Article

Resilient Distributed Coordination of Plug-In Electric Vehicles Charging under Cyber-Attack

Shengxuan Weng ^{1,*} , Yanman Li ² and Xiaohua Ding ²

¹ Institute of Advanced Technology, Nanjing University of Posts and Telecommunications, Nanjing 210023, China

² NARI Technology Co. Ltd., Nanjing 210023, China; liyanman@sgepri.sgcc.com.cn (Y.L.); dingxiaohua@sgepri.sgcc.com.cn (X.D.)

* Correspondence: shxweng@gmail.com

Received: 21 April 2020; Accepted: 3 May 2020; Published: 7 May 2020

Abstract: The coordinated scheduling of plug-in electric vehicle (PEV) charging should be constructed in distributed architecture due to the growing population of PEVs. Since the information and communication technology makes the adversary more permeable, the distributed PEV charging coordination is vulnerable to cyber-attack which may degrade the performance of scheduling and even cause the failure of scheduler task. Considering the tradeoff between system-wide economic efficiency, distribution level limitations and PEV battery degradation, this paper investigates the resilient distributed coordination of PEV charging to resist cyber-attack, where the steps of detection, isolation, updating and recovery are designed synthetically. Under the proposed scheduling scheme, the misbehaving PEVs suffering from cyber-attack are gradually marginalized and finally isolated, and the remaining well-behaving PEVs obtain their own optimal charging strategy to minimize the total system cost in distributed architecture. The simulation results verify the effectiveness of theoretical method.

Keywords: plug-in electric vehicle; distributed charging coordination; resilience; cyber-attack

1. Introduction

Due to the growing concerns about carbon emission, fossil energy depletion and climate change, plug-in electric vehicles (PEVs) will be integrated widely into the power system [1,2]. The global sales of PEVs have almost exponential growth over the past 10 years before 2020, and the selling number is predicted to be 30 million and 50 million at the year 2030 and 2040 respectively [3]. The rising population of PEVs facilitates the exploitation of sustainable and renewable energy, reduces environmental pollution and minimizes greenhouse gases [4]. However, their disordered charging behavior introduces significant adverse impacts on power grid including power unbalance between the demand of PEVs' charging and the supply of power grid, localized overloading, excessive losses and larger voltage deviation [5–7]. Therefore, it is desirable to study the proper coordination scheme of PEV charging to minimize the above mentioned negative effects.

Many research works have studied the issue of PEV charging strategy scheduling in centralized architecture. In Reference [8], a centralized minimum-cost load scheduling algorithm was constructed to determine the purchase of energy in the day-ahead market and a dynamic dispatch algorithm was developed for distributing the purchased energy to PEVs. A centralized aggregator was proposed in [9] to compute the optimal charging strategy of each PEV for efficient power utilization. The centralized coordinated PEV charging method aimed to minimize the power losses and maximize the main grid load factor was studied in [10]. The centralized scheduling method mentioned in the existing papers requires a control center to collect the information of all PEVs, make the charging decision and transmit the control signal back to each PEV. In the centralized architecture, expensive high-bandwidth

communication infrastructures are required, the system building cost increases, and the reliability and security are vulnerable to a single point of failure [11]. To address this issue, some research works focused on the distributed scheduling method, whose implementation is based on the neighboring communication and local computation without the usage of control center. A distributed cooperative charging control for PEVs was developed in [12] to avoid overload and maximize customer preference where the control center is eliminated. In Reference [13], the distributed consensus protocol contributed to a coordinated charging and discharging strategy of PEVs. The distributed optimal charging scheduling of PEVs considering multiple energy suppliers was studied in [14]. In Reference [15], a consensus algorithm was used in the distributed PEV charging coordination to facilitate the tradeoff between the total generation cost and local costs associated with battery degradation and distribution network overloading, and then the issue about the loading on the transformers was considered further in [16]. Compared with the centralized scheduling method, the distributed one in the above mentioned papers is more suitable for charging coordination with massive PEVs spread over a wide geographical area due to its characteristic of flexibility, scalability, robustness and economy.

In order to realize the centralized or distributed PEV charging coordination, information transmission plays an important role. However, the extensive utilization of information and communication technology makes the adversary more permeable, and causes the PEV charging system more vulnerable to cyber-attack [17]. The cyber-attack can violate the main security attributes of information transmission such as confidentiality, authenticity, integrity and availability [18]. This may degrade the performance of scheduling and control, and even lead to the failure of charging coordination [19]. Several potential failure scenarios for PEV charging system caused by cyber-attacks were defined and the adverse impacts were studied in [20]. Multiple jamming attacks for charging stations and PEVs were considered in [21]. These relative literatures verify the damage of cyber-attack in PEV charging, and it is necessary to identify the resilient PEV charging approach as a major research direction to resist the cyber-attack. In Reference [22], the model-based detection mechanism for cyber-attack was designed to protect the PEV battery packs during charging. The resilient PEV charging policy under price information attacks was considered in [23] where the DoS attack and price manipulation attack can be resisted.

Although there exists some research concerning with the resilient PEV charging method against cyber-attack as mentioned before, the topic about coordinated scheduling of PEV charging in distributed architecture is still lacking to the best of authors' knowledge, and this motivates our study. This paper concerns on the distributed coordinated scheduling of PEV charging under cyber-attack, where the trade-off between system-wide economic efficiency, distribution level limitations and PEV battery degradation are considered. Each participating PEV determines its own charging strategy with respect to an agreed common average price, which is obtained by a distributed consensus protocol of the individual price exchanged among the neighboring PEVs through communication network. The cyber-attack launched by an adversary tampers the individual price by unauthorized attack data injection. The modality and impact of cyber-attack are analyzed, and a novel resilient distributed coordination scheme of PEV charging based on dynamical confidence level is constructed in this paper. It is proved that the system cost function for PEV charging can be minimized even under cyber-attack. The main contributions of this paper are summarized as follows.

- (1) The confidence level based resilient PEV charging coordination in the presence of cyber-attack is proposed, where the detection, isolation, updating and recovery steps are designed synthetically. The misbehaving PEV under cyber-attack is gradually marginalized and finally isolated from the system according to its confidence level calculated in real-time by the above steps. In order to resist the cyber-attack and acquire the optimized charging strategy, these steps are executed at each participating PEV based on the information received from its neighbors.
- (2) The implementation of resilient PEV charging coordination only requires each participating PEV to communicate with its neighboring PEVs in communication network, which implies that the proposed charging scheduling method is compliant with distributed architecture. It is more suitable for the charging system containing massive PEVs.

- (3) The modality of cyber-attack is constructed and its negative effect on PEV charging coordination is analyzed. It is demonstrated that the common average price can not be obtained via the distributed consensus protocol when some PEVs suffer from cyber-attack, and this further results in the failure of traditional charging scheduling algorithm which was constructed without the consideration of cyber-attack.

This paper is organized as follows. The charging model and problem formulation are given in Section 2. Section 3 represents the modality and negative effects of cyber-attack in PEV charging coordination. The resilient distributed coordination of PEV charging against cyber-attack is constructed in Section 4, and the effectiveness of theory is verified by simulation in Section 5. Section 6 states the conclusion and future work.

2. Problem Formulation

2.1. Charging Model of Individual PEV

Consider the optimal charging scheduling of n PEVs labeling from 1 to n over the time horizon $\mathcal{T} = \{0, 1, \dots, T-1\}$. For each PEV i ($i = 1, 2, \dots, n$), denote the charging power at time $t \in \mathcal{T}$ as u_{it} and name the charging strategy over the horizon $\mathcal{T}$ as the vector $\mathbf{u}_i = \{u_{i0}, u_{i1}, \dots, u_{i(T-1)}\}$. The charging strategy $\mathbf{u}_i$ is admissible if

$$u_{it} = \begin{cases} \geq 0, & t \in \mathcal{T}_i \\ = 0, & \text{otherwise} \end{cases} \quad (1)$$

and

$$\|\mathbf{u}_i\|_1 \leq \Gamma_i \quad (2)$$

where $\|\mathbf{u}_i\|_1 \equiv \sum_{t \in \mathcal{T}} u_{it}$, Γ_i is the energy capacity and $\mathcal{T}_i \subseteq \mathcal{T}$ is the charging horizon of the PEV i respectively. Denote the set of admissible charging strategies of PEVs i which satisfy the restricted condition (1) and (2) as $\mathcal{U}_i$.

As mentioned in [24], the distribution-level harmful impacts caused by coincident high charger power demand of PEVs include line and transformer overloading, low voltages and increased losses. As a consequence, the PEVs are encouraged to charge at lower power level to minimize the above impacts. The strictly monotone increasing function $g_{demand,it}(u_{it})$ is introduced to describe the distribution-level cost corresponding to the charging power u_{it} of the PEV i at time t . Moreover, the battery degradation cost $g_{cell,i}(u_{it}) = a_n u_{it}^2 + b_n u_{it} + c_n$ with the constants a_n , b_n and c_n represents the monetary loss of PEV i charging at the rate of u_{it} for the period ΔT as shown in [24]. The individual local cost of PEV i at time t considering the distribution level cost and battery degradation is obtained as

$$g_{it}(u_{it}) = g_{demand,it}(u_{it}) + g_{cell,i}(u_{it}) \quad (3)$$

The individual local cost function $g_{it}(\cdot)$ is assumed to be monotonically increasing, strictly convex and differentiable for all i and t .

According to Reference [9], the benefit function of the PEV i with respect to the total energy delivered over the charging horizon is defined as

$$h_i(\|\mathbf{u}_i\|_1) = -\delta_i(\|\mathbf{u}_i\|_1 - \Gamma_i)^2 \quad (4)$$

where the positive constant δ_i denotes the the relative importance of delivering the full charge to the PEV i .

Based on Equations (3) and (4), the utility function of individual PEV i for the charging strategy $\mathbf{u}_i$ over the charging horizon satisfies

$$v_i(\mathbf{u}_i) = h_i(\|\mathbf{u}_i\|_1) - \sum_{t \in \mathcal{T}} g_{it}(u_{it}) \quad (5)$$

2.2. Communication Network for PEVs Interaction

In order to implement the distributed coordination of PEV charging, the information should be transmitted among the PEVs through the communication network whose topology can be described by an undirected graph $\mathcal{G} = (\mathcal{V}, \mathcal{E}, A)$. The node set $\mathcal{V} = \{1, 2, \dots, n\}$ contains all of the n PEVs, and the edge set $\mathcal{E} = \{(i, j) | i \rightarrow j\}$ contains all the communication links in $\mathcal{G}$ where the symbols $i \rightarrow j$ mean that the information of PEV i can be transmitted to PEV j directly through communication network. Noted that $(i, j) \in \mathcal{E}$ if and only if $(j, i) \in \mathcal{E}$ since graph $\mathcal{G}$ is undirected. The neighboring set of PEV i in communication network $\mathcal{G}$ is defined as $N_i = \{j \in \mathcal{V} | (j, i) \in \mathcal{E}\}$, and its cardinal number is $|N_i|$. The element a_{ij} in matrix $A = \{a_{ij}\} \in R^{n \times n}$ indicates the positive weight of edge (j, i) . Mentioned that $a_{ij} > 0$ if and only if $(j, i) \in \mathcal{E}$, otherwise $a_{ij} = 0$.

2.3. Formulation of Distributed Coordination about PEVs Charging

The coordination of PEV charging studies the trade-off between the total cost and the benefit of supplying energy to the PEVs. Considering the utility function (5) and the generation cost function $c(\cdot)$, the system cost function of PEVs coordinated charging is given as

$$J(\mathbf{u}) = \sum_{t \in \mathcal{T}} c(d_t + \sum_{i \in \mathcal{V}} u_{it}) - \sum_{i \in \mathcal{V}} v_i(\mathbf{u}_i) \quad (6)$$

where the admissible charging strategies $\mathbf{u} = \{\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_n\} \in \mathcal{U}$ satisfy $\mathbf{u}_i \in \mathcal{U}_i$, the quadratic function $c(y_t) = \frac{1}{2}\alpha y_t^2 + \beta y_t + \gamma$ with constants α, β and γ approximates the generation cost with respect to the aggregate demand $y_t = d_t + \sum_{i \in \mathcal{V}} u_{it}$ based on the analysis in [25,26], and the function d_t indicates the aggregate inelastic base demand at time t .

The objective of PEV coordinated charging is to implement a socially optimal collection of charging strategies for all participating PEVs to minimize the system cost function (6) under the restricted condition (1) and (2), which is characterized as the following optimization problem

$$\min_{\mathbf{u} \in \mathcal{U}} J(\mathbf{u}) \quad (7)$$

By introducing the price profile and consensus based price update process, the following Algorithm 1 was constructed in [15] to address the distributed coordination of PEV charging under the parameter restriction $A\mathbf{1} = \mathbf{1}, \mathbf{1}^T A = \mathbf{1}^T$ and $|1 - \eta| + 2n\kappa\nu\eta < 1$ where the n -dimensional vector $\mathbf{1} = \{1, 1, \dots, 1\}^T$, κ is the Lipschitz constant of derived function $c'(\cdot)$, and $\nu = \max_{i \in \mathcal{V}, t \in \mathcal{T}} \nu_{it}$ where ν_{it} is the Lipschitz constant of the function $[g'_{it}]^{-1}(\cdot)$ over the interval $[g'_{it}(0), g'_{it}(\Gamma_i)]$. The optimal charging strategy for each PEV can be obtained until the change in price profile is negligible.

Algorithm 1 satisfies the requirement of distributed architecture since the control center unit is nonexistent and each PEV updates its own individual electricity price $\hat{\mathbf{p}}_i$ based on neighborhood information transmission through communication network $\mathcal{G}$ as shown in (10). Mentioned that the information transmission in Algorithm 1 is required to be ideal. However, the communication network is vulnerable to cyber-attack usually in practical application, and the attack launched by adversary may deteriorate the performance of distributed consensus protocol (10) and even cause the failure of PEV charging coordination. This signifies that the security issue should be a major concern. In the next sections, the modality and impact of cyber-attack on Algorithm 1 will be analyzed, and then the resilient PEV charging coordination scheme will be constructed to resist the cyber-attack.

Algorithm 1: Distributed coordination of PEV charging without the consideration of cyber-attack.

- Specify the aggregate inelastic base demand $\mathbf{d} = (d_t, t \in \mathcal{T})$, total number of PEVs n , time horizon $\mathcal{T}$ and parameter η ;
- Define the allowable deviations ϵ_{stop} and ϵ_{stop} to terminate iterations;
- Initialize the initial common electricity price $\mathbf{p}^0 = (p_t^0, t \in \mathcal{T})$, $\epsilon > \epsilon_{stop}$ and $m = 0$;
- WHILE $\epsilon > \epsilon_{stop}$
 - Determine the charging profile $\mathbf{u}_i^{m+1}$ w.r.t. $\mathbf{p}^m$ for all PEVs $i \in \mathcal{V}$ simultaneously by minimizing the individual cost function

$$\mathbf{u}_i^{m+1}(\mathbf{p}^m) = \arg \min_{\mathbf{u}_i \in \mathcal{U}_i} \left\{ \sum_{t \in \mathcal{T}} p_t^m u_{it} - v_i(\mathbf{u}_i) \right\} \quad (8)$$

- Initialize $\epsilon > \epsilon_{stop}$ and $l = 0$;
- Initialize the initial individual electricity price $\hat{\mathbf{p}}_i(0) = (\hat{p}_{it}(0), t \in \mathcal{T})$ for each PEV $i \in \mathcal{V}$ and $t \in \mathcal{T}$ as

$$\hat{p}_{it}(0) = p_t^m + \eta(c'(d_t + n \cdot u_{it}^{m+1}) - p_t^m) \quad (9)$$

- WHILE $\epsilon > \epsilon_{stop}$
 - * Update the individual price $\hat{\mathbf{p}}_i(l) = (\hat{p}_{it}(l), t \in \mathcal{T})$ by executing the distributed consensus protocol at each PEV $i(i \in \mathcal{V})$ and time $t \in \mathcal{T}$ as

$$\hat{p}_{it}(l+1) = \sum_{j \in \mathcal{V}} a_{ij} \hat{p}_{jt}(l) \quad (10)$$

- * Update $\epsilon = \max_i \{\|\hat{\mathbf{p}}_i(l+1) - \hat{\mathbf{p}}_i(l)\|_1\}$;
 - * Update $l = l + 1$;
 - END WHILE
 - Specify the common price $\mathbf{p}^{m+1} = \hat{\mathbf{p}}_i(l)$;
 - Update $\epsilon = \|\mathbf{p}^{m+1} - \mathbf{p}^m\|_1$;
 - Update $m = m + 1$;
 - END WHILE
 - Specify the optimal charging strategy as $\mathbf{u}_i^m$ for PEV $i(i \in \mathcal{V})$.
-

3. Cyber-Attack against PEVs Charging Coordination

The distributed consensus protocol (10) in Algorithm 1 aims to drive the individual electricity price $\hat{p}_{it}$ of each PEV i to the average value (11) of all participating PEVs' initial individual prices by neighborhood information transmission through communication network $\mathcal{G}$. This is the precondition of solving the optimization problem (7), and more details can be found in [15].

$$\hat{p}_t^* = \frac{1}{n} \sum_{i \in \mathcal{V}} \hat{p}_{it}(0) = \frac{1}{n} \sum_{i \in \mathcal{V}} \left(p_t^m + \eta(c'(d_t + n \cdot u_{it}^{m+1}) - p_t^m) \right) \quad (11)$$

Considering the communication network suffering from cyber-attack, the distributed consensus protocol (10) in Algorithm 1 is affected as

$$\hat{p}_{it}(l+1) = \sum_{j \in \mathcal{V}} a_{ij} \hat{p}_{jt}(l) + u_{it}^a(l) \quad (12)$$

where $u_{it}^a(l)$ denotes the attack injection acting on individual price $\hat{p}_{it}$ of PEV i at iteration l . The aim of attack injection is to affect the convergence of consensus protocol and modify the convergent value (11), and finally destroy the effectiveness of Algorithm 1.

It can be seen from (12) that the attack injection $u_{it}^a(l)$ determines whether the PEV i suffers from cyber-attack. Moreover, the injection $u_{it}^a(l)$ describes the attack type launched by adversary. The injection $u_{it}^a(l) = -a_{ij}\hat{p}_{jt}(l)$ means the PEV j is under DoS attack since the information sent from PEV j to i is erased at iteration l . The injection $u_{it}^a(l) = c - \sum_{j \in \mathcal{V}} a_{ij}\hat{p}_{jt}(l)$ for all iterations l implies the PEV i is under replay attack with the replay signal c . The random $u_{it}^a(l)$ denotes the random attack on PEV i , and $u_{it}^a(l) = c_{it}(l)$ demonstrates PEV i suffers from false data injection attack with the designed injection $c_{it}(l)$.

The replay attack is given as an illustration to explain the impact of cyber-attack on distributed charging coordination scheme Algorithm 1. Denoting $\mathcal{M}$ and $\mathcal{H}$ as the sets of misbehaving PEVs under replay attack and well-behaving PEVs respectively, the distributed consensus protocols in Algorithm 1 is affected as

$$\begin{cases} \hat{p}_{it}(l+1) = \sum_{j \in \mathcal{V}} a_{ij}\hat{p}_{jt}(l), & i \in \mathcal{H} \\ \hat{p}_{it}(l+1) = \hat{p}_{it}^a, & i \in \mathcal{M} \end{cases} \quad (13)$$

where $\mathcal{H} \cap \mathcal{M} = \emptyset$, $\mathcal{H} \cup \mathcal{M} = \mathcal{V}$, and $\hat{p}_{it}^a$ is the replay fake electricity price of the misbehaving PEV i ($i \in \mathcal{M}$). According to Theorem 1 in [27], we can get that the individual electricity price of each well-behaving PEV converges into the convex hull $co\{\hat{p}_{jt}^a, j \in \mathcal{M}\}$ spanned by the fake prices of misbehaving PEVs, i.e.,

$$\lim_{l \rightarrow \infty} \hat{p}_{it}(l) = \sum_{j \in \mathcal{M}} c_{ij}\hat{p}_{jt}^a, \quad i \in \mathcal{H} \quad (14)$$

where the constants $c_{ij} \geq 0$ ($\forall j \in \mathcal{M}$) and they satisfy $\sum_{j \in \mathcal{M}} c_{ij} = 1$ for each i .

We can consider two cases. The first case is that there exist multiple PEVs under replay attack and the fake prices of these misbehaving PEVs are unequal. This results in the individual electricity prices of all PEVs converging into the convex hull $co\{\hat{p}_{jt}^a, j \in \mathcal{M}\}$, which implies that these prices cannot achieve consensus. This further means that $\epsilon > \epsilon_{stop}$ in Algorithm 1 for any times of iteration, which makes the algorithm loop infinitely and fail. The other case is that the fake prices of all the misbehaving PEVs are equal or there is only one PEV under replay attack. Denoting the fake price of misbehaving PEVs as $\hat{p}_t^{replay}$, it can be obtained from (14) that the convex hull $co\{\hat{p}_{jt}^a, j \in \mathcal{M}\}$ degrades into the value $\hat{p}_t^{replay}$, and the individual electricity prices of all PEVs converge to $\hat{p}_t^{replay}$. Although the consensus price can be ensured in this case, the average value $\hat{p}_t^*$ in (11) cannot be achieved since $\hat{p}_t^{replay}$ is unequal to $\hat{p}_t^*$ usually. It mismatches the precondition of solving the optimization problem (7) and leads to the failure of coordination of PEV charging.

Case application: Consider the communication network of five PEVs shown in Figure 1, and PEV 2 is assumed suffering from replay attack with the replay fake electricity price $\hat{p}_t^{replay} = \$0.9/\text{kWh}$. The impact of replay attack on Algorithm 1 is illustrated in this case application. The generation and individual local costs satisfy $c(y_t) = 2.9 \times 10^{-4}y_t^2 + 0.06y_t$ and $g_{it}(u_{it}) = 0.003u_{it}^2 + 0.11u_{it} - 0.02$ respectively. The battery capacity of each PEV is 40 kWh and the weight fact in (4) is set as $\delta_i = 0.03$. Assuming the initial and maximum state-of-charge (SoC) of each PEV as $soc_0 = 15\%$ and $soc_h = 90\%$ respectively, the energy capacity which can be delivered is calculated as $\Gamma_i = 40(soc_h - soc_0)\text{kWh} = 30 \text{ kWh}$ for all $i \in \mathcal{V}$. The aggregate inelastic base demand $\mathbf{d}$ is shown in Figure 2 which is representative of a typical hot summer day.

The charging strategy given by Algorithm 1 results in the aggregate demand shown in Figure 2, where the results in cases of no attack and replay attack are illustrated in Figure 2a,b respectively. It can be seen that the aggregate demands in these two cases are different under the same distributed PEV charging coordination scheme Algorithm 1. The system cost function (6) can be quantified according to the simulation result as $J(\mathbf{u}^a) = \$209.66/\text{day}$ and $J(\mathbf{u}) = \$183.51/\text{day}$ where $J(\mathbf{u}^a)$ denotes the system cost function under replay attack and $J(\mathbf{u})$ denotes that without attack. The overall waste caused by

replay attack is then calculated as $J(\mathbf{u}^a) - J(\mathbf{u}) = \$26.15/\text{day}$, which reveals the negative effects of replay attack against Algorithm 1.

Figure 1. Communication topology of five plug-in electric vehicles (PEVs).

Figure 2. Aggregate demand for Algorithm 1. (a) Without replay attack; (b) under replay attack.

Figures 3 and 4 illustrate the SoC and common electricity price evolution of each PEV under the two cases respectively. Since PEV 2 suffers from the replay attack with replay fake price $\hat{p}_t^{\text{replay}} = \$0.9/\text{kWh}$, the common electricity price obtained from Algorithm 1 is equal to $\hat{p}_t^{\text{replay}}$ in the whole charging horizon $\mathcal{T}$ as shown in Figure 4b. The comparison between Figure 4a,b demonstrates that

the adjusting ability of common electricity price with respect to charging profile is lost under the influence of replay attack, and the average common price (11) cannot be obtained under Algorithm 1. It further results that the optimal charging profile obtained from (8) with respect to the average common price (11) cannot be achieved as shown in Figure 3, which makes the overall waste \$26.15/day. This case application indicates that the PEV charging strategy profile calculated by Algorithm 1 under replay attack is not the solution of optimization problem (7), and the effectiveness of distributed PEV charging coordination scheme Algorithm 1 is damaged under replay attack.

Figure 3. Evolution of the PEV's state-of-charge (SoC) for Algorithm 1. (a) Without replay attack; (b) under replay attack.

Figure 4. Common electricity price updates for Algorithm 1. (a) Without replay attack; (b) under replay attack.

4. Resilient Distributed Coordination of PEVs Charging

This section proposes the resilient distributed consensus protocol to resist cyber-attack, and then the resilient distributed coordination scheme of PEV charging is constructed based on this novel consensus protocol. Within this resilient protocol, a confidence level is introduced to identify how healthy each participating PEV is, and the confidence level is dynamic updated in real-time based on attack detection mechanism. When some certain PEV is detected to suffer from cyber-attack, its confidence level is decreased to reduce its negative effect on the other PEVs. Consequently, the misbehaving PEV under cyber-attack is gradually marginalized and finally isolated from the charging system. The remaining well-behaving PEVs recover and update their individual electricity price to attain the new common average electricity price without the influence of cyber-attack. The detailed description of resilient distributed consensus protocol is given as follows, where the steps of detection, isolation, updating and recovery are included and constructed synthetically.

4.1. Detection of Cyber-Attack

In this step, each PEV i transmits the received neighboring PEVs' individual electricity prices $\hat{p}_{kt}(l) (k \in N_i)$ and its own individual electricity price $\hat{p}_{it}(l+1)$ to each of its neighboring PEV $j (j \in N_i)$

at each iteration l , where the price $\hat{p}_{it}(l+1)$ is calculated at iteration l by the resilient consensus protocol designed later. Based on the received information from the neighboring PEVs, PEV i executes the following attack detection mechanism

$$H_{ij}(l) = \begin{cases} H_{ij}(l-1) + 1, & |\sum_{k \in \mathcal{V}} a_{jk}(l) \hat{p}_{kt}(l) - \hat{p}_{jt}(l+1)| \leq \theta \\ H_{ij}(l-1), & |\sum_{k \in \mathcal{V}} a_{jk}(l) \hat{p}_{kt}(l) - \hat{p}_{jt}(l+1)| > \theta \end{cases} \quad (15)$$

where $H_{ij}(l)$ denotes the total number of verifiable correct price of the neighboring PEV j monitored by PEV i up to iteration l with the initial value $H_{ij}(0) = 0$, the positive constant θ represents the threshold and $a_{jk}(l)$ is the positive weight of edge (k, j) in communication network $\mathcal{G}$ at iteration l .

It should be mentioned that $\sum_{k \in \mathcal{V}} a_{jk}(l) \hat{p}_{kt}(l)$ in (15) is the expected normal price of PEV j at iteration $(l+1)$ in the absence of cyber-attack, while $\hat{p}_{jt}(l+1)$ is the actual price of PEV j at iteration $(l+1)$ which may be affected by cyber-attack injection $u_{jt}^a(l)$ as shown in (12). The attack detection mechanism (15) counts the number of verifiable correct price of PEV j according to the difference between these two types of prices in the whole iterative process, where the difference threshold θ is introduced to reduce the false positives caused by some normal disturbance. Based on detection mechanism (15), the PEV i constructs an index H_{ij} to each of its neighboring PEV j .

4.2. Isolation of Misbehaving PEVs

PEV i calculates and stores a confidence level to quantitatively measure the credibility for each of its neighboring PEV j in this step. The confidence level is calculated as (16) according to Bayesian Reputation function [28] based on the ratio of the number of verifiable correct price H_{ij} in (15) to the total number of price received.

$$conf_{ij}(l) = \frac{\mu H_{ij}(l) + 1}{\mu l + 2} \quad (16)$$

where $conf_{ij}(l)$ denotes the confidence level of PEV j calculated at PEV i at iteration l , and the positive coefficient μ is used to adjust the gradient of confidence level. It should be mentioned that $0 < conf_{ij}(l) < 1$ for all edges $(j, i) \in \mathcal{E}$ and iterations l .

The confidence level reflects the healthy degree of neighboring PEV. It can be seen from (16) that the confidence level $conf_{ij}$ decreases if the misbehaving PEV j is detected with abnormal price by attack detection mechanism (15) configured at PEV i , otherwise the confidence level $conf_{ij}$ increases. If the confidence level $conf_{ij}$ falls below the proposed anomaly threshold Θ , i.e., $conf_{ij} < \Theta$, the PEV j is identified to be attacked and it will be isolated from the communication network and physically disconnected from the PEV charging system. The anomaly threshold Θ is selected with weighting the false reject rate and the false accept rate in the practical application.

4.3. Updating and Recovery of Distributed Consensus Protocol

For the remaining PEVs after the isolation step, the weight $a_{ij}(l)$ is given as follows

$$a_{ij}(l) = \min \left\{ \frac{conf_{ij}(l)}{\xi \sum_{j \in N_i} conf_{ij}(l)}, \frac{conf_{ji}(l)}{\xi \sum_{i \in N_j} conf_{ji}(l)} \right\} \quad (17)$$

where the constant $\xi > 1$. Denoting the set containing all of the remaining PEVs as $\tilde{\mathcal{V}}$, the resilient distributed consensus protocol for the updating of PEVs' individual electricity prices is constructed as

$$\hat{p}_{it}(l+1) = \sum_{j \in \tilde{\mathcal{V}}} a_{ij}(l) \hat{p}_{jt}(l) \quad (18)$$

where the weight $a_{ii}(l) = 1 - \sum_{j \in \tilde{\mathcal{V}}, j \neq i} a_{ij}(l)$ for all $i \in \tilde{\mathcal{V}}$.

Theorem 1. Denoting the initial individual electricity price of PEV i in set $\tilde{\mathcal{V}}$ as $\hat{p}_{it}(l_0)$ where the initial iteration l_0 is the time when the last misbehaving PEV is isolated, the resilient distributed consensus protocol (18) drives the individual electricity price of each PEV to the average value of initial prices, i.e., $\lim_{l \rightarrow +\infty} \hat{p}_{it}(l) = \frac{1}{|\tilde{\mathcal{V}}|} \sum_{i \in \tilde{\mathcal{V}}} \hat{p}_{it}(l_0)$ for each $i \in \tilde{\mathcal{V}}$ where $|\tilde{\mathcal{V}}|$ is the cardinal number of set $\tilde{\mathcal{V}}$, provided that the remaining communication network is still connected after the isolation of misbehaving PEVs.

Proof. The isolation process described in Section 4.2 and the definition of confidence level (16) indicate that

$$\Theta \leq \text{conf}_{ij}(l) \leq 1 \quad (19)$$

for all $(j, i) \in \mathcal{E}$ where $i, j \in \tilde{\mathcal{V}}$. Formula (19) means that

$$n\tilde{\zeta}\Theta \leq \tilde{\zeta} \sum_{j \in N_i} \text{conf}_{ij}(l) \leq n\tilde{\zeta} \quad (20)$$

Combining (19), (20) and (17) yields

$$\frac{\Theta}{n\tilde{\zeta}} \leq a_{ij}(l) \leq \frac{1}{n\tilde{\zeta}\Theta} \quad (21)$$

The definition of $a_{ii}(l)$ leads to

$$1 \geq a_{ii}(l) \geq 1 - \sum_{j \in \tilde{\mathcal{V}}, j \neq i} \frac{\text{conf}_{ij}(l)}{\tilde{\zeta} \sum_{j \in N_i} \text{conf}_{ij}(l)} = 1 - \frac{1}{\tilde{\zeta}} \quad (22)$$

Inequalities (21) and (22) imply that $\min\{\frac{\Theta}{n\tilde{\zeta}}, 1 - \frac{1}{\tilde{\zeta}}\} \leq a_{ij}(l) \leq \max\{\frac{1}{n\tilde{\zeta}\Theta}, 1\}$ for any node $i, j \in \tilde{\mathcal{V}}$ and iteration l . This together with the fact $\sum_{j \in \tilde{\mathcal{V}}} a_{ij}(l) = 1$ for all $i \in \tilde{\mathcal{V}}$ indicates that the individual electricity price $\hat{p}_{it}(l)$ of each PEV converges to a common value $\hat{p}_t^{\text{com}}$ as $l \rightarrow +\infty$ according to Proposition 2 in [29]. Furthermore, it can be seen from (18) that

$$\frac{1}{|\tilde{\mathcal{V}}|} \sum_{i \in \tilde{\mathcal{V}}} \hat{p}_{it}(l+1) = \frac{1}{|\tilde{\mathcal{V}}|} \sum_{i \in \tilde{\mathcal{V}}} \sum_{j \in \tilde{\mathcal{V}}} a_{ij}(l) \hat{p}_{jt}(l) = \frac{1}{|\tilde{\mathcal{V}}|} \sum_{j \in \tilde{\mathcal{V}}} \left(\sum_{i \in \tilde{\mathcal{V}}} a_{ij}(l) \right) \hat{p}_{jt}(l) = \frac{1}{|\tilde{\mathcal{V}}|} \sum_{j \in \tilde{\mathcal{V}}} \hat{p}_{jt}(l) = \frac{1}{|\tilde{\mathcal{V}}|} \sum_{i \in \tilde{\mathcal{V}}} \hat{p}_{it}(l) \quad (23)$$

Equation (23) means $\frac{1}{|\tilde{\mathcal{V}}|} \sum_{i \in \tilde{\mathcal{V}}} \hat{p}_{it}(l)$ is constant for all iteration l and thus we have $\frac{1}{|\tilde{\mathcal{V}}|} \sum_{i \in \tilde{\mathcal{V}}} \hat{p}_{it}(l) \equiv \frac{1}{|\tilde{\mathcal{V}}|} \sum_{i \in \tilde{\mathcal{V}}} \hat{p}_{it}(l_0)$ for any $l \in [l_0, +\infty)$. This implies $\hat{p}_t^{\text{com}} = \frac{1}{|\tilde{\mathcal{V}}|} \sum_{i \in \tilde{\mathcal{V}}} \hat{p}_{it}(l_0)$ by the help of [30,31], which concludes the proof. $\square$

Remark 1. Formula (17) guarantees $a_{ij}(l) = a_{ji}(l)$ for any edge (j, i) and iteration l , which realizes the weight balance of the remaining communication network, i.e., $\sum_{j \in \tilde{\mathcal{V}}} a_{ij}(l) = \sum_{j \in \tilde{\mathcal{V}}} a_{ji}(l)$ for all $i \in \tilde{\mathcal{V}}$. This is the precondition of average consensus as shown in the proof of Theorem 1.

Remark 2. The selection method of weight $a_{ij}(l)$ given in (17) demonstrates the ability of the proposed resilient distributed consensus algorithm in adaptive adjusting weight based on confidence level. If PEV j is detected by PEV i with low confidence level conf_{ij} , the weight a_{ij} in communication network is decreased. The protocol (18) implies that the decreased weight a_{ij} mitigates the effects of PEV j 's abnormal individual price information on the entire system. As a consequence, the spread speed of the negative effect caused by the potential misbehaving PEV is restrained.

Although the individual electricity prices of the remaining well-behaving PEVs converge to $\hat{p}_t^{\text{com}} = \frac{1}{|\tilde{\mathcal{V}}|} \sum_{i \in \tilde{\mathcal{V}}} \hat{p}_{it}(l_0)$ under the protocol (18), the convergent value $\hat{p}_t^{\text{com}}$ may be not the desired one $\hat{p}_t^* = \frac{1}{|\tilde{\mathcal{V}}|} \sum_{i \in \tilde{\mathcal{V}}} \hat{p}_{it}(0)$ given in (11) which is required by distributed PEV charging coordination. The reason is that the misbehaving PEVs are not fully isolated in the iteration interval $[0, l_0)$, and the contribution of them has already affected the average consensus computation. Therefore, a rollback

recovery mechanism should be introduced to set $\hat{p}_{it}(l_0) = \hat{p}_{it}(0)$ for each well-behaving PEVs i ($i \in \tilde{\mathcal{V}}$) in order to restore the average common price $\hat{p}_t^{com}$ to the desired value $\hat{p}_t^*$. The implementation of recovery mechanism requires each PEV i to save its own initial individual electricity price $\hat{p}_{it}(0)$. When the misbehaving PEV is isolated, the current individual price of each remaining PEV i is replaced by the saved initial one $\hat{p}_{it}(0)$ and the resilient distributed consensus protocol is resumed.

Integrating the above steps of detection, isolation, updating and recovery, the resilient distributed consensus protocol of PEVs' individual electricity prices is given in the following Algorithm 2.

Algorithm 2: Resilient distributed consensus protocol of PEVs' individual electricity price.

- Specify the aggregate inelastic base demand $\mathbf{d} = (d_t, t \in \mathcal{T})$, total number of the remaining well-behaving PEVs $\tilde{n}$, time horizon $\mathcal{T}$ and parameter η, μ and ζ ;
 - Define the allowable deviation ϵ_{stop} to terminate iterations;
 - Specify the thresholds θ and Θ ;
 - Specify the common electricity price $\tilde{\mathbf{p}} = (\tilde{p}_t, t \in \mathcal{T})$ and the corresponding optimal charging profile $\tilde{\mathbf{u}}_i(\tilde{\mathbf{p}}) = (\tilde{u}_{it}(\tilde{\mathbf{p}}), t \in \mathcal{T})$;
 - Initialize $\epsilon > \epsilon_{stop}$ and $l = 0$;
 - Initialize the initial individual electricity price $\hat{\mathbf{p}}_i(0) = (\hat{p}_{it}(0), t \in \mathcal{T})$ for each PEV $i \in \tilde{\mathcal{V}}$ and $t \in \mathcal{T}$ as $\hat{p}_{it}(0) = \tilde{p}_t + \eta(c'(d_t + \tilde{n} \cdot \tilde{u}_{it}(\tilde{\mathbf{p}})) - \tilde{p}_t)$;
 - WHILE $\epsilon > \epsilon_{stop}$
 - Update the total number of verifiable correct price $H_{ij}(l)$ using (15);
 - Update the confidence level $conf_{ij}(l)$ using (16);
 - IF $conf_{ij}(l) < \Theta$, THEN
 - * Isolate PEV j from the communication network and disconnect it physically from the PEV charging system;
 - * Replace the current price of the remaining PEVs by the initial value such that $\hat{p}_{it}(l) = \hat{p}_{it}(0)$ for each i ;
 - END IF
 - Update the weight $a_{ij}(l)$ of edge (j, i) using (17);
 - Calculate the weight $a_{ii}(l) = 1 - \sum_{j \neq i} a_{ij}(l)$;
 - Update the individual electricity price $\hat{\mathbf{p}}_i(l) = (\hat{p}_{it}(l), t \in \mathcal{T})$ by executing (18) at each remaining PEV i and time $t \in \mathcal{T}$;
 - Update $\epsilon = \max_i \{\|\hat{\mathbf{p}}_i(l+1) - \hat{\mathbf{p}}_i(l)\|_1\}$;
 - Update $l = l + 1$;
 - END WHILE
 - Specify the common price $\hat{\mathbf{p}}^* = \hat{\mathbf{p}}_i(l)$.
-

4.4. Resilient Distributed PEVs Charging Coordination

Algorithm 3 represents the resilient distributed coordination of PEV charging considering cyber-attack based on the consensus protocol shown in Algorithm 2. Since Algorithm 2 can drive the common electricity price to the average value of all remaining well-behaving PEVs' initial individual electricity prices as illustrated in Theorem 1, the following main theorem can be obtained obviously and the proof is omitted. The flowchart of the proposed resilient distributed coordinated charging scheme containing Algorithm 2 and 3 is shown in Figure 5.

Theorem 2. Supposing the positive constant η satisfies $|1 - \eta| + 2n\kappa v\eta < 1$ and the remaining communication network is connected, Algorithm 3 guarantees the optimal charging strategy $\mathbf{u}_i^* = (u_{it}^*, t \in \mathcal{T})$ for each remaining well-behaving PEV i even under cyber-attack, which is the solution of optimization problem (7).

Figure 5. The flowchart of resilient distributed coordination of PEV charging.

Algorithm 3: Resilient distributed coordination of PEV charging considering cyber-attack.

- Specify the aggregate inelastic base demand $\mathbf{d} = (d_t, t \in \mathcal{T})$, total number of PEVs n , time horizon $\mathcal{T}$ and parameter η ;
- Define the allowable deviation ε_{stop} to terminate iterations;
- Initialize the initial common electricity price $\mathbf{p}^0 = (p_t^0, t \in \mathcal{T})$, $\varepsilon > \varepsilon_{stop}$ and $m = 0$;
- WHILE $\varepsilon > \varepsilon_{stop}$
 - Determine the charging profile $\mathbf{u}_i^{m+1}$ w.r.t. $\mathbf{p}^m$ for all PEVs simultaneously by minimizing the individual cost function
$$\mathbf{u}_i^{m+1}(\mathbf{p}^m) = \arg \min_{\mathbf{u}_i \in \mathcal{U}_i} \left\{ \sum_{t \in \mathcal{T}} p_t^m u_{it} - v_i(\mathbf{u}_i) \right\}$$
 - Specify the price $\tilde{\mathbf{p}} = \mathbf{p}^m$ and the corresponding charging profile $\tilde{\mathbf{u}}_i(\tilde{\mathbf{p}}) = \mathbf{u}_i^{m+1}(\mathbf{p}^m)$, and input $\tilde{\mathbf{p}}$ and $\tilde{\mathbf{u}}_i(\tilde{\mathbf{p}})$ into Algorithm 2;
 - Determine the common electricity price $\mathbf{p}^{m+1}$ by the output of Algorithm 2 such that $\mathbf{p}^{m+1} = \hat{\mathbf{p}}^*$;
 - Update $\varepsilon = \|\mathbf{p}^{m+1} - \mathbf{p}^m\|_1$;
 - Update $m = m + 1$;
- END WHILE
- Specify the optimal charging strategy as $\mathbf{u}_i^* = \mathbf{u}_i^m$ for the remaining well-behaving PEV i .

5. Simulation

This section verifies the effectiveness of Algorithm 3 by numerical simulation of five PEVs with the communication network shown in Figure 1, where the issue of cyber-attack is considered. The generation cost function $c(y_t)$, individual local cost function $g_{it}(u_{it})$, aggregate inelastic based demand $\mathbf{d}$, energy capacity Γ_i and weight fact δ_i in (4) are the same with those in the case application given in Section 3. The parameter $\eta = 1$ in Algorithm 3 to satisfy $|1 - \eta| + 2n\kappa\nu\eta < 1$ where $n = 5$, $\kappa = 5.8 \times 10^{-4}$ and $\nu = 166.7$ calculated from the above given functions. The parameters satisfy $\mu = 0.5$ in (16) and $\zeta = 2$ in (17). The allowable deviations are set as $\varepsilon_{stop} = 0.001$ and $\epsilon_{stop} = 0.002$, and the thresholds are selected as $\theta = 0.1$ and $\Theta = 0.25$ respectively.

5.1. Response under Replay Attack

In this scenario PEV 2 suffered from replay attack with the replay fake electricity price $\hat{p}_t^{replay} = \$0.9/\text{kWh}$, which is the same with that in the case application of Section 3. Figure 6 illustrates the evolution of weight $a_{ij}(l)$ in each edge (j, i) in communication network under the execution of Algorithm 3, where only the weights of six edges were displayed instead of all 12 edges since $a_{ij}(l) = a_{ji}(l)$. It should be mentioned that the weights of edges connected to PEV 2 decreased and these weights finally achieved 0 at the 13th step of iteration shown in Figure 6. This demonstrates that the misbehaving PEV 2 was detected to be attacked and then it was isolated from the communication network under Algorithm 3, which prevented it from negatively affecting the other PEVs.

Figure 7 shows that the common electricity price could still be adjusted adaptively with respect to charging profile under Algorithm 3 even under replay attack, which is different to the result shown in Figure 4b where the price was fixed by the fake replay signal $\$0.9/\text{kWh}$ under Algorithm 1. This implies that each PEV could obtain its own optimal charging strategy according to the dynamical common price under Algorithm 3 as shown in the evolution of SoC illustrated in Figure 8, and it is different to the constant power charging strategy under Algorithm 1 shown in Figure 3b where the economy was destroyed under replay attack. The aggregate demand under Algorithm 3 is given by Figure 9, and it can be obtained that the system cost function satisfied $J(\mathbf{u}^r) = \$177.82/\text{day}$ where the optimal charging strategy $\mathbf{u}^r$ is given by Algorithm 3. Algorithm 3 saved the total cost $J(\mathbf{u}^a) - J(\mathbf{u}^r) = \$31.84/\text{day}$ compared with Algorithm 1 under replay attack. Moreover, the charging strategy for four PEVs calculated

under Algorithm 1 without replay attack was the same as shown in Figure 8. This further demonstrates that the optimal charging strategy can be realized for Algorithm 3 after the isolation of misbehaving PEV 2.

Figure 6. Edge weights update for Algorithm 3 under replay attack.

Figure 7. Common electricity price updates for Algorithm 3 under replay attack or random attack.

Figure 8. Evolution of the PEV's SoC for Algorithm 3 under replay attack or random attack.

Figure 9. Aggregate demand for Algorithm 3 under replay attack or random attack.

5.2. Response under Random Attack

In this scenario, PEV 4 suffered from random attack so that it could randomly set its individual electricity price $\hat{p}_{4t}(l)$ which was a random number satisfying the normal distribution $N(0.1, 0.03)$ at each iteration l . Because of the stochastic behavior of $\hat{p}_{4t}(l)$, the simulation result indicated that it always had $\epsilon > \epsilon_{stop}$ for any step of iteration under Algorithm 1. This implies that the convergent common price within acceptable deviation range could not be obtained and it led to the failure of Algorithm 1. Algorithm 1 fell into an endless loop under random attack and the optimal charging strategy could not be acquired. On the other hand, the simulation result for Algorithm 3 under this random attack was the same as those shown in Figures 7–9, and the evolution of edge weights is given in Figure 10. This illustrates that the weights of edges connecting to the misbehaving PEV 4 achieved 0 at the 9th step of iteration, and PEV 4 was detected to be under attack and finally isolated by Algorithm 3. Moreover, the remaining well-behaving four PEVs obtained the optimal charging strategy. It verified the effectiveness of the proposed resilient distributed PEV charging coordination scheme Algorithm 3 under random attack.

Figure 10. Edge weights update for Algorithm 3 under random attack.

6. Conclusions

The resilient distributed PEV charging coordination in the presence of cyber-attack is studied in this paper, where the trade-off between total generation cost and local cost associated with overloading and battery degradation is considered. The cyber-attack tampers the individual electricity price by injecting unauthorized attack data to exert its negative influence. In order to resist the cyber-attack, a novel type of resilient charging coordination scheduling method is constructed which contains the steps of detection, isolation, updating and recovery. It is proved theoretically that the misbehaving PEVs under cyber-attack are gradually marginalized and finally isolated according to its real-time updated confidence level, and the remaining well-behaving PEVs obtain their optimal charging strategy to minimize the total system cost in distributed architecture. The simulation result confirms the effectiveness of theoretical method.

Some of the future directions of the present research are given as follows. (i) The unified cooperative optimal dispatch between charging of PEVs and power generation of microgrids cluster can be explored; (ii) The cyber-attack with stealthy characteristic which can cheat the attack detection mechanism should be studied in the PEV charging coordination; (iii) The proposed resilient scheduling framework can be extended considering the discharging behavior of PEV where the energy storage function of PEV is taken into account. These research directions will be considered in our future works.

Author Contributions: S.W. studied the methodology and implemented the experimental simulation. Y.L. and X.D. formulated the PEV charging model and scheduling objective. All authors have read and agreed to the published version of the manuscript.

Funding: This work was sponsored by the Science and Technology Project of NARI Technology Co. Ltd. “Research on key technologies for simulation and evaluation of comprehensive energy systems” (2019out129), Project funded by China Postdoctoral Science Foundation (2018M642294) and Jiangsu Planned Projects for Postdoctoral Research Funds (2018K006A).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Chan, C.C. The state of the art of electric, hybrid, and fuel cell vehicles. *Proc. IEEE* **2007**, *95*, 704–718. [\[CrossRef\]](#)
2. Iqbal, S.; Xin, A.; Jan, M.U.; Salman, S.; Zaki, A.M.; Rehman, H.U.; Shinwari, M.F.; Abdelbaky, M.A. V2G Strategy for Primary Frequency Control of an Industrial Microgrid Considering the Charging Station Operator. *Electronics* **2020**, *9*, 549. [\[CrossRef\]](#)

3. Lü, X.; Wu, Y.; Lian, J.; Zhang, Y.; Chen, C.; Wang, P.; Meng, L. Energy management of hybrid electric vehicles: A review of energy optimization of fuel cell hybrid power system based on genetic algorithm. *Energy Convers. Manag.* **2020**, *205*, 112474. [\[CrossRef\]](#)
4. Karmaker, A.K.; Hossain, M.A.; Manoj Kumar, N.; Jagadeesan, V.; Jayakumar, A.; Ray, B. Analysis of Using Biogas Resources for Electric Vehicle Charging in Bangladesh: A Techno-Economic-Environmental Perspective. *Sustainability* **2020**, *12*, 2579. [\[CrossRef\]](#)
5. Hadley, S.W.; Tsvetkova, A.A. Potential impacts of plug-in hybrid electric vehicles on regional power generation. *Electr. J.* **2009**, *22*, 56–68. [\[CrossRef\]](#)
6. Fernandez, L.P.; San Román, T.G.; Cossent, R.; Domingo, C.M.; Frias, P. Assessment of the impact of plug-in electric vehicles on distribution networks. *IEEE Trans. Power Syst.* **2010**, *26*, 206–213. [\[CrossRef\]](#)
7. Hermans, R.; Almassalkhi, M.; Hiskens, I. Incentive-based coordinated charging control of plug-in electric vehicles at the distribution-transformer level. In Proceedings of the 2012 American Control Conference (ACC), Montreal, QC, USA, 27–29 June 2012; pp. 264–269.
8. Wu, D.; Aliprantis, D.C.; Ying, L. Load Scheduling and Dispatch for Aggregators of Plug-In Electric Vehicles. *IEEE Trans. Smart Grid* **2012**, *3*, 368–376. doi:10.1109/TSG.2011.2163174. [\[CrossRef\]](#)
9. Han, S.; Han, S.; Sezaki, K. Development of an optimal vehicle-to-grid aggregator for frequency regulation. *IEEE Trans. Smart Grid* **2010**, *1*, 65–72.
10. Clement-Nyns, K.; Haesen, E.; Driesen, J. The Impact of Charging Plug-In Hybrid Electric Vehicles on a Residential Distribution Grid. *IEEE Trans. Power Syst.* **2010**, *25*, 371–380. doi:10.1109/TPWRS.2009.2036481. [\[CrossRef\]](#)
11. Amjad, M.; Ahmad, A.; Rehmani, M.H.; Umer, T. A review of EVs charging: From the perspective of energy optimization, optimization approaches, and charging techniques. *Transp. Res. Part D Transp. Environ.* **2018**, *62*, 386–417. [\[CrossRef\]](#)
12. Rahbari-Asr, N.; Chow, M.Y. Cooperative Distributed Demand Management for Community Charging of PHEV/PEVs Based on KKT Conditions and Consensus Networks. *IEEE Trans. Ind. Inform.* **2014**, *10*, 1907–1916. doi:10.1109/TII.2014.2304412. [\[CrossRef\]](#)
13. Zeraati, M.; Golshan, M.E.H.; Guerrero, J.M. A consensus-based cooperative control of PEV battery and PV active power curtailment for voltage regulation in distribution networks. *IEEE Trans. Smart Grid* **2017**, *10*, 670–680. [\[CrossRef\]](#)
14. Rahbari-Asr, N.; Chow, M.Y.; Chen, J.; Deng, R. Distributed real-time pricing control for large-scale unidirectional V2G with multiple energy suppliers. *IEEE Trans. Ind. Inform.* **2016**, *12*, 1953–1962. [\[CrossRef\]](#)
15. Zou, S.; Hiskens, I.; Ma, Z.; Liu, X. Consensus-Based Coordination of Electric Vehicle Charging. *IFAC-PapersOnLine* **2017**, *50*, 8881–8887. [\[CrossRef\]](#)
16. Zou, S.; Hiskens, I.; Ma, Z. Consensus-based coordination of electric vehicle charging considering transformer hierarchy. *Control Engineering Practice* **2018**, *80*, 138–145. [\[CrossRef\]](#)
17. Mousavian, S.; Erol-Kantarci, M.; Wu, L.; Ortmeier, T. A risk-based optimization model for electric vehicle infrastructure response to cyber attacks. *IEEE Trans. Smart Grid* **2017**, *9*, 6160–6169. [\[CrossRef\]](#)
18. Chhaya, L.; Sharma, P.; Bhagwatikar, G.; Kumar, A. Wireless sensor network based smart grid communications: Cyber attacks, intrusion detection system and topology control. *Electronics* **2017**, *6*, 5. [\[CrossRef\]](#)
19. Niyato, D.; Hoang, D.T.; Wang, P.; Han, Z. Cyber insurance for plug-in electric vehicle charging in vehicle-to-grid systems. *IEEE Netw.* **2017**, *31*, 38–46. [\[CrossRef\]](#)
20. Reeh, D.; Tapia, F.C.; Chung, Y.W.; Khaki, B.; Chu, C.; Gadh, R. Vulnerability Analysis and Risk Assessment of EV Charging System under Cyber-Physical Threats. In Proceedings of the 2019 IEEE Transportation Electrification Conference and Expo (ITEC), Jeju, Korea, 8–10 May 2019; pp. 1–6.
21. Zhang, Z.; Yuan, W.; You, F. Power allocation of jamming attackers against PEV charging stations: A game theoretical approach. In Proceedings of the 2015 7th International Conference of Soft Computing and Pattern Recognition (SoCPar), Fukuoka, Japan, 13–15 November 2015; pp. 111–116.
22. Dey, S.; Khanra, M. Cybersecurity of Plug-in Electric Vehicles: Cyber Attack Detection During Charging. *IEEE Trans. Ind. Electron.* **2020**. doi:10.1109/TIE.2020.2965497. [\[CrossRef\]](#)
23. Li, Y.; Wang, R.; Wang, P.; Niyato, D.; Saad, W.; Han, Z. Resilient PHEV charging policies under price information attacks. In Proceedings of the 2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm), Tainan, Taiwan, 5–8 November 2012; pp. 389–394.

24. Ma, Z.; Zou, S.; Ran, L.; Shi, X.; Hiskens, I.A. Efficient decentralized coordination of large-scale plug-in electric vehicle charging. *Automatica* **2016**, *69*, 35–47. [[CrossRef](#)]
25. Bompard, E.; Ma, Y.; Napoli, R.; Abrate, G. The demand elasticity impacts on the strategic bidding behavior of the electricity producers. *IEEE Trans. Power Syst.* **2007**, *22*, 188–197. doi:10.1109/tpwrs.2006.889134. [[CrossRef](#)]
26. Gountis, V.P.; Bakirtzis, A.G. Bidding strategies for electricity producers in a competitive electricity marketplace. *IEEE Trans. Power Syst.* **2004**, *19*, 356–365. [[CrossRef](#)]
27. Liu, H.; Xie, G.; Wang, L. Necessary and sufficient conditions for containment control of networked multi-agent systems. *Automatica* **2012**, *48*, 1415–1422. [[CrossRef](#)]
28. Franceschelli, M.; Egerstedt, M.; Giua, A. Motion probes for fault detection and recovery in networked control systems. In Proceedings of the 2008 American Control Conference, Seattle, WA, USA, 11–13 June 2008; pp. 4358–4363.
29. Moreau, L. Stability of multiagent systems with time-dependent communication links. *IEEE Trans. Autom. Control* **2005**, *50*, 169–182. [[CrossRef](#)]
30. Olfati-Saber, R.; Murray, R.M. Consensus problems in networks of agents with switching topology and time-delays. *IEEE Trans. Autom. Control* **2004**, *49*, 1520–1533. [[CrossRef](#)]
31. Kia, S.S.; Van Scoy, B.; Cortes, J.; Freeman, R.A.; Lynch, K.M.; Martinez, S. Tutorial on dynamic average consensus: The problem, its applications, and the algorithms. *IEEE Control Syst. Mag.* **2019**, *39*, 40–72. [[CrossRef](#)]

© 2020 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).