Distributed Control for AC Microgrids with False Data Injection Attacks and Time Delays

Rentao Lu, *Jie* Wang*

School of Electrical and Electronic Engineering, Shanghai Jiaotong University, Minhang District, Shanghai 200240, China

Abstract. Distributed control is widely used in AC microgrids to maintain frequency and voltage stability and internal power balance. However, distributed control need realizes information interaction through communication network, which makes microgrid vulnerable to network attack. A distributed control strategy based on consensus theory is proposed in this paper to enhance the resilience of microgrid to attack. An attack detection and localization method is designed for the false data injection attack. The Artstein's transformation is introduced to process the delay data and the performance of controller under delay can be enhanced. An isolated island AC microgrid model was built in Simulink platform for simulation to verify the performance of the controller. The simulation results verified the effectiveness of the control strategy against false data injection attack and time delay.

1 INTRODUCTION

With the increasing demand of power supply, new energy represented by photovoltaic and wind power has developed rapidly because of its renewable, clean and pollution-free nature [1]. However, photovoltaic and wind power generation are relatively dispersed due to environmental location and other factors, thus forming distributed generation (DG). Effective network management of distributed generations is particularly important to ensure the reliability, stability and economy of power supply. Microgrids are widely used as an effective network management method for distributed generations. Microgrid is a small power generation and distribution system composed of distributed generations, energy storage devices, electrical loads, conversion, control and other equipment [2]. In order to achieve the accurate power sharing and frequency/voltage stability of DGs in microgrid, distributed control has been widely used due to its good robustness, communication flexibility and system expansibility [3].

Distributed control consists of distributed controllers and communication network, which realize the consensus control of the controlled state variables based on the information exchange through the communication network. The stability and reliability of communication network are important to maintain the normal operation of microgrid consensus control system. In the actual communication network, interference is often difficult to avoid, and it will affect the normal operation of the microgrid in severe cases. Communication interference will cause deviations in frequency, voltage and power distribution between DGs in the microgrid [4].

The information exchange in distributed control makes microgrid vulnerable to network attacks. The attack may destroy the exchanged data by attacking the node, the communication link or hijacking the entire node. The destroyed data can interrupt the synchronization of DGs and lead to the instability of the entire microgrid system.

Existing research mainly focuses on attack detection and enhancement of network architecture. In [5], the characteristics and effects of several different types of false data injection attacks (FDIAs) are analysed and corresponding countermeasures are proposed. A signal temporal logic detection method is proposed in [6] for effectively detect, locate and qualify attack. In [7], a cooperative vulnerability factor (CVF) framework is introduced for each agent, and the positive value of CVF represents that the agent is attacked. A software-defined networking communication architecture and a secure network of assured power enclaves are respectively proposed in [8-9] to enhance the attack resistance of microgrid.

Distributed control also inevitably has the problem of communication delay, and the high communication delay will lead to the performance degradation of distributed controller [10-11]. For distributed control, the communication delay compensation strategies mainly include predictive control method [12], gain scheduling method [13], H-∞ control method [14], sliding mode control [15] and control method based on multi-timer [16]. In [17], a distributed control strategy with high delay adaptability is proposed, which can enhance the system's resistance to high delay. A coordinated control based on droop theory for time-varying delay is developed in [18], which can eliminate the influence of delay based on the local information and the neighbor information at the same time point. In this paper, the Artstein's transformation is implemented to transform the input

* Jie Wang: jiewangxh@sjtu.edu.cn

delay system into an ordinary differential system, which can effectively simplify the stability analysis and reduce the impact of delay on the controller performance. This paper proposes a new hierarchical cooperative control strategy under the premise of fully considering false data injection attack and communication delay.

The organization of this paper is as follows. The attack detection and localization method and the processing method of delayed data are present in section II. Section III presents the hierarchical control structure. With this, we present the case study that was carried out in section IV, ending with section V with the conclusions.

2 PROBLEM FORMULATION

2.1. Conensus Control

The combination of distributed generation, LCL filter, inverter and load in the microgrid is labeled as an agent. The communication data of the i-th agent is marked as $x_i(t)(i = 1,2,\cdots,n)$. The virtual leader can transmit communication data to other agents, and the leader's communication data is marked as $x_L(t)$. For a multi-agent system, the leader-follower consensus is given as

$$\lim_{t\to\infty}\left\|x_i(t)-x_L(t)\right\|=0 \tag{1}$$

The first-order mathematical model of multi-agent system is as follows:

$$\dot{x}_i(t)=u_i(t) \tag{2}$$

where $u_i \in R^n$ is the control input of the i-th agent.

Based on the above analysis, the communication data of each follower will be consistent with the leader's communication data through the consensus protocol which is given by

$$\dot{x}_i(t)=c_1\sum_{j\in N_i}a_{ij}\left(x_j(t)-x_i(t)\right)+c_2a_{i0}\left(x_L-x_i(t)\right) \tag{3}$$

where c_1 and c_2 are the gain of the consensus protocol.

2.2 Attack detection and location

There are two main types of cyber attacks in the microgrid, namely denial of service attacks and FDIAs. FDIA disrupts the stable state by injecting false data into communication information, and denial of service attack disrupts the stable operation of the system by interrupting the information exchange in the communication link.

1) Link attack

The communication link suffers from false data injection attack, and the communication information is injected with additional disturbance quantity. The receiver of the attacked communication link will receive the damaged information. The model of the link attack is given by

$$y_i = x_i + \sum_{j\in N_i}a_{ij}\left[\left(x_j+\sigma_j x_j^a\right)-x_i\right]+a_{i0}\left[x_L-x_i\right] \tag{4}$$

where x_j^a is the false data that the transmission information is injected; σ_j is the attack coefficient, in the presence of false data injection, $\sigma_j = 1$, otherwise, $\sigma_j = 0$; y_i is the measurement of DG$_i$.

2) Node attack

The malicious input acts on the attacked node. Additional false data is injected to destroy the information of the node and all neighbors of the attacked node will receive the destroyed information. The model of the node attack is given by

$$y_i = x_i + \sum_{j\in N_i}a_{ij}\left[\left(x_j+\varepsilon_j x_j^a\right)-\left(x_i+\varepsilon_i x_i^a\right)\right]$$
$$+a_{i0}\left[x_L-\left(x_i+\varepsilon_i x_i^a\right)\right] \tag{5}$$

where x_j^a is the false data injected into the node information; ε_i is the attack coefficient, in the presence of false data injection, $\varepsilon_i = 1$, otherwise, $\varepsilon_i = 0$; y_i is the measurement of DG$_i$.

3) Detection and location method

In order to realize the detection of cyber attacks, according to the local neighbor tracking error we can define

$$\Delta x_i(t)=x^{ref}(t)-x_i(t) \tag{6}$$

$$b_i(t)=h_i\sum_{j\in N_i}a_{ij}\left(\Delta x_j(t)-\Delta x_i(t)\right)+\sum_{j\in N_i}a_{ij}\left(\Delta x_j(t)+\Delta x_i(t)\right) \tag{7}$$

In the normal operation, $x_i(t) = x_j(t) = x^{ref}$, $b_i(t) = 0$; in the presence of attack, $\Delta x_i(t) \neq \Delta x_j(t) \neq 0$, $b_i(t) \neq 0$. Therefore, the existence of FDIA can be determined by detecting the value of $b_i(t)$.

The value of $b_i(t)$ can detect the existence of FDIA, but the localization of FDIA cannot be achieved. To achieve this goal, we define

$$d_i(t)=\sigma_i\left(\sigma_i+b_i(t)\right)^{-1} \tag{8}$$

$$\dot{C}_i(t) = \mu d_i(t) - \mu C_i(t) \tag{9}$$

where $\mu > 0$ is the weigh of C_i.

The value of $\mathrm{C_i}$ of the node close to the attack source is small, and the location of the node attack can be realized by detecting the value of $\mathrm{C_i}$.

For link attacks, we define

$$\rho_{ij}(t)=nx_j(t)-\sum_{k\in N_i}x_k(t) \tag{10}$$

where n is the number of neighbor nodes of DG$_i$.

$$s_{ij}(t)=\varepsilon_i\left(\varepsilon_i+\rho_{ij}(t)\right)^{-1} \tag{11}$$

where ε_i is a threshold set according to the microgrid.

$$T_{ij}(t)=\chi s_{ij}(t)-\chi T_{ij}(t) \tag{12}$$

where$\mathcal{X} > 0$ is the weigh of T_{ij}.

In the presence of attack, $\rho_{ij} \neq 0$, the distance between the communication link and the attack source determines the value of ρ_{ij}. Link attack localization can be realized by detecting the value of T_{ij}.

2.3 Communication time delay

The information exchange in distributed control determines the inevitability of time delay. Therefore, it is necessary to design distributed controller to improve the controller performance under the premise of considering delay. In this paper, the Artstein's transformation is introduced to transform the delay control system into an ordinary differential control system, and the stability problem can be analyzed based on the simplified system.

The application of Artstein's transformation can transform the input delay system (2) into a first-order integral system without delay which can given by

$$x_i^y = x_i + \int_{t-\tau_i}^{t} u_i(s)ds \tag{13}$$

$$\dot{x}_i^y = u_i(t) \tag{14}$$

The Artstein transformation can guarantee the stability of the time-delay system as long as the simplified ordinary differential control system is stable.

The consensus control after Artstein's transformation is as follows:

$$\dot{x}_i(t) = c_1 \sum_{j\in N_i} a_{ij}\left(x_j^y(t) - x_i^y(t)\right) + c_2 a_{i0}\left(x_L - x_i^y(t)\right) \tag{15}$$

3 DESIGN OF DISTRIBUTED CONTROL

3.1. Primary Control

Consider an isolated AC microgrid with multiple DGs. In order to improve system performance, hierarchical coordinated control is used in the microgrid. The primary control is used to maintain frequency, voltage stability and active/reactive power distribution. The secondary control is used to eliminate the deviation caused by the primary control.

The primary control usually adopts droop theory, and the design of droop controller considers the dynamic characteristics of active and reactive power droop technology. The primary control method based on droop technology is:

$$\begin{cases} \omega_i = \omega_{ni} - m_i P_i \\ V_i = V_{ni} - n_i Q_i \end{cases} \tag{16}$$

where ω_i and V_i are the output angular frequency and voltage magnitude of the ith DG, respectively; ω_{ni} and V_{ni} are the frequency and voltage amplitudes of the nominal set point, respectively, which will be regulated by the secondary control; m_i and n_i are the droop coefficients of active power and reactive power, respectively; P_i and Q_i are the measured active and reactive power, respectively.

Transform (16) into *d*-*q* reference frame form as

$$\begin{cases} \omega_i = \omega_{ni} - m_i P_i \\ \begin{cases} V_i^{od} = V_{ni} - n_i Q_i \\ V_i^{oq} = 0 \end{cases} \end{cases} \tag{17}$$

where V_i^{od} and V_i^{oq} are the d-axis and q-axis output voltage references, respectively.

The measured active and reactive power of DG i is given by

$$\begin{cases} P_i = \dfrac{\omega_i^c}{\omega_i^c + s}\left(V_i^{od} I_i^{od} + V_i^{oq} I_i^{oq}\right) \\ Q_i = \dfrac{\omega_i^c}{\omega_i^c + s}\left(V_i^{od} I_i^{oq} - V_i^{oq} I_i^{od}\right) \end{cases} \tag{18}$$

where ω_i^c is the cutoff frequency of the low pass filter.

3.2. Secondary Control

The primary control will produce deviations that make the frequency and voltage amplitude lower than their respective rated values, and the secondary control aims to eliminate the deviation. In this distributed structure, each DG's controller only needs the local information and the information of neighbor nodes to achieve the control goal, which greatly reducing the amount of communication and improving the robustness of the system.

According to the previous analysis, the input and output of the secondary frequency controller are ω_{ni} and ω_i respectively. The secondary control is to design an appropriate ω_{ni} to achieve synchronization between ω_i and the reference value.

By using feedback linearization, the derivative of (17) is obtained

$$\dot{\omega}_i = \dot{\omega}_{ni} - m_i \dot{P}_i = u_{\omega i} \tag{19}$$

where $u_{\omega i}$ is the designed secondary frequency controller.

In order to enhance the resilience of the microgrid against attacks and delays, a secondary frequency controller is designed as:

$$u_{\omega_i} = c_1 \sum_{j\in N_i} a_{ij} C_j T_{ij}\left(\omega_j^y(t) - \omega_i^y(t)\right) + c_2 a_{i0}\left(\omega_L - \omega_i^y(t)\right) \tag{20}$$

The input of the secondary control is given by

$$\omega_{ni} = \int\left(u_i + m_i \dot{P}_i\right)dt \tag{21}$$

4 CASE STUDY

The distributed controller is applied to the island AC microgrid with 5 DGs, and its system topology is shown in Figure 1. The system is built in Matlab-Simulink environment, and the distributed controller designed in this paper is assembled to verify its performance. The parameters of the controller are $c_1 = c_2 = 2$, $c_3 = 2$.

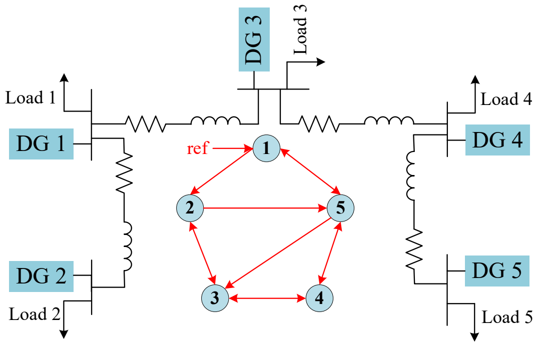

Fig. 1 The test islanded AC microgrid with five DGs.

In order to verify the performance of the distributed controller consider attack and communication delay proposed in this paper, the following five scenarios are verified:

1)$t = 1s$, start the secondary controller considering attack and communication delay;

2)$t = 2s$, apply communication delay $\tau = 0.2s$;

3)$t = 3s$, apply link attack; the communication link between DG2 and DG3 was attacked, generate a damaged frequency $f_2 = 50.1Hz$.

4)$t = 4s$, apply node attack; the entire controller of DG2 was hijacked and the frequency information was destroyed, generate a damaged frequency $f_2 = 50.1Hz$.

5)$t = 5s$, remove node attack.

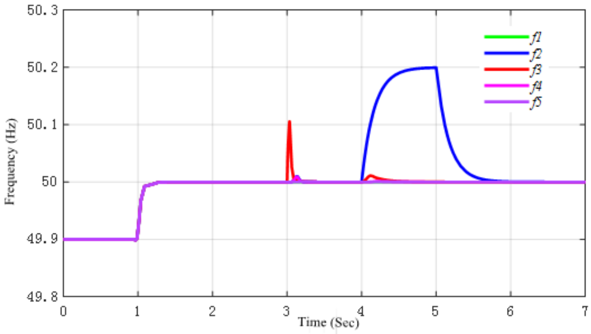

Fig. 2 The frequencies of DGs in different scenaios.

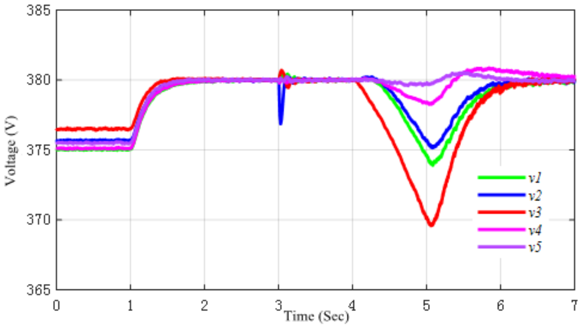

Fig. 3 The voltages of DGs in different scenarios.

The primary control is initially activated, while the secondary control is deliberately disabled. The primary control causes voltage and frequency to deviate from the nominal value. In the first scenario, the secondary control in (20) is activated at t=1s. It can be seen from Fig. 2 and Fig. 3 that the frequencies and voltages can quickly aligned to their reference values. In the second scenario, we add additional communication delays to the controller, and the controller can realize almost no fluctuation control of system frequency and voltage.

In the third scenario, the link attack can be quickly eliminated through the attack detection and localization method in the controller, and the system voltage and frequency stability can be quickly restored. The node attack in scenario 4 directly hijacks the entire controller and causing the frequency of DG2 oprating in an abnormal state. The internal physical connection of the system causes the voltages of DGs to oscillate. Although the controller cannot eliminate the node attack, it can still detect and prevent the spread of the attack in the communication network. After the node attack is eliminated in scenario 5, the system voltage and frequency gradually stabilize.

5 CONCLUSION

This paper proposes a distributed control strategy based on the consensus theory for voltage and frequency control of AC microgrids. The designed attack detection and location strategy can effectively realize the processing of both link and node FDIAs. The Arestein's transformation is used to transform the input delay system into an ordinary differential system to enhance the delay characteristic of the controller. The simulation results show that the distributed control method proposed in this paper can effectively detect false data injection attacks and enhance the delay characteristics, thereby improving the resilience and stability of microgrid.

References

1. Y. Han, K. Zhang, H. Li, E. A. A. Coelho and J. M. Guerrero, "MAS-based distributed coordinated control and optimization in microgrid and microgrid clusters: A comprehensive overview," *IEEE Transactions on Power Electronics*, vol. 33, no. 8, pp. 6488-6508, Aug. 2018.
2. X. Lu, X. Yu, J. Lai, Y. Wang and J. M. Guerrero, "A novel distributed secondary coordination control approach for islanded microgrids," *IEEE Transactions on Smart Grid*, vol. 9, no. 4, pp. 2726-2740, July 2018.
3. N. Li and J. R. Marden, "Decoupling coupled constraints through utility design," *IEEE Transactions on Automatic Control*, vol. 59, no. 8, pp. 2289-2294, Aug. 2014.
4. A. Nisar and M. S. Thomas, "Comprehensive control for microgrid sutonomous operation with demand response," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2081-2089, Sept. 2017.
5. O. Kosut, L. Jia, R. J. Thomas and L. Tong, "Malicious data attacks on the smart grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 645-658, Dec. 2011.
6. O. A. Beg, L. V. Nguyen, T. T. Johnson and A. Davoudi, "Signal temporal logic-based attack detection in DC microgrids," *IEEE Transactions on Smart Grid*, vol. 10, no. 4, pp. 3585-3595, July 2019.
7. S. Sahoo, S. Mishra, J. C. Peng and T. Dragičević, "A stealth cyber-attack detection strategy for DC microgrids," *IEEE Transactions on Power Electronics*, vol. 34, no. 8, pp. 8162-8174, Aug. 2019.
8. D. Jin et al., "Toward a cyber resilient and secure microgrid using software-defined networking," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2494-2504, Sept. 2017.
9. M. Rana, "Architecture of the internet of energy network: an application to smart grid communications," *IEEE Access*, vol. 5, pp. 4704-4710, 2017.
10. L. Ding, Q. Han, L. Y. Wang and E. Sindi, "Distributed cooperative optimal control of DC microgrids with communication delays," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 9, pp. 3924-3935, Sept. 2018.

11. C. Zhao, W. Sun, J. Wang, Q. Li, D. Mu and X. Xu, "Distributed cooperative secondary control for islanded microgrid with markov time-varying delays," *IEEE Transactions on Energy Conversion*, vol. 34, no. 4, pp. 2235-2247, Dec. 2019.
12. C. Ahumada, R. Cárdenas, D. Sáez and J. M. Guerrero, "Secondary control strategies for frequency restoration in islanded microgrids with consideration of communication delays," *IEEE Transactions on Smart Grid*, vol. 7, no. 3, pp. 1430-1441, May 2016.
13. J. Mei, W. Ren and J. Chen, "Distributed consensus of second-order multi-agent systems with heterogeneous unknown inertias and control gains under a directed graph," *IEEE Transactions on Automatic Control*, vol. 61, no. 8, pp. 2019-2034, Aug. 2016.
14. C. Dou, D. Yue, J. M. Guerrero, X. Xie and S. Hu, "Multiagent system-based distributed coordinated control for radial DC microgrid considering transmission time delays," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2370-2381, Sept. 2017.
15. P. Ignaciuk and A. Bartoszewicz, "Discrete-time sliding-mode Congestion Control in Multisource Communication Networks With time-varying delay," *IEEE Transactions on Control Systems Technology*, vol. 19, no. 4, pp. 852-867, July 2011.
16. J. Qin, F. Li, S. Mou and Y. Kang, "Multi-timer based event synchronization control for sensor networks and its application," *IEEE Transactions on Industrial Electronics*, vol. 63, no. 12, pp. 7765-7775, Dec. 2016.
17. C. Ahumada, R. Cárdenas, D. Sáez and J. M. Guerrero, "Secondary control strategies for frequency restoration in islanded microgrids with consideration of communication delays," *IEEE Transactions on Smart Grid*, vol. 7, no. 3, pp. 1430-1441, May 2016.
18. J Lai，H Zhou，X Lu，X Yu and W Hu, "Droop-based distributed cooperative control for microgrids with time-varying delays," *IEEE Transactions on Smart Grid*，vol. 7, no. 4, pp. 1775-1789, July 2016.
19. Z. Artstein, "Linear systems with delayed controls: A reduction," *IEEE Transactions on Automatic Control*, vol. 27, no. 4, pp. 869-879, Jan 1982.