in (4) can achieve convergence and the final point is feasible but not optimal.

Proof: As the structure of the algorithm in (4) under constant false data injection into generation cost parameters remains constant, Lemma 3 still holds. It means that the algorithm in (1) can achieve convergence and the power imbalance will disappear with iteration. Therefore, the final point is feasible.

As the objective function of the problem in (1) is strictly convex and the feasible set is convex, the problem in (1) has only one optimal point P^* and one incremental cost λ^*. Suppose that there exits no $\Delta_{\beta_{i_a}}$ or $\Delta_{\alpha_{i_a}}$ injected by attack node i such that the optimal point will change. Accordingly, the optimal incremental cost and the optimal solution under attacks will satisfy $\tilde{\lambda}^* = \lambda^*$ and $\tilde{P}^* = \tilde{P}^*$. For attack node i_a with any $\Delta_{\beta_{i_a}}$ or $\Delta_{\alpha_{i_a}}$, there must hold

$$\begin{aligned}
\tilde{P}_{i_a}^* &= \begin{cases} P_{i_a}^M, & \tilde{\lambda}^* \geq \tilde{\lambda}_{i_a}^M \\ \tilde{\beta}_{i_a}\tilde{\lambda}^* + \tilde{\alpha}_{i_a}, & \tilde{\lambda}_{i_a}^m < \tilde{\lambda}^* < \tilde{\lambda}_{i_a}^M \\ P_{i_a}^m, & \tilde{\lambda}^* \leq \tilde{\lambda}_{i_a}^m \end{cases} \\
&= \begin{cases} P_i^M, & \lambda^* \geq \lambda_{i_a}^M \\ \beta_{i_a}\lambda^* + \alpha_{i_a}, & \lambda_{i_a}^m < \lambda^* < \lambda_{i_a}^M \\ P_{i_a}^m, & \lambda^* \leq \lambda_{i_a}^m \end{cases}
\end{aligned} \tag{28}$$

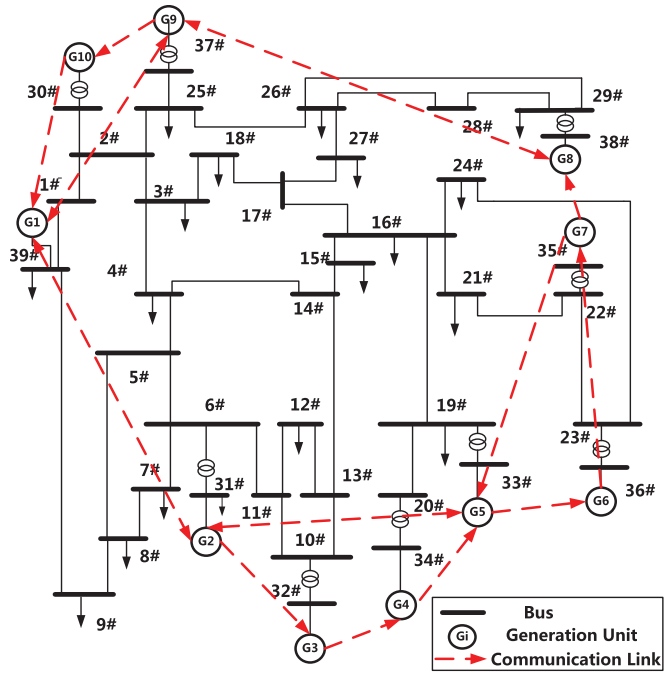

Fig. 1. IEEE 39-Bus.

where $\tilde{\beta}_{i_a} = (\Delta_{\beta_{i_a}} + \beta_{i_a})$, $\tilde{\alpha}_{i_a} = \Delta_{\alpha_{i_a}} + \alpha_{i_a}$, $\tilde{\lambda}_{i_a}^m = \frac{1}{\tilde{\beta}_{i_a}} P_{i_a}^m - \frac{\tilde{\alpha}_{i_a}}{\tilde{\beta}_{i_a}}$ and $\tilde{\lambda}_{i_a}^M = \frac{1}{\tilde{\beta}_{i_a}} P_{i_a}^M - \frac{\tilde{\alpha}_{i_a}}{\tilde{\beta}_{i_a}}$. One observes that there must exist $\Delta_{\beta_{i_a}}$ and $\Delta_{\alpha_{i_a}}$ such that (28) does not hold. Consequently, we can conclude the result. ■

Remark 5: One notices that by injecting constant false data into generation cost parameters, the convergence and feasibility of the final point can be guaranteed but the optimality is ruined stealthily for both online and offline cases. Consequently, these parameters are very important, which should be well protected. The deviation of the total generation cost caused by this form of attack is determined by the constant false data injection and the generation power bounds. Moreover, different attack node has different effective manipulation range, which means the effective false data injection range for generation cost parameters. With lots of attack nodes, if the manipulation range of the attacker becomes larger, the total generation cost will be larger.

V. Performance Evaluation

We consider the IEEE 39-bus system with ten generation units and 18 demands. Suppose there are $N = 10$ agents in ED, where each agent can control one generation unit and its demand can include some local demands. The communication network, which is described by the red lines in Fig. 1, is strongly connected. Here, we consider three kinds of generation units including coal-fired steam unit and two different oil-fired steam units. The related parameters are shown in Table I by referring to [36]. Nodes $i = 1, 2, 5, 6$ contain coal-fired steam units, nodes $i = 3, 7, 9$ contain coal-fired-1 steam units and other nodes have coal-fired-2 steam units.

Meanwhile, we set $\epsilon = 7.75 * 10^{-4}$ and the total demand satisfies $\sum_{i \in V} d_i = 3300$. When there is no attack, the incremental costs will converge to the same value $\lambda^* = 8.82$ and the power

TABLE I
Parameters of Generation Units for IEEE 39-Bus

	a_i	b_i	c_i	P_i^m	P_i^M
Coal-fired	0.00142	7.20	510	150	650
Oil-fired-1	0.00194	7.85	310	100	400
Oil-fired-2	0.00482	7.97	78	50	200

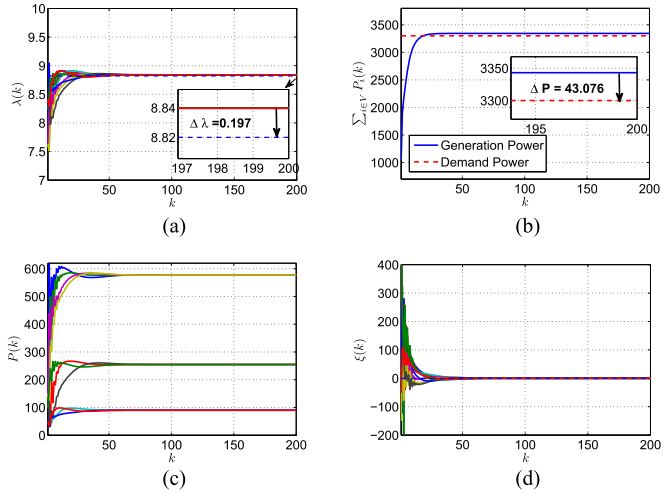

Fig. 2. Convergence performance without generation bounds. (a) Incremental cost. (b) Total power mismatch. (c) Generation power. (d) Local power mismatch.

mismatch will converge to zero, and the generation power converges to a stable state with iterations.

A. False Data Injection into the Broadcast Information

1) Unbounded Generation Cases: Assume that node $i = 1$ is an attack node and it tries to keep offline stealthiness through injecting false data $u_1^\lambda(k) = 4 * 0.15^k$ and $u_1^\xi(k) = 80 * 0.35^k$. We investigate how attacks can affect the convergence and the feasibility of the final point under the algorithm in (5). It can be seen in Fig. 2(a) that all incremental cost will achieve consensus under such false data injection. However, the final incremental cost is not the optimal one, which means that the optimality of the algorithm in (4) is ruined. Meanwhile, the balance between the generation and demand is broken, which is shown in Fig. 2(b). Thus, such attack can be detected by frequency deviation measurements and online stealthy attack cannot be achieved. We observe from Fig. 2(c) that all generation power P_i's converge to stable states. Meanwhile, one can see in Fig. 2(d) that local power mismatch approaches to zero with iterations. Thus, there exist attacks, which can guarantee the convergence of the distributed algorithm in (4) but can break up the optimality of the final point, i.e., the offline stealthy attack is realized.

2) Bounded Generation Cases: Under the same setting, if each optimal generation power P_i^* satisfies $P_i^m < P_i^* < P_i^M$ and the initial point is within the generation bounds, the optimal solution of the problem in (1) is the same as the problem in (1) without inequality constraints (1c) and the convergence

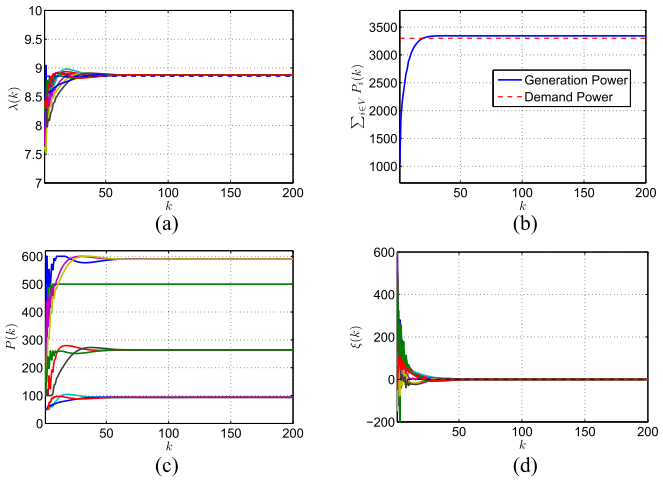

Fig. 3. Convergence performance under bounded power. (a) Incremental cost. (b) Power generation. (c) Generation power. (d) Local power mismatch.

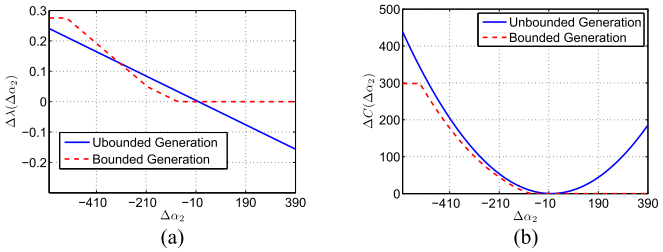

Fig. 4. False data injection for generation parameters. (a) Incremental cost variance. (b) Total cost variance.

curves of $\lambda_i(k)$, $\xi_i(k)$ will be the same under two situations considering the small bounded false data injection. To investigate how the bounded power generation will affect convergence under attacks, we change the upper bound of node $i = 2$ as $P_2^M = 500$. Since the problem changes, the optimal incremental cost turns into $\lambda^* = 8.8557$. Under the same bounded false data injection, we can obtain almost the same convergence performance, which is shown in Fig. 3(a)–(d). It also verifies our theoretical analysis for the convergence of the algorithm in (4) considering the bounded generation.

B. False Data Injection into Generation Cost Parameters

We investigate how the attacker injecting constant false data to generation cost parameters can influence the optimality of ED. The above scenario setting for the bounded generation case is considered. By manipulating parameters α_i for $i = 2$ where Δ_{α_2} changes from -600 to 390, we conduct simulations for both bounded and unbounded generation cases, respectively. As shown in Fig. 4(a) and (b), the overall tendency exhibits that the total generation cost increases as the incremental cost deviates from the optimal one. For the unbounded generation case, as deviation of incremental cost becomes larger, the total generation cost grows, i.e., the efficiency of ED is lowered by such stealthy attack. For the bounded generation case, the attack node has the limited effective manipulation range, beyond which, the total generation cost would not change. Considering how the number

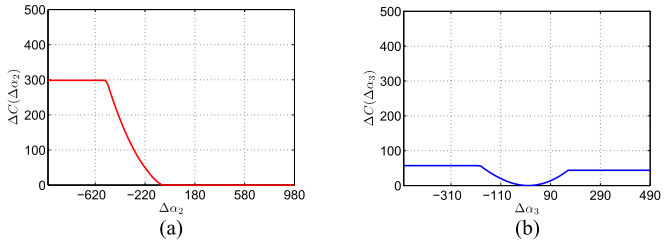

Fig. 5. ΔC for cases with one attack node. (a) $\Delta C(\Delta\alpha_2)$. (b) $\Delta C(\Delta\alpha_3)$.

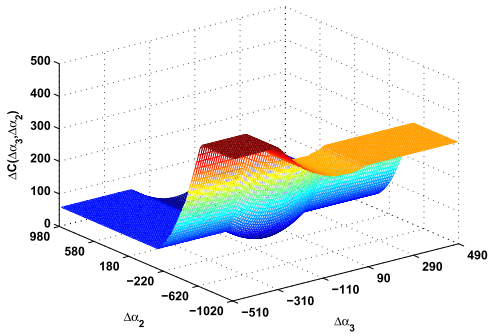

Fig. 6. ΔC for the case with two attack nodes.

of attack nodes will affect the effective manipulation range, we conduct simulations for cases, i.e., the attack only injects constant false data to α_2, the attack only injects constant false data into α_3, and the attack injects constant false data to α_2 and α_3. From Fig. 5 and 6, we can observe that the total generation cost of the case with two attack nodes is larger than that with one attack node.

VI. Conclusion

In this paper, we analyzed how the consensus-based ED algorithm performs under stealthy attacks. We proved that for the false data injection into the broadcast information, the algorithm can still achieve convergence but the final state must be optimal one if it is feasible. Considering only the divergence of the algorithm can be detected for the offline case, we proved that such attack can be stealthy. Then, for the online case, we assume that the imbalance between the generation and demand can be recognized by frequency deviation measurements. We obtained the stealthy attack that injects constant false data into generation cost parameters. Under such attack, the power mismatch approaches to zero but the total cost increases. Furthermore, we found that the constant false data injection into generation cost parameters can affect the deviation of the optimal total cost through the deviation of the final incremental cost. As the power of generation unit is bounded, each attack node has limited effective false data injection range. Simulation results showed that for the bounded generation case, the convergence of the algorithm under attacks had the same performance as the unbounded one, which also illustrated our obtained results. For the future work, we will analyze whether the results can be generalized for more general distributed optimization problems under attacks.

ACKNOWLEDGMENT

The authors would like to thank the Editor-in-Chief, the Associate Editor, and the anonymous reviewers for their valuable comments and suggestions that have significantly improved the quality of this paper.

REFERENCES

[1] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart grid—The new and improved power grid: A survey," *IEEE Commun. Surv. Tuts.*, vol. 14, no. 4, pp. 944–980, Oct.–Dec. 2012.

[2] M. Liu, Y. Shi, and H. Gao, "Aggregation and charging control of PHEVs in smart grid: A cyber-physical perspective," *Proc. IEEE*, vol. 104, no. 5, pp. 1071–1085, May 2016.

[3] H. S. V. S. K. Nunna and S. Doolla, "Multiagent-based distributed-energy-resource management for intelligent microgrids," *IEEE Trans. Ind. Electron.*, vol. 60, no. 4, pp. 1678–1687, Apr. 2013.

[4] X. Liu, M. Dong, K. Ota, P. Hung, and A. Liu, "Service pricing decision in cyber-physical systems: Insights from game theory," *IEEE Trans. Serv. Comput.*, vol. 9, no. 2, pp. 186–198, Apr. 2016.

[5] V. Loia and A. Vaccaro, "Decentralized economic dispatch in smart grids by self-organizing dynamic agents," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 44, no. 4, pp. 397–408, Apr. 2014.

[6] W. Tushar *et al.*, "Three-party energy management with distributed energy resources in smart grid," *IEEE Trans. Ind. Electron.*, vol. 62, no. 4, pp. 2487–2498, Apr. 2015.

[7] N. Rahbari-Asr, U. Ojha, Z. Zhang, and M.-Y. Chow, "Incremental welfare consensus algorithm for cooperative distributed generation/demand response in smart grid," *IEEE Trans. Smart Grid*, vol. 5, no. 6, pp. 2836–2845, Nov. 2014.

[8] T. Sauter and M. Lobashov, "End-to-end communication architecture for smart grids," *IEEE Trans. Ind. Electron.*, vol. 58, no. 4, pp. 1218–1228, Apr. 2011.

[9] H. Zhang, P. Cheng, L. Shi, and J. Chen, "Optimal dos attack scheduling in wireless networked control system," *IEEE Trans. Control Syst. Technol.*, vol. 24, no. 3, pp. 843–852, May 2016.

[10] S. M. Amin, "Securing the electricity grid," *Bridge*, vol. 40, no. 1, pp. 13–20, 2010.

[11] A. R. Metke and R. L. Ekl, "Security technology for smart grid networks," *IEEE Trans. Smart Grid*, vol. 1, no. 1, pp. 99–107, Jun. 2010.

[12] Y. Mo *et al.*, "Cyber-physical security of a smart grid infrastructure," *Proc. IEEE*, vol. 100, no. 1, pp. 195–209, Jan. 2012.

[13] H. Zhang, P. Cheng, L. Shi, and J. Chen, "Optimal denial-of-service attack scheduling with energy constraint," *IEEE Trans. Autom. Control*, vol. 60, no. 11, pp. 3023–3028, Nov. 2015.

[14] W. Zeng, Y. Zhang, and M. Yuen Chow, "A resilient distributed energy management algorithm for economic dispatch in the presence of misbehaving generation units," in *Proc. Resilience Week*, Philadelphia, PA, USA, Oct. 2015, pp. 12–16.

[15] J. Duan, W. Zeng, and M.-Y. Chow, "Economic impact of data integrity attacks on distributed dc optimal power flow algorithm," in *Proc. North Amer. Power Symp.*, Charlotte, NC, USA, Oct. 2015, pp. 1–7.

[16] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inform. Syst. Security*, vol. 14, no. 1, Jan. 2011, Art. no. 13.

[17] S. Amin, X. Litrico, S. Sastry, and A. M. Bayen, "Cyber security of water scada systems—Part I: Analysis and experimentation of stealthy deception attacks," *IEEE Trans. Control Syst. Technol.*, vol. 21, no. 5, pp. 1963–1970, Sep. 2013.

[18] A. Teixeira, D. Pérez, H. Sandberg, and K. H. Johansson, "Attack models and scenarios for networked control systems," in *Proc. 1st Int. Conf. High Confidence Netw. Syst.*, New York, NY, USA, Apr. 2012, pp. 55–64.

[19] G. Chen, F. L. Lewis, E. N. Feng, and Y. Song, "Distributed optimal active power control of multiple generation systems," *IEEE Trans. Ind. Electron.*, vol. 62, no. 11, pp. 7079–7090, Nov. 2015.

[20] M. D. Ilic, L. Xie, and J.-Y. Joo, "Efficient coordination of wind power and price-responsive demand—Part I: Theoretical foundations," *IEEE Trans. Power Syst.*, vol. 26, no. 4, pp. 1875–1884, Nov. 2011.

[21] Y. Liu, H. Xin, Z. Qu, and D. Gan, "A distributed solution to real-time economic dispatch problem under power flow congestion," in *Proc. IEEE Power Energy Soc. Gen. Meeting*, Denver, CO, USA, Jul. 2015, pp. 1–5.

[22] H. Bevrani, *Robust Power System Frequency Control*. New York, NY, USA: Springer, 2009.

[23] J. Qin, W. Fu, H. Gao, and W. X. Zheng, "Distributed k-means algorithm and fuzzy c-means algorithm for sensor networks based on multi-agent consensus theory," *IEEE Trans. Cybern.*, to be published, doi:10.1109/TCYB.2016.2526683.

[24] R. Olfati-Saber, J. A. Fax, and R. M. Murray, "Consensus and cooperation in networked multi-agent systems," *Proc. IEEE*, vol. 95, no. 1, pp. 215–233, Jan. 2007.

[25] J. Qin, H. Gao, and C. Yu, "On discrete-time convergence for general linear multi-agent systems under dynamic topology," *IEEE Trans. Autom. Control*, vol. 59, no. 4, pp. 1054–1059, Apr. 2014.

[26] J. He, P. Cheng, L. Shi, J. Chen, and Y. Sun, "Time synchronization in WSNS: A maximum-value-based consensus approach," *IEEE Trans. Autom. Control*, vol. 59, no. 3, pp. 660–675, Mar. 2014.

[27] Z. Zhang and M.-Y. Chow, "Convergence analysis of the incremental cost consensus algorithm under different communication network topologies in a smart grid," *IEEE Trans. Power Syst.*, vol. 27, no. 4, pp. 1761–1768, Nov. 2012.

[28] S. Kar, G. Hug, J. Mohammadi, and J. M. F. Moura, "Distributed state estimation and energy management in smart grids: A consensus + innovations approach," *IEEE J. Sel. Topics Signal Process.*, vol. 8, no. 6, pp. 1761–1768, Dec. 2014.

[29] S. Yang, S. Tan, and J.-X. Xu, "Consensus based approach for economic dispatch problem in a smart grid," *IEEE Trans. Power Syst.*, vol. 28, no. 4, pp. 4416–4426, Nov. 2013.

[30] T. Yang, D. Wu, Y. Sun, and J. Lian, "Minimum-time consensus-based approach for power system applications," *IEEE Trans. Ind. Electron.*, vol. 63, no. 2, pp. 1318–1328, Feb. 2016.

[31] Y. Xu and Z. Li, "Distributed optimal resource management based on the consensus algorithm in a microgrid," *IEEE Trans. Ind. Electron.*, vol. 62, no. 4, pp. 2584–2592, Apr. 2015.

[32] G. Binetti, A. Davoudi, F. L. Lewis, D. Naso, and B. Turchiano, "Distributed consensus-based economic dispatch with transmission losses," *IEEE Trans. Power Syst.*, vol. 29, no. 4, pp. 1711–1720, Jul. 2014.

[33] J. He, P. Cheng, L. Shi, and J. Chen, "Sats: Secure average-consensus-based time synchronization in wireless sensor networks," *IEEE Trans. Signal Process.*, vol. 61, no. 24, pp. 6387–6400, Dec. 2013.

[34] M. Zhou, J. He, P. Cheng, and J. Chen, "Discrete average consensus with bounded noise," in *Proc. 52nd Annu. IEEE Conf. Decision Control*, Florence, Italy, Jul. 2013, pp. 5270–5275.

[35] J. He, M. Zhou, P. Cheng, L. Shi, and J. Chen, "Consensus under bounded noise in discrete network systems: An algorithm with fast convergence and high accuracy," *IEEE Trans. Cybern.*, vol. 46, no. 12, pp. 2874–2884, Dec. 2016.

[36] A. J. Wood and B. F. Wollenberg, *Power Generation, Operation, and Control*. Hoboken, NJ, USA: Wiley, 2012.

Chengcheng Zhao (S'15) received the B.E. degree in measurement and control technology and instrumentation from Hunan University, Changsha, China, in 2013. She is working toward the Ph.D. degree in control science and engineering in the College of Control Science and Engineering, Zhejiang University, Hangzhou, China.

She is a member of the Networked Sensing and Control Group, Zhejiang University. Her research interests include distributed computation and optimization in multi-agent networks and distributed energy management in smart grid.

Jianping He (M'15) received the Ph.D. degree in control science and engineering from Zhejiang University, Hangzhou, China, in 2013.

He is currently an Associate Research Fellow in the Department of Automation, Shanghai Jiao Tong University, Shanghai, China. His research interests include the control and optimization of sensor networks and cyber-physical systems, scheduling and optimization in VANETs and social networks, and investment decisions in financial markets and electricity markets.

Peng Cheng (M'10) received the B.E. degree in automation and the Ph.D. degree in control science and engineering from Zhejiang University, Hangzhou, China, in 2004 and 2009, respectively.

He is currently a Professor in the College of Control Science and Engineering, Zhejiang University. His research interests include networked sensing and control, cyber-physical systems, and robust control and applications.

Prof. Cheng serves as an Associate Editor of *Wireless Networks* and the *International Journal of Communication Systems* and as a Guest Editor of the IEEE TRANSACTIONS ON CONTROL OF NETWORK SYSTEMS. He served as a Local Arrangement Chair of IEEE MobiHoc 2015 and the Publicity Co-Chair of IEEE MASS 2013.

Jiming Chen (M'08–SM'11) received the B.Sc. and Ph.D. degrees from Zhejiang University, Hangzhou, China, in 2000 and 2005, respectively, both in control science and engineering.

From 2008 to 2010, he was a Visiting Researcher at the University of Waterloo. He is currently a Full Professor in the College of Control Science and Engineering and the Vice-Director of the State Key Laboratory of Industrial Control Technology and Institute of Industrial Process Control, Zhejiang University. His research interests include sensor networks, networked control, and cyber security.

Prof. Chen serves/served as an Associate Editor of several international journals, including the IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEM, IEEE NETWORK, IEEE TRANSACTIONS ON CONTROL OF NETWORK SYSTEMS, etc. He was Guest Editor of the IEEE TRANSACTIONS ON AUTOMATIC CONTROL, etc.