APPENDIX I

TABLE VI
POWER DISPATCH RESULTS (KW) AT T=4 WHEN NODE 10 IS UNDER A NON-COLLUSION ATTACK, NODE 11 AND 12 ARE THE AFFECTED NODES.

Node	10	11	12	Normal nodes	$\sum P - \sum D$
Without attack	13.5135	-19.1000	-4.5000	10.0865	0.0000
Under attack	17.5661	-19.1000	4.5000	-2.9661	0.0000
Difference	+4.0526	0.0000	+9.0000	-13.0526	0.0000

TABLE VII
POWER DISPATCH RESULTS (KW) AT T=5 WHEN NODE 10 IS UNDER A COLLUSION ATTACK, NODE 11 AND 12 ARE THE AFFECTED NODES.

Node	10	11	12	Normal nodes	$\sum P - \sum D$
Without attack	17.4000	-17.5000	4.5000	-4.4000	0.0000
Under attack	12.1120	-17.5000	-4.5000	9.8880	0.0000
Difference	-5.2880	0.0000	-9.0000	14.2880	0.0000

APPENDIX II
CONVERGENCE ANALYSIS

As proved in [24], [26], [27], if the digraph $\mathcal{G}$ is strongly connected, and $\eta>0$ is sufficiently small, $s \in \mathcal{V}$, $z \in N_s$, $\omega_{s,z}$ is restricted to $0 < w_{s,z} < (\max_{s\in\mathcal{V}} |N_s|)^{-1}$, then the DEM algorithm in (2) - (5) converges to a stable point.

Under the proposed attack, the DEM algorithm can still converge as long as the attacker avoids causing drastic changes in the convergence process of the target value. We set up *Case IV* to validate the convergence of the proposed algorithm under different experiment parameters.

Case IV: The attacker and attacked node are node 9 and 10 respectively, a non-collusion attack is launched on node 10 at t=4. To differentiate from previous experiments, k_{attack} is set to 450. The target value is set to 20.27, a 50% increase compared to that without attack. The control parameters $\omega_{s,z}$ and η significantly impact the convergence speed, so we set the values of them from large to small in Table VIII.

TABLE VIII
EXPERIMENT PARAMETERS IN *Case IV*

Fig. 13	$\omega_{s,z}$	η
Row 1	0.1541	0.1502
Row 2	0.1410	0.1295
Row 3	0.1279	0.1088
Row 4	0.1148	0.0881
Row 5	0.1017	0.0674
Row 6	0.0886	0.0468
Row 7	0.0755	0.0261
Row 8	0.0624	0.0055

The experimental results, as depicted in Fig. 13, show that the algorithm converged while maintaining both power balance and the consistency. The actual power command $P_{10,\text{f}}$ follows the attacker's set curve $P_{10,\text{aim}}$, indicating the success of the attack. When setting the convergence process of $P_{10,\text{aim}}$, drastic changes should be avoid, as the false data $P^k_{9,f}$ is generated from $P_{10,\text{aim}}$. Drastic changes in $P_{10,\text{aim}}$ could cause fluctuations in $P^k_{9,f}$. If these fluctuations are too sharp, the DEM algorithm may fail to converge. There are many ways to generate $P_{10,\text{aim}}$ and prevent drastic fluctuations. In this paper, we use linear convergence to generate $P_{10,\text{aim}}$, i.e.,

$$P^{k+1}_{10,\text{aim}} = P^k_{10,\text{aim}} \pm \alpha \left| P^k_{10,\text{aim}} - P_{\text{aim}} \right| \tag{25}$$

where P_{aim} is the target value, which is 20.27 in Case IV. α is a parameter controlling the convergence speed of $P^k_{10,\text{aim}}$. The smaller the value of α, the lighter the fluctuations in consensus variables. For example, we set it to 0.05 in Case IV.

In summary, by avoiding drastic changes in the convergence process of the set value $P_{10,\text{aim}}$, the convergence of the proposed algorithm can be guaranteed.

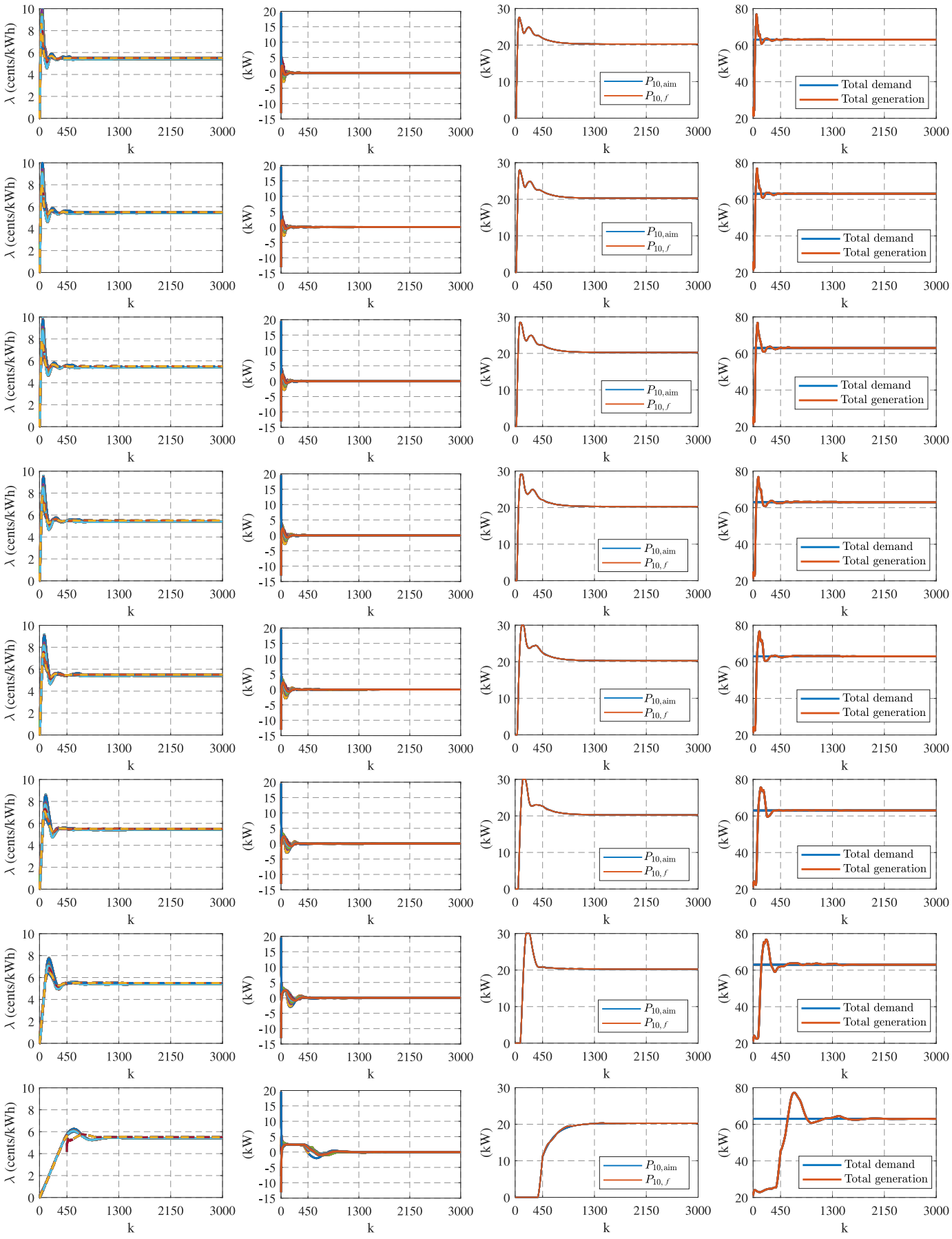

Fig. 13. The experiment results in *Case IV*.