frontiers | Frontiers in Energy Research

ORIGINAL RESEARCH
published: 29 April 2022
doi: 10.3389/fenrg.2022.845341

Distributed Resilient Mitigation Strategy for False Data Injection Attack in Cyber-Physical Microgrids

Ge Cao[1,2]*, *Rong Jia*[1,2] *and Jian Dang*[1,2]

[1]School of Electrical Engineering, Xi'an University of Technology, Xi'an, China, [2]Institute for Electrical Power and Integrated Energy of Shaanxi Province, Xi'an, China

The stable and reliable operation of microgrids requires the immediate communication and accurate measuring data of cyber systems. The cyber security of smart grids consists of detection and mitigation, where the latter mainly refers to resisting the attack and recovering the physical operation state through various means after cyber attacks. With the flexible electrical topology and the distributed control strategy based on the public communication network and end-to-end neighbor communication, the application and effect of cyber security technologies (firewall and encryption) in traditional cyber systems are limited. However, due to the fact that the cyber system and power system are coupled in microgrid cooperative control, countermeasures are added to the control to enhance the cyber security of microgrids, which has drawn more attention. Therefore, considering the control failure and even system results from the false data inject attack (FDIA) on the cooperative control of microgrids, this study investigates the synchronous mitigation framework based on local detection where the reactive power cooperative control targets of microgrids with and without FDIA are compatible by the resilient control method. The credibility is utilized to measure the reliability of local and neighbor data in the proposed method. The consensus communication coupling gain is weighted corrected by an adaptive update strategy of credibility to delete the attack signal. Moreover, the proposed method directly improves the conventional distributed secondary controller that reduces the complexity of controller design. Simulations investigate the effectiveness of the proposed distributed resilient mitigation strategy under conditions of deception and disruption attacks.

Keywords: cyber-physical system, microgrid, distributed resilient control, false data injection attack, local attack detection

OPEN ACCESS

Edited by:
Peng Li,
Tianjin University, China

Reviewed by:
Hongbin Wu,
Hefei University of Technology, China
Bin Zhou,
Hunan University, China

***Correspondence:**
Ge Cao
gcao@xaut.edu.cn

Specialty section:
This article was submitted to Smart Grids, a section of the journal Frontiers in Energy Research

Received: *29 December 2021*
Accepted: *28 March 2022*
Published: *29 April 2022*

Citation:
Cao G, Jia R and Dang J (2022) Distributed Resilient Mitigation Strategy for False Data Injection Attack in Cyber-Physical Microgrids. Front. Energy Res. 10:845341. doi: 10.3389/fenrg.2022.845341

1 INTRODUCTION

The distributed generator (DG) integrates renewable energy into power systems by microgrids that are one vital infrastructure of smart grids (Olivares et al., 2014). With the communication, control, and computation technologies utilized in power systems to facilitate the optimal operation and reliable supplement, power grids have been developing into typical cyber-physical systems (CPSs) (Yu and Xue, 2016). The microgrid CPS exchanges measurement quantities and control signals among sensors and actuators through wired or wireless links and conducts decision making through channels like centralized or distributed computation. Despite the merits of CPS, microgrids are confronting additional risks due to the deep cyber-physical coupling. Cyber events that include

network fluctuations and cyber attacks have a marked impact on the physical states of power systems (Cao et al., 2020).

As the controllable resources (DGs, energy storage, flexible loads, etc.) are distributed scatteringly in distribution networks or microgrids, their intelligent electronic devices will result in massive amounts of communication data. Thus, the public communication mechanisms are applied more widely to reduce the cost and reinforce the flexibility of networks, which is convenient for third-party applications to have easy access to the cyber side of power systems. On one hand, it provides ancillary services for customers and suppliers; on the other hand, the level of cyber risk in cyber-physical power systems is upgraded (Li et al., 2017; Alavi et al., 2018). Such a feature brings more potential cyber attack access points for cyber systems of microgrids (Li et al., 2016). In recent years, large-scale electric power outages resulting from cyber attacks occur frequently (E-ISAC, 2016). The famous blackout in Ukraine on December 23, 2015 (Lai et al., 2019), for example, caused 30 substations to disconnect from the power grid and millions of residents to suffer a massive 6-h power outage, which resulted from the Trojan horse virus called BlackEnergy implanted into the network of a Ukrainian electric power company by a malicious attacker.

Moreover, the denial-of-service (DoS) attack reduces the availability of communication networks by blocking channels, thereby interfering with data flow (Liu et al., 2021). The man-in-the-middle (MITM) attack invades the communication link between two communication nodes through the third-party application, tampers with information data, or destroys data channels (Sahoo et al., 2021). The false data injection attack (FDIA) affects the physical operational status of CPS by invading sensors, controllers, or other communication nodes and writing false data into network loops (He et al., 2017).

As the typical attack form that directly disturbs the calculation of control commands, FDIA has become the most studied cyber attack in power CPS (Wang et al., 2017). In successful FDIAs, the manager of power systems takes the status information injected with attack signals as sensor measurement results, which may result in the malfunction of some equipment and seriously threaten the physical operation security. In Liu et al., 2015b, the actual FDIA problem, and the mechanism model are studied, where the attacker only acquires less system information to carry out. The influence of FDIA on power system state estimation is analyzed (Liang et al., 2016), and FDIA is introduced into a two-layer optimization problem to maximize power line flows. *Liang et al* . investigate several FDIA models consisting of the deterministic constraint model, incomplete information model, forged topology model, and AC power flow model (Liang et al., 2017). The influences of FDIA on the electricity market, load redistribution, and distributed energy routers are also explored. Furthermore, optimization models with various constraints are utilized to describe FDIA in different situations (Deng et al., 2017). For the dynamic use of autonomous microgrids, Zhang et al. studied the impact of FDIA on distributed load sharing and derived the stability region and sufficient conditions for the stable operation of microgrids (Zhang et al., 2019).

The distributed control based on multi-agent systems (MASs) has become the main content in the research field of microgrid control (Liu et al., 2014). For the problems where cyber attacks impact physical system operations due to the cyber-physical interdependence, some resilient control methods were presented, which aim to solve the stability issue under communication failures and cyber attacks. To resist actuator fault and DoS attack, a resilient adaptive distributed observer and fault-tolerant controller were proposed (Deng and Wen, 2020), which effectively improves the anti-cyber-attack ability of MAS. Further considering the MAS with nonuniform communication delays, a proposed distributed resilient control method was presented by introducing a buffer mechanism and a time-varying sampling period sequence (Deng and Wen, 2021). It was proved to have the ability to eliminate errors caused by time delays and prevent the DoS attack. In Deng et al., 2021, a distributed adaptive resilient control method is provided for multiple energy storage systems in microgrids to balance the state of charge and restore the frequency and voltage under cyber fault and attack. For hybrid AC/DC microgrids, the authors (Wang Y. et al., 2021) proposed a cyber-resilient cooperative control strategy for bidirectional converters to defend an FDIA, which is validated on the RT-LAB simulation system. These researches primarily focus on the impact of cyber attacks and mitigation by designing novel controllers, which requires a significant cost to transform the controllers.

However, these methods invest cost to again switch the additional controller instead of optimizing the control parameter to improve the resilience of microgrids. We study the distributed mitigation strategy against FDIA in microgrids. Considering the reactive power and voltage control in microgrids, a distributed resilient control methodology for autonomous microgrids is presented in this study to eliminate the impact of FDIA on microgrid control. The proposed method can not only restore the deviation of reactive power and voltage in microgrids but also adapt to the different types of FDIA. Additionally, the distributed resilient consensus cooperative control method avoids the extra communication traffic and cumbersome switching of controllers.

The rest of this article is organized as follows: **Section 2** gives the introduction to the hierarchical control architecture and distributed secondary voltage control of microgrids. The synchronous mitigation framework against FDIA in microgrid CPS is introduced in **Section 3**. In **Section 4**, the distributed resilient consensus cooperative control method is presented. **Section 5** studies simulated cases to investigate the effectiveness of the proposed strategy. Finally, **Section 6** concludes this article.

2 HIERARCHICAL CONTROL STRUCTURE OF MICROGRIDS

There are a variety of operating requirements in microgrids, such as frequency and voltage regulation, load power distribution and coordination, optimization cost, and so forth, corresponding to different control strategies and time scales. Therefore, the two-layer control structure is utilized in microgrids to realize the different control objectives, as depicted in **Figure 1**. Due to the

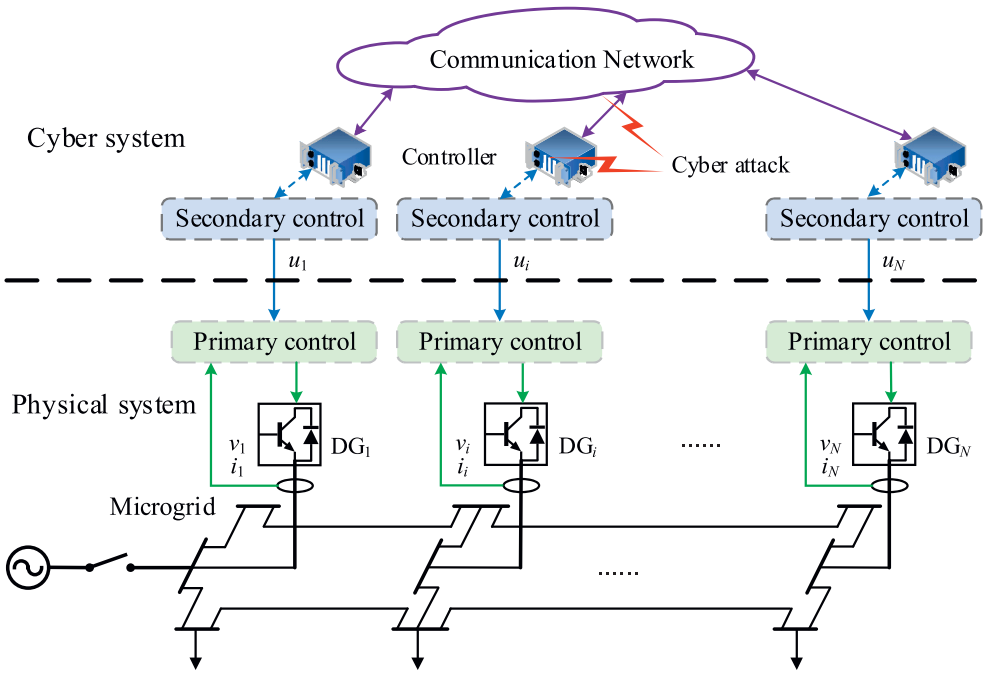

FIGURE 1 | General cyber-physical structure of microgrids.

fact that the primary control directly guarantees the stability of inverters, it is included in the physical system of microgrid CPS, while the secondary control that requires the communication network and operational data of other DGs is one part of the cyber system, which is the target of FDIA (Wang T. et al., 2021).

2.1 Primary Control

The primary control maintains the frequency and voltage stability, power balance, and plug and play function for DG, which is deployed in the local side (Liu et al., 2015a; Lou et al., 2017). The droop control changes the output power of inverters automatically according to the deviation of frequency and voltage. Specifically, the droop relationship between voltage and reactive power is described as

$$v_i = v_0 - n_i Q_i, \tag{1}$$

where *vi* is the voltage magnitude of DG*i*, *v*0 is the designed nominal voltage magnitude, *Qi* is the output reactive power of DG*i*, and *ni* is the voltage-reactive power droop coefficient of DG*i*. Note that the primary control is the deviating regulation.

2.2 Secondary Control

Due to the compromise of primary control in deviating adjustment, the secondary control aims to eliminate the steady-state deviation of frequency and voltage and achieve the rebalanced power sharing optimally among DGs, which relies on communication networks. The distributed secondary voltage controller (Cao et al., 2022) is the basis of the proposed mitigation strategy, described as

$$\begin{aligned} v_i &= v_0 - v_i - n_i Q_i + u_i \\ u_i &= c_i^v + c_i^Q \\ c_i^v &= \left(k_{Pv} + \frac{k_{Iv}}{s}\right)(v_{ref} - \bar{v}_i) \\ c_i^Q &= \left(k_{PQ} + \frac{k_{IQ}}{s}\right)(Q_{ref} - u_i^Q) \end{aligned} \tag{2}$$

where *ui* is the secondary control input of DG*i*; *cv i* and *cQ i* are the voltage and reactive power control inputs, respectively; *v*ref and Q_{ref} are the voltage and reactive power reference values of the microgrid, respectively; k_{Pv}, k_{Iv}, k_{PQ}, and k_{IQ} are the proportional and integral parameters of proportional-integral (PI) controllers, respectively; $\bar{v}_i$ is the average voltage estimate of DG*i*; and *uQ i* is the reactive power offset of DG*i*. Based on the MAS and consensus algorithm, the calculation of $\bar{v}_i$ and *uQ i* adopts a distributed manner which is described as follows:

$$\begin{aligned} \bar{v}_i &= v_i + \int u_i^v \mathrm{d}t \\ u_i^v &= \sum_{j \in N_i} a_{ij}\left(\bar{v}_j - \bar{v}_i\right) \\ u_i^Q &= \sum_{j \in N_i} a_{ij}\left(C_j Q_j - C_i Q_i\right) \end{aligned} \tag{3}$$

where N_i is the set of neighbors of DG_i and a_{ij} represents the communication coupling gain, with $a_{ij}>0$ if there is a communication path between DG_i and DG_j and $a_{ij} = 0$ implying otherwise. C_i donates the capacity coefficient of DG*i*. The purpose of the secondary voltage control is to adjust the

average voltage of microgrids to the reference values, while cooperatively averaging the load power sharing among DGs according to their capacities. When satisfying the convergence condition, $\bar{v}_i$ and $uQ\ i$ will adjust to the reference values after the dynamic process, that is, the average voltage estimators of all DGs are the same and the reactive power of loads are shared proportionately:

$$\begin{aligned} \lim_{t\to\infty} \bar{v}_i &= v_{\text{ref}} \\ \lim_{t\to\infty} u_i^Q &= 0 \end{aligned} \tag{4}$$

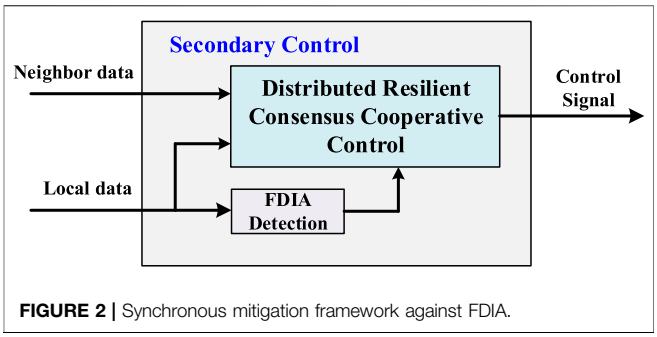

FIGURE 2 | Synchronous mitigation framework against FDIA.

3 SYNCHRONOUS MITIGATION FRAMEWORK AGAINST FALSE DATA INJECT ATTACK

3.1 False Data Inject Attack Model and Local Detection

Generally, the cyber attacker has two main paths to paralyze the physical system: 1) immediately invade the cyber system to result in instability and 2) secretly invade to seize the control of the operator (Dibaji et al., 2019). In this article, we study the single FDIA that only one agent is attacked at one time. For convenience, we assume that the reactive power data are injected with the attack signal. Thus, there are two forms of FDIA:

$$\hat{Q}_i = Q_i + \mu Q_i^{\text{a}} \tag{5}$$

$$\hat{Q}_{ij} = Q_{ij} + \mu Q_i^{\text{a}} \tag{6}$$

where $\hat{Q}_i$ and $\hat{Q}_{ij}$ are the native estimation data and the estimation data that are sent to the neighbor agent, respectively. $Qa\ i$ is the attack signal that is assumed to be constant. μ is the flag value that indicates the attack behavior: $\mu = 1$ if the FDIA occurs; otherwise, $\mu = 0$. Based on the different forms of FDIA, two types of FDIA are considered in this study: 1) deception attack that does not affect the original secondary PI controller inputs, and 2) disruption attack where the average voltage and reactive power offset converge to illegal values different from the preset reference values:

$$\begin{aligned} \lim_{t\to\infty} \bar{v}_i &= v_{\text{ref}}^{\text{a}} \\ \lim_{t\to\infty} u_i^Q &\neq 0 \end{aligned} \tag{7}$$

The local detection can determine whether the local agent is suffering from FDIA and the credibility of local data information. According to the detailed model and analysis of FDIA (Cao et al., 2022), the combination of local information can be selected for local detection:

$$l_i(t) = \left| \frac{C_i \hat{Q}_i}{\bar{v}_i} - i_{\text{qi}}^{\text{ref}} \right| \tag{8}$$

where l_i is the local detection signal of DG_i. $i\text{ref}\ \text{q}i$ is the reference value of q-axis current. Obviously, $l_i = 0$ if DG_i is not attacked, and the local data are credible; otherwise, $l_i \neq 0$ and the local data are not credible.

Based on the two FDIA forms **(Eq. 5)** and **(Eq. 6)** and the analysis in Sahoo et al., 2020, the two situations of FDIA are considered in this article:

1) Both the FDIA forms **(Eq. 5)** and **(Eq. 6)** occur, that is, deception attack. The local detection value $l_i > 0$.
2) Only FDIA form **(Eq. 5)** occurs, that is, disruption attack. The local detection value $l_i = 0$.

3.2 Synchronous Mitigation Framework Based on Local Detection

Considering the distributed control structure of cyber-physical microgrids, a synchronous mitigation framework based on local detection is proposed in this study, as depicted in **Figure 2**. The mitigation framework can implement active synchronous defense against FDIA by the FDIA identification for native DG based on the local data and the adaptive updating for communication coupling gain based on the credibility of neighbors. The proposed synchronous mitigation framework avoids the disadvantage of adding new communication traffic by using local detection and neighbor data. The distributed resilient consensus cooperative control method simplifies the design of secondary controllers, which is applicable to switching network topologies and communication latency. The detailed control method is presented in the next section.

4 DISTRIBUTED RESILIENT CONSENSUS COOPERATIVE CONTROL

The distributed resilient consensus cooperative control method is proposed in this study to degrade the impact of FDIA on the microgrid control. The proposed method can improve the operational resilience of microgrid CPSs by evaluating the information credibility according to the local detection result and the communication data of neighbor DGs and by isolating the data of the attacked agent by adaptive adjustment of communication coupling gain in the consensus algorithm, which prevents the attack signal from spreading in the cyber system. Specifically, there are two stages:

1) Determine whether the native agent is suffering from FDIA according to the local detection result. If the FDIA occurs, the

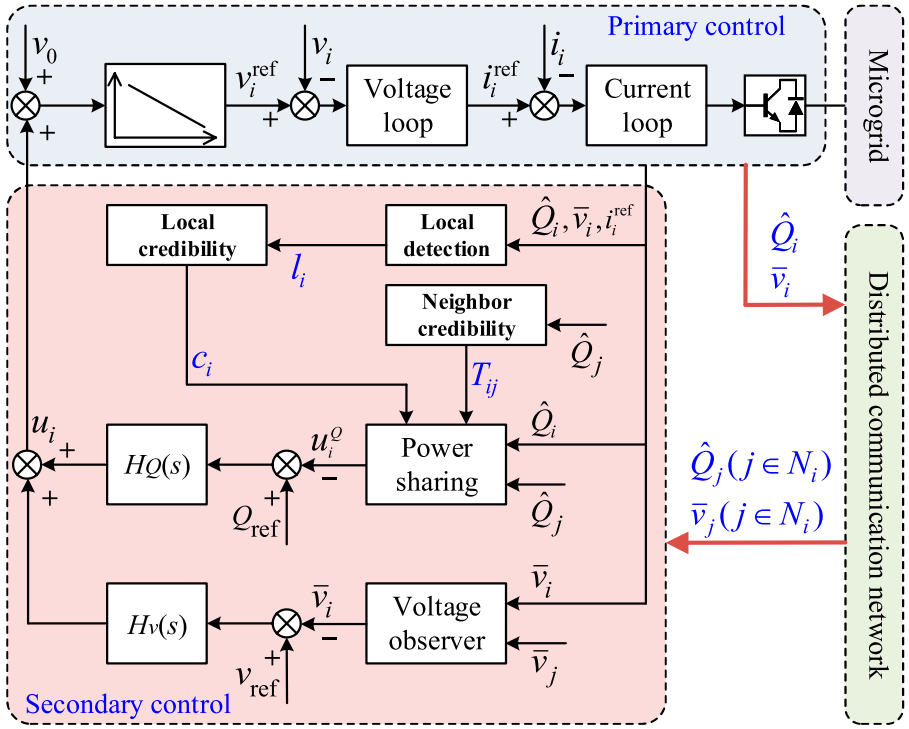

FIGURE 3 | Distributed resilient consensus cooperative control diagram.

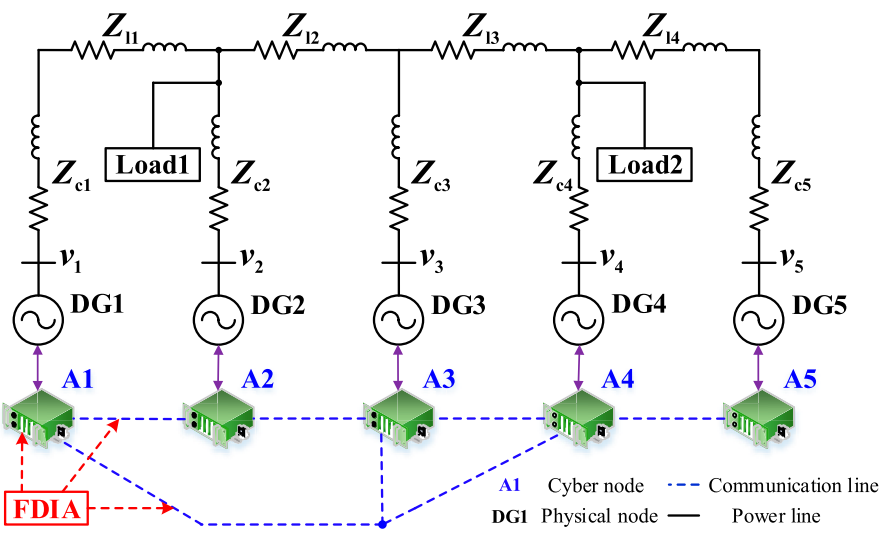

FIGURE 4 | Schematic diagram of the test microgrid CPS.

native agent exits the consensus synchronization process to prevent the attack signal from influencing the local states in the physical system.

2) Calculate the credibility of the neighbor agent by its communication data. If the neighbor agent data are injected into the attack signal, the credibility would be

TABLE 1 | Procedure of the proposed method.

Procedure: The secondary control of DG$_i$
1: initial local and neighbor credibility values $c_i = T_{ij} = 1$
2: while ($t > 0$)
3: input native data $\hat{Q}_i$, $\bar{v}_i$, $i$ref q, i, and neighbor data $C_j\hat{Q}_j$
4: calculate the local detection result l_i of FDIA by **(8)**
5: update the neighbor credibility c_i by **(Eq. 11)** and **(Eq. 12)**
6: if $c_i < c\text{th}_j$
7: $c_i = 0$
8: end if
9: update the neighbor credibility T_{ij} by **(Eq. 13)** and **(Eq. 14)**
10: if $T_{ij} < T\text{th}_{ij}$
11: $T_{ij} = 0$
12: end if
13: update secondary control input u_i
14: end while

lower than the threshold value. Thus, the native agent discards the neighbor data to isolate the attack signal.

4.1 Distributed Resilient Consensus Algorithm Based on Credibility

In order to overcome the disadvantage of the traditional average consensus algorithm susceptible to cyber attacks, an improved resilient consensus based on credibility is proposed in this section to realize the distributed information exchange of MAS under cyber attacks. Each agent sets credibility to measure the confidence level of its native data and received neighbor data, whose value depends on whether it is the attack target and how close it is to the attack source. If the attacked agent detects the FDIA, it exits the consensus synchronization process; meanwhile, other agents calculate each neighbor credibility value. If one credibility of the neighbor agent is lower than the threshold value, it is judged as the attack resource and its data are discarded in the consensus calculation process. The attacked agent is isolated by adjusting communication coupling gains according to credibility, which makes MAS resilient. The improved resilient consensus algorithm based on credibility is described as follows:

$$\dot{x}_i(t) = c_i(t)\sum_{j\in N_i} a_{ij}T_{ij}(t)\left[\hat{x}_j(t) - \hat{x}_i(t)\right] \tag{9}$$

where x_i represents the real state information of the ith agent. $\hat{x}_i$ represents the state estimation value of the ith agent. a_{ij} represents the communication coupling gain in MAS. N_i represents the neighbor agent set of the ith agent. c_i represents the local credibility of the ith agent. T_{ij} represents the neighbor credibility of the ith agent. If there is no FDIA in MAS, $c_i = 1$, $T_{ij} = 1$, and the consensus calculation is normal. When the ith agent is suffering from FDIA (deception attack), $c_i < 1$, and the larger the attack signal is, the closer c_i is to 0, which means that the communication coupling gains between the native agent and all its neighbor agents are reduced and this attacked agent exits the consensus synchronization process gradually. When the state estimation value of the neighbor jth agent is injected with an attack signal (deception attack), the ith agent set the corresponding neighbor credibility value $T_{ij} < 1$, and the larger the attack signal is, the closer T_{ij} is to 0, that is, the communication coupling gain between the native agent and the neighbor jth agent is reduced and the impact of attacked state estimation data of the neighbor agent on the native state update has degenerated.

TABLE 2 | Electrical parameters of the microgrid.

Type	Parameter	Value	Parameter	Value
—	Voltage	380 V	Frequency	50 Hz
DG	Droop coefficient		Connection impedances	
	n_1, n_2	1×10^{-5}	Z_{c1}	0.2 + j0.3 Ω
	n_3	0.5×10^{-5}	Z_{c2}	0.1 + j0.22 Ω
	n_4, n_5	1.5×10^{-5}	Z_{c3}	0.08 + j0.15 Ω
	m_1–m_5	7.5×10^{-4}	Z_{c4}	0.15+j0.28 Ω
	—	—	Z_{c5}	0.05+j0.13 Ω
Load	Load1	18 kW + 12 kvar	Load2	12 kW+8 kvar
Line	Z_{l1}	0.05 + j0.1 Ω	Z_{l2}	0.13 + j0.2 Ω
	Z_{l3}	0.03 + j0.1 Ω	Z_{l4}	0.08 + j0.13 Ω

4.2 Adaptive Update Strategy of Credibility

The key aspect of the distributed resilient consensus algorithm based on credibility is that credibility values can adaptively update according to whether the MAS is subjected to FDIA (Abhinav et al., 2019). The reactive power control in **(Eq. 3)** is improved to the distributed resilient consensus cooperative control:

$$u_i^Q = c_i(t)\sum_{j\in N_i} a_{ij}T_{ij}(t)\left(C_j\hat{Q}_j - C_i\hat{Q}_i\right) \tag{10}$$

Considering the FDIA forms against reactive power data, as in **(Eq. 5)** and **(Eq. 6)**, the adaptive update strategies of credibility based on local detection and neighbor average are proposed in this section to adjust the communication coupling gains dynamically, which isolates the attack signal of FDIA and improves the operational resilience of microgrid CPSs against cyber attacks.

4.2.1 Adaptive Update of Credibility Based on Local Detection

The update process of the local credibility value is directed as

$$\dot{c}_i(t) = \alpha[k_i(t) - c_i(t)] \tag{11}$$

where $0 \le c_i(t) \le 1$. $\alpha > 0$ is utilized to adjust the update speed of local credibility value c_i. $k_i(t)$ determines the value of c_i, which can be calculated as follows:

$$k_i(t) = \frac{\delta_i}{\delta_i + l_i(t)} \tag{12}$$

where δ_i represents the detection threshold value, which is utilized to distinguish the attack signal from other disturbances. $l_i(t)$ represents the native detection signal obtained from **(Eq. 8)**. The local detection result indicates that if no FDIA has occurred, then $l_i(t) = 0$ and $k_i(t) = 1$ in the steady state. Thus, $c_i = 1$ means that the distributed control is carried out normally in microgrids. Else, if the local detects the attack signal, $l_i(t) > \delta_i$ and $k_i(t) < 1$. Thus, $c_i < 1$ depends on the size of the attack signal, which indicates that the reactive power control offset is

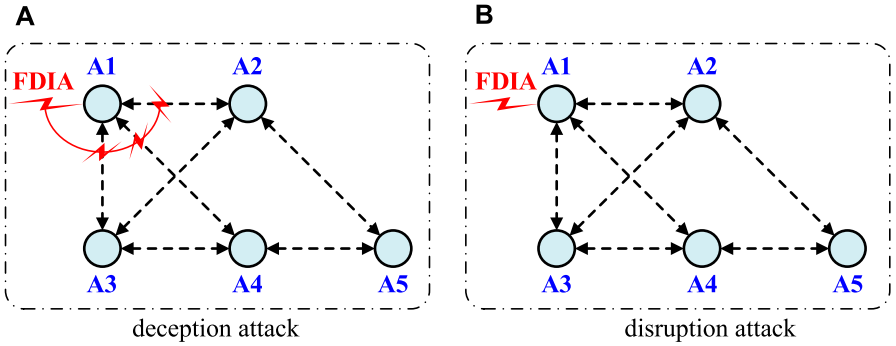

FIGURE 5 | FDIA situation: **(A)** deception attack and **(B)** disruption attack.

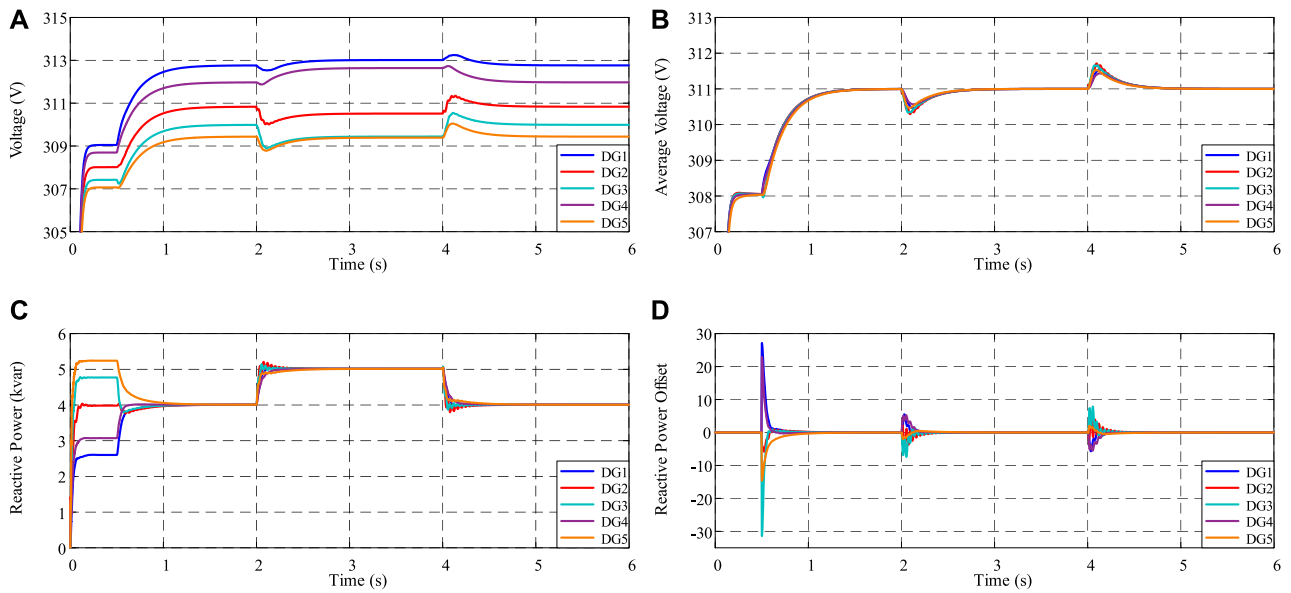

FIGURE 6 | Simulation results of the test microgrid without FDIA.

reduced gradually. When $c_i < c\text{th},_i$, the native DG_i exits the secondary control to prevent the system from instability.

4.2.2 Adaptive Updating of Credibility Based on Neighbor Average

The update process of neighbor credibility value is directed as

$$\dot{T}_{ij}(t) = \beta_j\left[s_{ij}(t) - T_{ij}(t)\right], \tag{13}$$

where $0 \le T_{ij}(t) \le 1$. $\beta_j > 0$ is utilized to adjust the update speed of the neighbor's credibility value T_{ij}. $s_{ij}(t)$ determines the value of T_{ij}, which can be calculated as follows:

$$s_{ij}(t) = \frac{\sigma_i}{\sigma_i + \left|C_j\hat{Q}_j(t) - \frac{1}{|N_i|}\sum_{k\in N_i} C_k\hat{Q}_k(t)\right|}, \tag{14}$$

where σ_i represents the update threshold value, which is utilized to distinguish the attack signal from other cyber disturbances. $|N_i|$ represents the neighbor number of DG_i. $h_i = \frac{1}{|N_i|}\sum_{k\in N_i} C_k\hat{Q}_k$ represents the mean value of neighbor reactive power estimations in the consensus iterative of DG_i. If the information of the neighbor DG_j is reliable, $C_j\hat{Q}_j = h_i$ and $s_{ij}(t) = 1$ in the steady state. Thus, $T_{ij} = 1$ means that the distributed control is carried out normally in microgrids. If the data of neighbor DG_j are injected into the attack signal of FDIA, $C_j\hat{Q}_j \neq h_i$ and $s_{ij}(t) < 1$. Thus, $T_{ij}<1$ depends on the size of $|C_j\hat{Q}_j - h_i|$, which implies that the larger value means that T_{ij} is more close to 0, which indicates that the reactive power estimation of DG_j is less reliable. It is necessary to reduce the impact of the neighbor estimation on the native reactive power control offset. If $T_{ij} > T\text{th},_{ij}$, the data of neighbor DG_j exit the consensus cooperative process of native DG_i to prevent the system from instability.

4.3 Control Procedure

The distributed resilient consensus cooperative control method is suitable for both normal and FDIA situations. In the normal

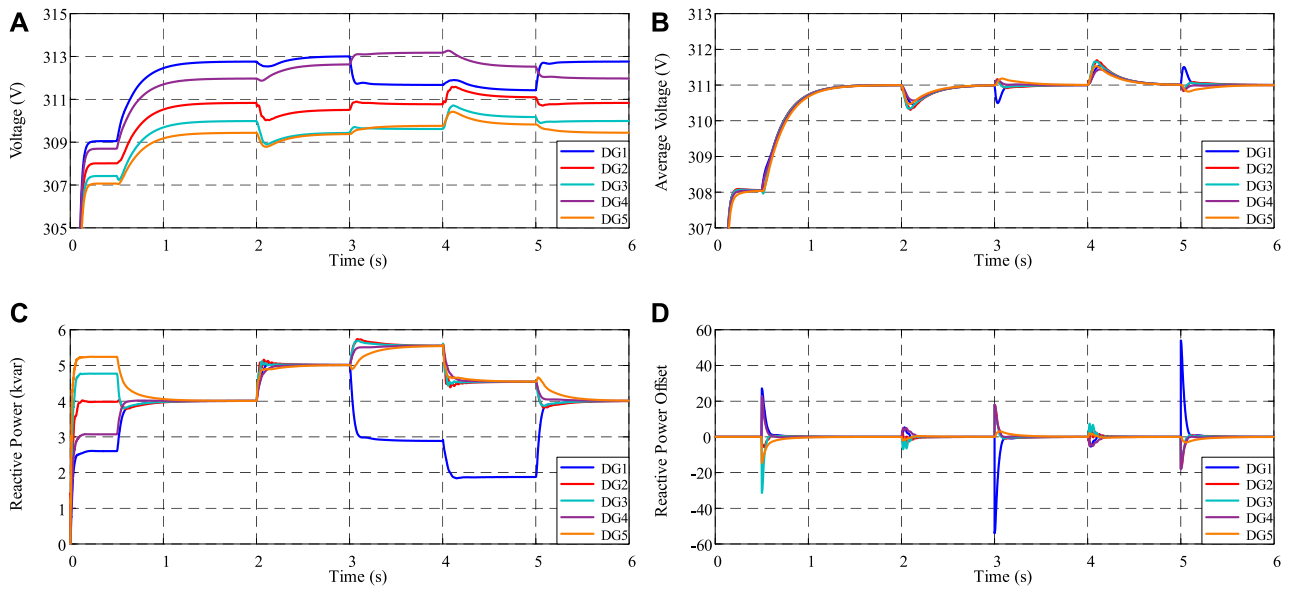

FIGURE 7 | Simulation results of the test microgrid with deception attack.

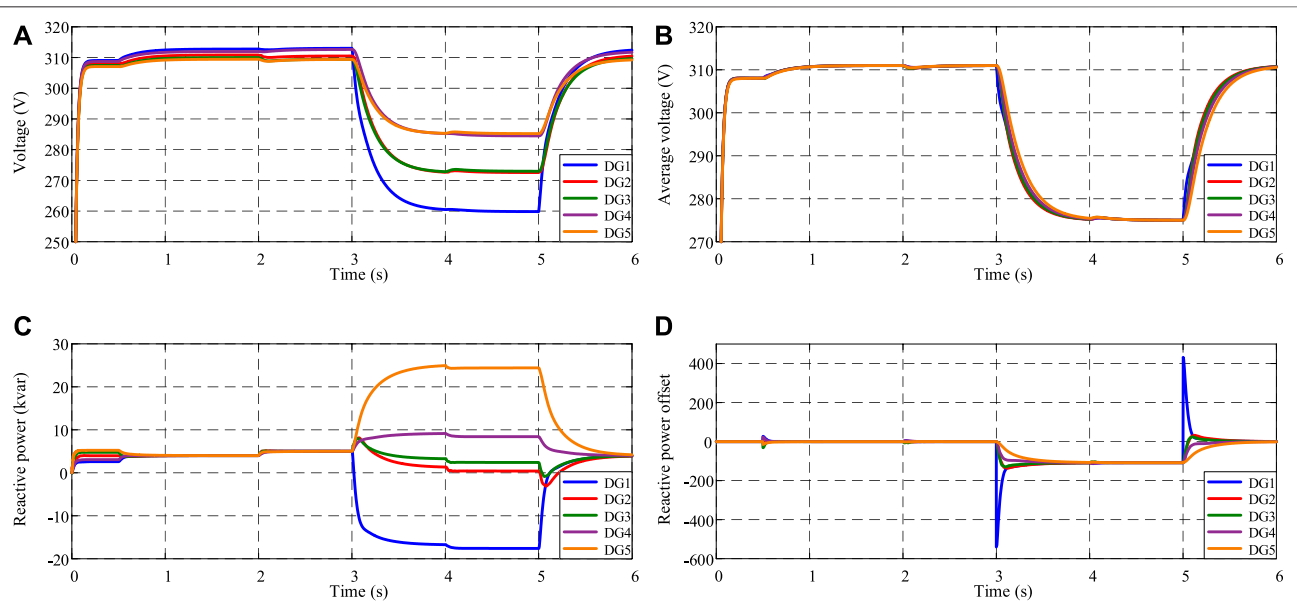

FIGURE 8 | Simulation results of the test microgrid with disruption attack.

operation, both the local and neighbor credibility values are 1, which do not affect the preset communication coupling gain parameters. Therefore, the reactive power of the microgrid can converge to the reference value according to **(Eq. 10)**. When FDIA occurs, the distributed resilient consensus cooperative control adjusts communication coupling gain parameters by updating credibility values, which guarantees the safe and stable operation of microgrids. For instance, if the attack signal is injected into the whole system by attacking one agent, the attacked agent exits the consensus calculation process; in the meanwhile, its neighbor agents discard the attacked agent data that include the attack signal. Thus, the operation state of the system is not impacted by FDIA. Note that this way does not directly block the propagation of the attack signal in the cyber system but "house arrest" the attack signal in the distributed secondary control module, which isolates the attacked agent in disguise and disconnects its external communication link so that the attack signal cannot harm the power system with the help of control commands.

By the synchronous mitigation based on local detection, the distributed resilient consensus cooperative control method avoids

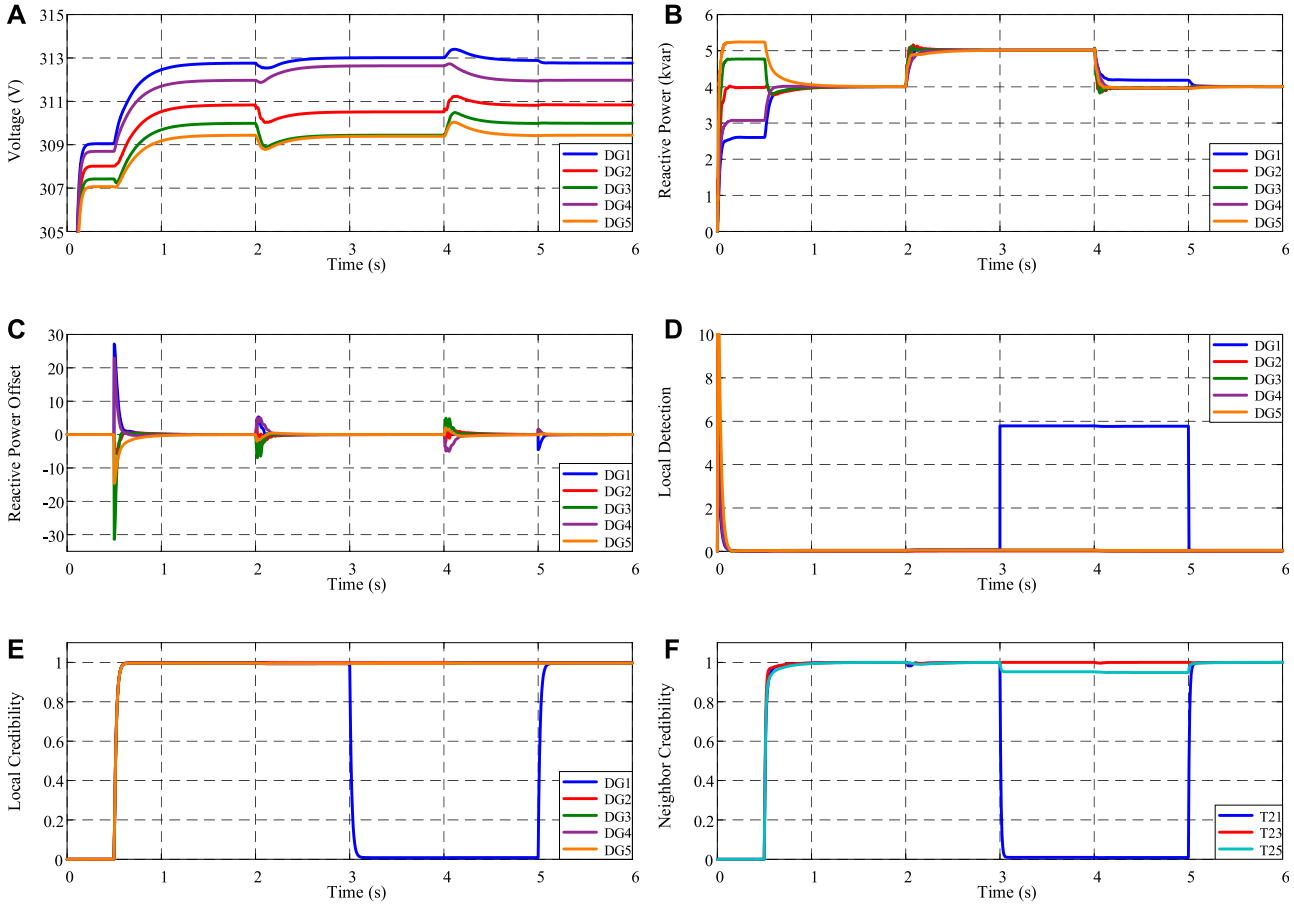

FIGURE 9 | Simulation results of deception attack mitigation.

the extra communication traffic and cumbersome switching of controllers, which only increases the local detection and credibility computing module on the basis of the original distributed secondary control. The controller design is not complex to be implemented on embedded systems. The control diagram of the proposed distributed resilient consensus cooperative method is depicted in **Figure 3**.

To guarantee the resilient operation of microgrids under FDIA, the distributed resilient consensus cooperative control method consists of three parts: 1) recognize the native attack signal by local credibility, 2) identify the neighbor attack signal by neighbor credibility, and 3) adjust the communication coupling gain in real time by adaptive update. The control flow is depicted in **Table 1**.

5 CASE STUDY

In this section, simulations are performed to investigate the effectiveness of the proposed method by a test microgrid CPS as depicted in **Figure 4**, where five DGs based on droop control are connected and communicate through power and communication lines. The control and electrical parameters are listed in **Table 2**. Note that all DGs have the same capacity. MATLAB/Simulink is utilized to simulate the test microgrid CPS.

5.1 Case 1: False Data Inject Attack Impact

The simulation, in this case, concentrates on the normal scenario and FDIA scenario as references. The simulation process is described as follows: 1) at t = 0s, the microgrid operates in the primary droop control; 2) at t = 0.5 s, the distributed secondary control is activated; 3) at t = 2 s, an additional load 10 kW + 5 kvar is attached to Load1 and detached at t = 4 s; 4) at t = 3 s, the different attack situation of FDIA is carried out in microgrid and removed at t = 5 s, as presented in **Figure 5**. The simulation result in the normal situation is depicted in **Figure 6**.

Then, the attacker implements the deception attack on the reactive power data of cyber node A1 in **Figure 5A** to sneak on the cyber system of the microgrid. The injected attack signal is 2. The simulation result with the deception attack is depicted in **Figure 7**. Due to the attack signal injected into A1, the voltage and reactive power of DG1 adjust in the light of the error control commands. Nevertheless, the average voltage and reactive power offset can converge to the preset consensus value 311V and 0. Thus, the microgrid operator cannot judge whether FDIA has occurred.

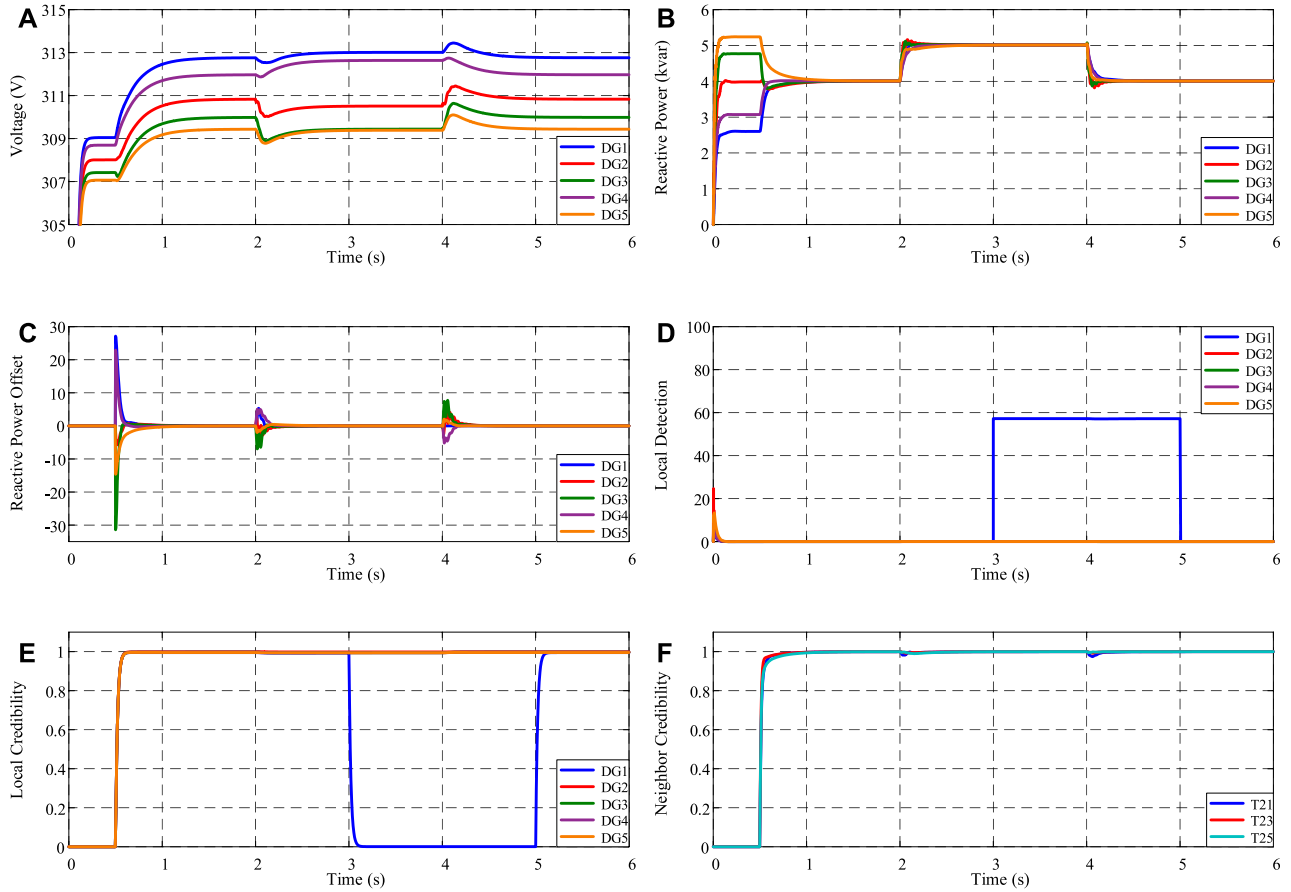

FIGURE 10 | Simulation results of disruption attack mitigation.

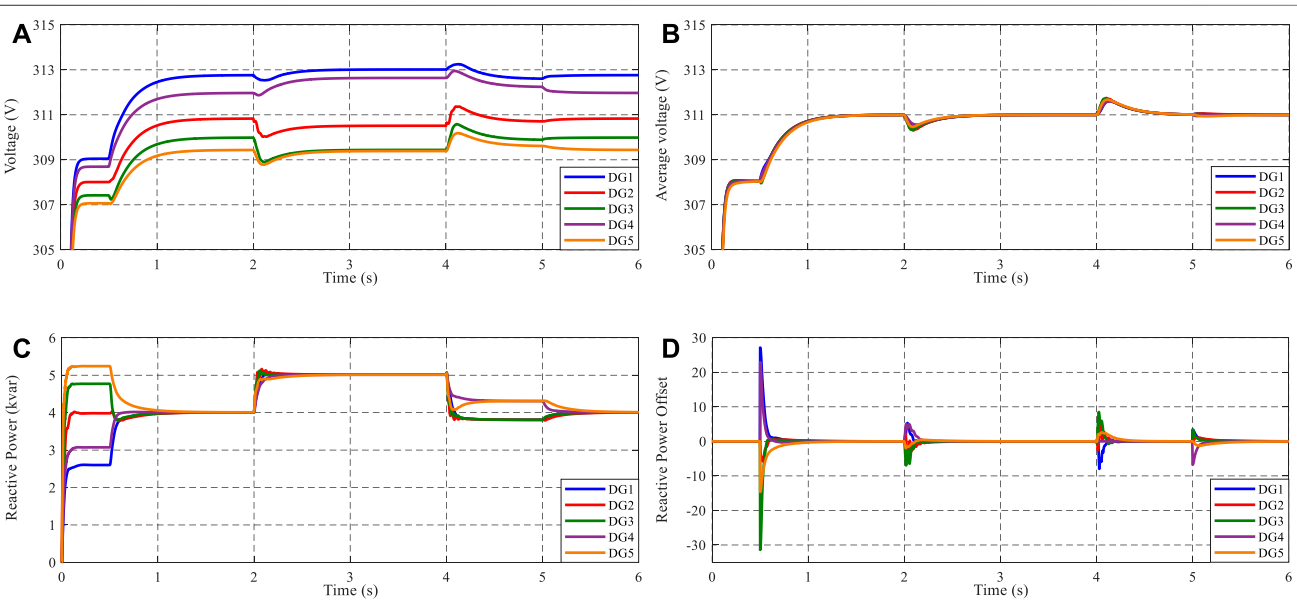

FIGURE 11 | Simulation results of the median-based consensus algorithm.

In the disruption attack, the attack signal 20 is injected into the reactive power data of cyber node A1 in **Figure 5B**. The transmitted reactive power data of A1 are sent to its neighbor nodes A2, A3, and A4, which are none of the attack signals. The simulation result with the disruption attack is depicted in **Figure 8**. The average voltage and reactive power offset of the microgrid converge to default values. Due to the impact of the disruption attack, the output reactive power of DG1 reduces rapidly and even absorbs reactive power, which leads to the reactive power changes of other DGs. Meanwhile, the average voltage of the microgrid adjusts to an error value (275 V in **Figure 8**) and the voltages of DGs continue to decrease, resulting in voltage sag in the microgrid, which means the voltage instability of the microgrid. It demonstrates that the purpose of destroying the microgrid operation has been achieved. The microgrid operator can detect FDIA by the two control errors of average voltage and reactive power control offset.

5.2 Case 2: Deception Attack Mitigation

This case tests the effectiveness of the distributed resilient mitigation strategy against deception attacks. The attack signal is injected into the secondary control of A1 and sent to the neighbor nodes A2, A3, and A4. The simulation result is depicted in **Figure 9**. According to **Figure 7**, although the average voltage and reactive power offset can be adjusted to the preset value under the deception attack, the actual voltage and reactive power output of DGs have abnormal changes. From **Figure 9**, when deception occurs (t = 3s), the output voltage and reactive power of each DG remain normal. After power disturbance, except for the attacked DG1, other DGs obtain the equal sharing of reactive power, which indicates that the proposed control approach makes the microgrid maintain normal physical operation under deception attack. The original control purpose of the microgrid has still not been achieved either. Comparing **Figure 6** and **Figure 9**, during the deception attack, the reactive power of the attacked DG1 changes to the local control by the distributed resilient control method. Thus, its reactive power automatically adjusts according to the droop characteristic rather than reaching equal sharing with other DGs after load disturbance at t = 4 s. The local credibility of each DG and the neighbor credibility of DG2 are depicted in **Figure 9**. The local detection of A1 can effectively identify the native FDIA, verifying the analysis of the FDIA situation in **section 3.2**. In the meantime, the local credibility value $c_1 = 0$ protects the physical state of DG1 from the impact of the injected attack signal. Additionally, for instance, A2 eliminates the reactive power data from A1 that are injected by the attack signal by setting neighbor credibility value $T_{21} = 0$. The results of A3 and A4 are the same as A2. In this way, the attack signal is isolated in A1 to realize the resilient operation of microgrid CPS.

5.3 Case 3: Disruption Attack Mitigation

In this case, the attack signal is injected into the attacked cyber node A1, whose actual reactive power data are transmitted to its neighbor nodes A2, A3, and A4. The simulation result is depicted in **Figure 10**. Comparing **Figure 8** and **Figure 10**, the operation state is the same as that under disruption attack, which indicates that the proposed resilient control method can effectively avoid the voltage and reactive power instability caused by disruption attack in the microgrid. From **Figure 10**, the local detection successfully identifies FDIA. Then, DG1 updates local credibility $c_1 = 0$ to make its secondary reactive power control exits, which guarantees the cyber security of microgrid CPS. Besides, due to the actual operation data sent from A1 to neighbor nodes, the neighbor credibility value T_{21} remains around 1, as well as the neighbor credibility values T_{31} and T_{41} of A3 and A4. Thus, A1 is equivalent to the leader in MAS. The output reactive power of other DGs follows DG1 so that the output reactive power of all DGs in the microgrid can still achieve average sharing.

5.4 Case 4: Comparison of Different Resilient Control Algorithms

To verify the effectiveness and advantage of the distributed credibility-based consensus algorithm, the median-based consensus algorithm (Sheng et al., 2021) is used to mitigate the FDIA in microgrids, which removes the attack signal by selecting the median value of neighbor data to participate in the iteration of consensus update. The FDIA scenario is the same as that in Case 2. **Figure 11** depicts the simulation results of the distributed median-based consensus control method. According to **Figure 11**, the distributed median-based consensus control method has the ability to restrain the effect of the deception attack during t = 3–5 s. Comparing **Figure 9** and **Figure 11**, both the resilient consensus algorithms can mitigate the deception attack. However, in order to remove the attack signal, the median-based consensus algorithm abandons the normal neighbor data as the expense, which only retains the middle state of all neighbors. Thus, the reactive power of DGs cannot synchronize the average value when the load disturbance occurs at t = 4 s during the deception attack. The proposed credibility-based consensus algorithm only removes the data of the attacked neighbor by an adaptive update of credibility values, which results in that the normal DGs achieve the consensus whenever load disturbance occurs. In addition, the median-based consensus algorithm only has an effect in the situation where the transmitted data have been injected with the attack signal. The proposed method can mitigate FDIA whether in deception or disruption attack, which indicates its advantage.

6 CONCLUSION

With the control failure and even system results from cyber attack on the cooperative control of microgrids, this article investigates the synchronous mitigation framework based on local detection where the reactive power cooperative control targets of microgrids with and without FDIA are compatible with the resilient control method. The credibility is utilized to measure the reliability of local and neighbor data in the proposed method. The consensus communication coupling

gain is weighted corrected by the adaptive update strategy of credibility to delete the attack signal. Besides, the proposed method directly improves the conventional distributed secondary controller that reduces the complexity of controller design. Simulations verify the effectiveness of the distributed resilient consensus cooperative control method under conditions of deception and disruption attacks.

DATA AVAILABILITY STATEMENT

The original contributions presented in the study are included in the article/Supplementary Material, further inquiries can be directed to the corresponding author.

AUTHOR CONTRIBUTIONS

GC and RJ proposed the methodology. GC and JD conducted the theoretical analysis as well as the simulation verification. GC wrote the original draft, which was reviewed and edited by RJ and JD. All authors agree to be accountable for the content of the work.

FUNDING

This research was supported by the key project of the Natural Science Basic Research Plan in Shaanxi Province of China, Grant 2019ZDLGY18-03.

REFERENCES

Abhinav, S., Modares, H., Lewis, F. L., and Davoudi, A. (2019). Resilient Cooperative Control of DC Microgrids. *IEEE Trans. Smart Grid* 10 (1), 1083–1085. doi:10.1109/tsg.2018.2872252

Alavi, S. A., Mehran, K., Hao, Y., Rahimian, A., Mirsaeedi, H., and Vahidinasab, V. (2019). A Distributed Event-Triggered Control Strategy for DC Microgrids Based on Publish-Subscribe Model over Industrial Wireless Sensor Networks. *IEEE Trans. Smart Grid* 10 (4), 4323–4337. doi:10.1109/TSG.2018.2856893

Cao, G., Gu, W., Li, P., Sheng, W., Liu, K., Sun, L., et al. (2020). Operational Risk Evaluation of Active Distribution Networks Considering Cyber Contingencies. *IEEE Trans. Ind. Inf.* 16 (6), 3849–3861. doi:10.1109/tii.2019.2939346

Cao, G., Gu, W., Lou, G., Sheng, W., and Liu, K. (2022). Distributed Synchronous Detection for False Data Injection Attack in Cyber-Physical Microgrids. *Int. J. Electr. Power Energ. Syst.* 137, 107788. doi:10.1016/j.ijepes.2021.107788

Deng, C., Wang, Y., Wen, C., Xu, Y., and Lin, P. (2021). Distributed Resilient Control for Energy Storage Systems in Cyber-Physical Microgrids. *IEEE Trans. Ind. Inf.* 17 (2), 1331–1341. doi:10.1109/tii.2020.2981549

Deng, C., and Wen, C. (2020). Distributed Resilient Observer-Based Fault-Tolerant Control for Heterogeneous Multiagent Systems under Actuator Faults and DoS Attacks. *IEEE Trans. Control. Netw. Syst.* 7 (3), 1308–1318. doi:10.1109/tcns.2020.2972601

Deng, C., and Wen, C. (2021). MAS-based Distributed Resilient Control for a Class of Cyber-Physical Systems with Communication Delays under DoS Attacks. *IEEE Trans. Cybern.* 51 (5), 2347–2358. doi:10.1109/TCYB.2020.2972686

Deng, R., Xiao, G., Lu, R., Liang, H., and Vasilakos, A. V. (2017). False Data Injection on State Estimation in Power Systems-Attacks, Impacts, and Defense: A Survey. *IEEE Trans. Ind. Inf.* 13 (2), 411–423. doi:10.1109/tii.2016.2614396

Dibaji, S. M., Pirani, M., Flamholz, D. B., Annaswamy, A. M., Johansson, K. H., and Chakrabortty, A. (2019). A Systems and Control Perspective of CPS Security. *Annu. Rev. Control.* 47, 394–411. doi:10.1016/j.arcontrol.2019.04.011

E-ISAC (2016). *Analysis of the Cyber Attack on the Ukrainian Power Grid*. Washington, D.C., USA: E-ISAC.

He, Y., Mendis, G. J., and Wei, J. (2017). Real-Time Detection of False Data Injection Attacks in Smart Grid: A Deep Learning-Based Intelligent Mechanism. *IEEE Trans. Smart Grid* 8 (5), 2505–2516. doi:10.1109/tsg.2017.2703842

Lai, R., Qiu, X., and Wu, J. (2019). Robustness of Asymmetric Cyber-Physical Power Systems against Cyber Attacks. *IEEE Access* 7, 61342–61352. doi:10.1109/access.2019.2915927

Li, Z., Shahidehpour, M., Alabdulwahab, A., and Abusorrah, A. (2016). Bilevel Model for Analyzing Coordinated Cyber-Physical Attacks on Power Systems. *IEEE Trans. Smart Grid* 7 (5), 2260–2272. doi:10.1109/TSG.2015.2456107

Li, Z., Shahidehpour, M., and Aminifar, F. (2017). Cybersecurity in Distributed Power Systems. *Proc. IEEE* 105 (7), 1367–1388. doi:10.1109/jproc.2017.2687865

Liang, G., Zhao, J., Luo, F., Weller, S. R., and Dong, Z. Y. (2017). A Review of False Data Injection Attacks against Modern Power Systems. *IEEE Trans. Smart Grid* 8 (4), 1630–1638. doi:10.1109/tsg.2015.2495133

Liang, J., Sankar, L., and Kosut, O. (2016). Vulnerability Analysis and Consequences of False Data Injection Attack on Power System State Estimation. *IEEE Trans. Power Syst.* 31 (5), 3864–3872. doi:10.1109/tpwrs.2015.2504950

Liu, J., Du, Y., Yim, S.-i., Lu, X., Chen, B., and Qiu, F. (2021). Steady-State Analysis of Microgrid Distributed Control under Denial of Service Attacks. *IEEE J. Emerg. Sel. Top. Power Electron.* 9 (5), 5311–5325. doi:10.1109/jestpe.2020.2990879

Liu, W., Gu, W., Sheng, W., Meng, X., Wu, Z., and Chen, W. (2014). Decentralized Multi-Agent System-Based Cooperative Frequency Control for Autonomous Microgrids with Communication Constraints. *IEEE Trans. Sustain. Energ.* 5 (2), 446–456. doi:10.1109/TSTE.2013.2293148

Liu, W., Gu, W., Sheng, W., Meng, X., Xue, S., and Chen, M. (2016a). Pinning-based Distributed Cooperative Control for Autonomous Microgrids under Uncertain Communication Topologies. *IEEE Trans. Power Syst.* 31 (2), 1320–1329. doi:10.1109/TPWRS.2015.2421639

Liu, X., Bao, Z., Lu, D., and Li, Z. (2015b). Modeling of Local False Data Injection Attacks with Reduced Network Information. *IEEE Trans. Smart Grid* 6 (4), 1686–1696. doi:10.1109/tsg.2015.2394358

Lou, G., Gu, W., Xu, Y., Cheng, M., and Liu, W. (2017). Distributed MPC-Based Secondary Voltage Control Scheme for Autonomous Droop-Controlled Microgrids. *IEEE Trans. Sustain. Energ.* 8 (2), 792–804. doi:10.1109/TSTE.2016.2620283

Olivares, D. E., Mehrizi-Sani, A., Etemadi, A. H., Canizares, C. A., Iravani, R., Kazerani, M., et al. (2014). Trends in Microgrid Control. *IEEE Trans. Smart Grid* 5 (4), 1905–1919. doi:10.1109/tsg.2013.2295514

Sahoo, S., Dragicevic, T., and Blaabjerg, F. (2021). Multilayer Resilience Paradigm against Cyber Attacks in DC Microgrids. *IEEE Trans. Power Electron.* 36 (3), 2522–2532. doi:10.1109/tpel.2020.3014258

Sahoo, S., Peng, J. C.-H., Devakumar, A., Mishra, S., and Dragicevic, T. (2020). On Detection of False Data in Cooperative DC Microgrids-A Discordant Element Approach. *IEEE Trans. Ind. Electron.* 67 (8), 6562–6571. doi:10.1109/tie.2019.2938497

Sheng, L., Gu, W., Cao, G., and Chen, X. (2021). A Distributed Detection Mechanism and Attack-Resilient Strategy for Secure Voltage Control of AC Microgrids. *CSEE Power Energ. Syst*. Accepted.

Wang, T., Rong, C., Tang, S., and Hong, Y. (2021a). Stability Analysis for Distributed Secondary Control with Consideration of Diverse Input and Communication Delays for Distributed Generations in a DC Integrated Energy System. *Front. Energ. Res.* 8, 633334. doi:10.3389/fenrg.2020.633334

Wang, Y., Amin, M. M., Fu, J., and Moussa, H. B. (2017). A Novel Data Analytical Approach for False Data Injection Cyber-Physical Attack Mitigation in Smart Grids. *IEEE Access* 5, 26022–26033. doi:10.1109/access.2017.2769099

Wang, Y., Mondal, S., Deng, C., Satpathi, K., Xu, Y., and Dasgupta, S. (2021b). Cyber-Resilient Cooperative Control of Bidirectional Interlinking Converters in Networked AC/DC Microgrids. *IEEE Trans. Ind. Electron.* 68 (10), 9707–9718. doi:10.1109/tie.2020.3020033

Yu, X., and Xue, Y. (2016). Smart Grids: A Cyber-Physical Systems Perspective. *Proc. IEEE* 104 (5), 1058–1070. doi:10.1109/JPROC.2015.2503119

Zhang, H., Meng, W., QiWang, J. X., Wang, X., and Zheng, W. X. (2019). Distributed Load Sharing under False Data Injection Attack in an Inverter-Based Microgrid. *IEEE Trans. Ind. Electron.* 66 (2), 1543–1551. doi:10.1109/TIE.2018.2793241

Conflict of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.