An Attack-Resilient Cooperative Control Strategy of Multiple Distributed Generators in Distribution Networks

Yun Liu, *Student Member, IEEE*, Huanhai Xin, *Member, IEEE*, Zhihua Qu, *Fellow, IEEE*, and Deqiang Gan, *Senior Member, IEEE*

***Abstract*—Distributed generators (DGs) have been developing rapidly in power systems. Motivated by their intrinsic distributed nature, distributed cooperative control based upon local communication recently emerge as a preferred strategy. For instance, a cooperative power control strategy can regulate the active power from a cluster of DGs at a certain ratio of its maximal available power according to a dispatch command. However, such a networked control system is susceptible to both communication failure and cyber-attack, e.g., denial-of-service attack and deceptive attack. To address this potential problem, an attack-resilient cooperative control strategy is proposed in this paper. With a properly designed observation network, each DG can monitor the behaviors of all its in-neighbors, and gradually isolate the misbehaving DGs (when present) from the network as long as they do not collude with each other. Consequently, even certain DGs misbehave, the rest of them can together accomplish the control objective provided that the remaining communication network is still connected. Simulations of the IEEE standard 34-bus test feeder demonstrate effectiveness of the proposed strategy.**

***Index Terms*—Cyber-attack, distribution network, networked control system, attack-resilient cooperative control, virtual power plant.**

I. Introduction

IN THE past decade, due to the increasing cost of fossil fuels and environmental problems, the focus of power industry has gradually shifted from synchronous generators to power converter based distributed generators (DGs) [1]. DGs, most of which are connected to the distribution networks, can reduce power transmission loss and maintain power supply to communities even in emergency conditions by operating the microgrid in an islanded mode [2]. However, since DGs are generally small-scale resources [3], several of them should be clustered in the distribution network to accumulate enough capacity. This challenges the conventional centralized control scheme, which requires each DG to communicate with a central controller directly. This centralized scheme, although enjoys the advantage of simplicity in design and can achieve complicated control objectives, is not suitable for geographically dispersed DGs and real-time control since it requires a high bandwidth of communication and is not plug-and-play for DGs [4].

Motivated by the intrinsic distributed nature of DGs, networked control system (NCS) based distributed cooperative control scheme, which only requires local communications among geographic neighbors to fulfill certain goals, is more preferred in the control of multiple DGs due to its advantages including low operating cost, less system requirement, robustness to communication interruption, and flexible scalability. For these reasons, relevant work has extensively been done in the past five years. To name a few, cooperative control is applied to the design of a virtual power plant (VPP) [5], which is composed of multiple photovoltaic systems in a radial distribution network. The active power flow across a certain line and voltage of a critical bus are regulated to preferred values, while the active power/reactive power of each photovoltaic system reaches a consensus utilization ratio of its maximal available active/reactive power. The authors in [6] propose a distributed economic dispatch method to adjust the power generation of each DG by collectively estimating the mismatch between power generation and consumption.

Despite the aforementioned advantages, cyber-physical security issue has always been a major concern of distributed decision-making. Due to the lack of a central authority and relatively low security level, an NCS is more susceptible to cyber-attacks than its centralized counterpart. Also, because of the collaborative nature of state update, a simple cyber-attack on a certain agent (refers to DG in this study) can make the NCS deviate from the optimal solution or even unstable [7], [8]. Generally, there are two ways to increase cyber-physical security of an NCS. One way focuses on encryption and protection of data [9], while another way is to design algorithm that is resilient to cyber-attack and communication failure. However, the latter has not yet received enough

Manuscript received September 1, 2015; revised December 20, 2015 and March 6, 2016; accepted March 9, 2016. Date of publication March 25, 2016; date of current version October 19, 2016. The work of Y. Liu, H. Xin, and D. Gan was supported in part by the National Science Foundation of China under Grant 51177146 and Grant 51577168, in part by the National High Technology Research and Development Program of China under Grant 2015AA050202, and in part by the China Scholarship Council under Grant 201406320064. Paper no. TSG-01072-2015.

Y. Liu and H. Xin were with the University of Central Florida, Orlando, FL 32816 USA. They are now with the Department of Electrical Engineering, Zhejiang University, Hangzhou 310027, China (e-mail: yunliu@zju.edu.cn; xinhh@zju.edu.cn).

Z. Qu is with the Department of Electrical and Computer Engineering, University of Central Florida, Orlando, FL 32815 USA (e-mail: qu@ucf.edu).

D. Gan is with the Department of Electrical Engineering, Zhejiang University, Hangzhou 310027, China (e-mail: deqiang.gan@ieee.org).

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

Digital Object Identifier 10.1109/TSG.2016.2542111

attention in application to smart grid. To the best of our knowledge, only [10] proposes a distributed reactive power control strategy that is resilient to packet loss.

Actually, security of NCS based on cooperative control [11] has always been a hot issue in the control systems society. For example, the authors in [12] present a receding-horizon control law, which is resilient to replay attacks (the classification of cyber-attacks will be introduced in Section III). Reference [13] proposes an adversarial robust consensus protocol, based on which convergence of the NCS can be guaranteed whenever the number of adversaries is bounded by a number. A resilient distributed control is proposed in [14], which first suspects potential misbehaving agents and then gradually isolates them from the communication network.

In this paper, an advanced cooperative control strategy of VPP is proposed, which can achieve the objective in [5] and is resilient to various kinds of non-colluding cyber-attacks and possible communication failures. Within this strategy, each DG controller has an estimate of the lower and upper bounds of the states of its in-neighbors through some observation communication links. If the state value received from a certain in-neighbor continuously falls out of the feasible range, that in-neighbor should be gradually isolated from the communication network. Different from the method in [14], this method does not require each DG to estimate the exact state values of its in-neighbors, thus the weights locally stored in each DG are not required to be shared with others, which relieves the burden on communication and preserves information privacy to some extent. The main contributions of the paper are as follows: 1) since the frequently used communication protocols are packet based (e.g., TCP/IP) [15], the continuous-time version of the cooperative control strategy in [5] is reformulated into a discrete-time version, and a strict proof for convergence is also included; 2) it is demonstrated that when the controllers of certain DGs are compromised, e.g., under a replay attack, consensus in utilization ratios of the DGs can be violated, resulting in unfair split of the profit among the DG owners, and a narrower adjustable range of the aggregated VPP power; 3) with the attack-resilient control, the negative effects of the cyber-attacks can be confined to the misbehaving DGs, and all the rest of DGs can still accomplish the objective on condition that the remaining communication network is still connected.

The rest of the paper is organized as follows. Section II presents some preliminary knowledge on graph theory. Section III derives a discrete-time cooperative control strategy of VPP. Section IV studies the possible cyber-attacks on the control strategy, which justifies the significance of the research. The design of attack-resilient cooperative control of VPP is introduced in Section V and some discussions are also included. Simulation results and conclusions are presented in Sections VI and VII, respectively.

II. Preliminaries on Graph Theory

The communication network G that enables cooperative control is described by a triplet (V, E, A), where $V = \{0, 1, \ldots, n\}$ is the index set of agents, $E \subseteq V \times V$ is the set

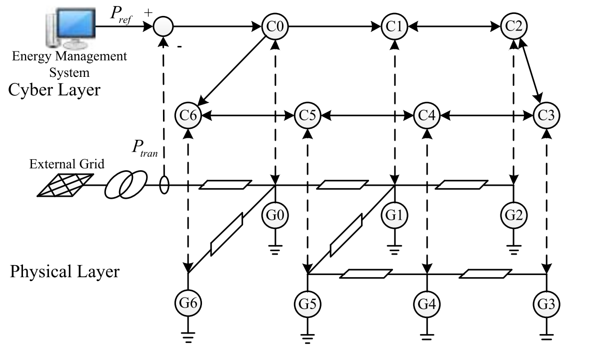

Fig. 1. Diagram of the cooperative control of DGs. Solid arrow denotes communication within the cyber layer and dash arrow denotes communication between the physical and cyber layers.

of communication links, and $A \in \mathrm{R}^{(n+1)\times(n+1)}$ is the weighted adjacency matrix of the graph. Pair $(i, j) \in E$ implies agent j can send information to i. Trivially, a self-loop always exists for every agent, i.e., $(i, i) \in E$. The set of in-neighbors of agent i is defined as $N_i^{\text{in}} = \{j \in V|(i, j) \in E\}$, while the set of its out-neighbors is $N_i^{\text{out}} = \{j \in V|(j, i) \in E\}$. $|\cdot|$ denotes cardinality of the corresponding set. A path from agent i to j is a sequence of successive links $\{(j, k_1), (k_1, k_2), \ldots, (k_l, i)\}$ in E that connects agent i to j. Graph G has a globally reachable node or a spanning tree if there exists an agent from which there is a path to every other agent. Such kind of graph is connected, in which the globally reachable agent is the leader, while the rest of agents are the followers. A matrix is row-stochastic if it is non-negative and each of its row sums up to 1. The weighted adjacency matrix A is defined as

$$[A]_{ij} = \begin{cases} a_{ij} > 0 & \text{if } (i, j) \in E \text{ and } i \neq j \\ 1 - \sum_{j \in N_i^{\text{in}}} a_{ij} > 0 & \text{if } i = j \\ 0 & \text{otherwise} \end{cases},$$

thus it is row-stochastic. Generally, the weights a_{ij} can be chosen freely by the designer according to the connectivity but to satisfy the following assumption.

Assumption 1: The nonzero entries of A are all uniformly lower and upper bounded as $\eta \leq a_{ij} \leq 1$ for all $j \in N_i^{\text{in}}$, where $0 < \eta \leq \min_i \{1/N_i^{\text{in}}\}$.

III. Discrete-Time Cooperative Control of VPP Without Misbehaving DGs

A radial distribution network is typically connected to the transmission grid through a step-up transformer. Such a distribution network can be regarded as a VPP, as shown in Fig. 1. The objective of the cooperative control [5] can be formulated as: make the active power to the transmission network P_{tran} track a reference value P_{ref}, while the utilization ratio of each DG, which is defined as the ratio of its active power output P_i to its maximal available power $P_{i\max}$, converges to a common utilization ratio α^*. The problem can be stated as

$$\min_{P} \quad \left(P_{tran}(\boldsymbol{P}) - P_{ref}\right)^2 \tag{1}$$

$$\text{s.t.} \quad P_0/P_{0\max} = \cdots = P_n/P_{n\max} = \alpha^* \tag{2}$$

$$0 \leq P_i \leq P_{i\max}, \quad \forall i \in V \tag{3}$$

where P_{tran} is a function of the active power outputs of DGs $\boldsymbol{P}=[P_0, \ldots, P_n]^T$ (P_{tran} is positive if the distribution grid injects power to the external grid, otherwise it is negative). $P_{i\max}$ can be estimated using the algorithms in [16] and [17] and thus is assumed available in this paper.

For the power converter of DG i, by applying the d-q transformation so that the d- axis and q-axis voltages are $U_{di} = U_i$ and $U_{qi} = 0$, respectively, the active power output can be calculated as

$$P_i = U_{di}I_{di} + U_{qi}I_{qi} = U_iI_{di}, \tag{4}$$

where I_{di} and I_{qi} are the d- axis and q-axis currents, and U_i is the magnitude of terminal voltage. Reactive power regulation is out of the scope of this work.

If the grid-feeding control scheme [2] is adopted for the control of power converters, I_{di} tracks its reference value I_{di_ref}. I_{di_ref} is updated in a period of T, which should be long enough to guarantee that I_{di} converges to I_{di_ref} at the end of each period, i.e., $I_{di}^{(k)} = I_{di\_ref}^{(k)}$ with k denoting the iteration number. In the kth iteration, $I_{di\_ref}^{(k)}$ can be designed as

$$I_{di\_ref}^{(k)} = P_{i\max}\alpha_i^{(k)}/U_i^{(k)}, \tag{5}$$

where $\alpha_i^{(k)} \in [0, 1]$ is the utilization ratio of DG i to be determined. When I_{di} converges to I_{di_ref} at the end of the kth iteration, $P_i^{(k)} = P_{i\max}\alpha_i^{(k)}$.

The utilization ratio $\alpha_i^{(k)}$ evolves according to the discrete-time leader-following consensus algorithm [11]. The leader agent should have access to the information of $P_{ref}^{(k)}$ and $P_{tran}^{(k)}$. In principle, the leader would simply be the controller at the substation but could alternatively be any DGs in the NCS. Nevertheless, it is preferred that the substation is the leader due to its easy access to P_{tran} and high information security level. In addition, for the sake of information privacy, global information like P_{tran} is preferred not to be revealed to the customers' DGs. Without loss of generality, DG 0 is selected as the leader. Its utilization is updated as

$$\alpha_0^{(k+1)} = \min\left\{\max\left\{\alpha_0^{(k)} + k_p\left[P_{ref} - P_{tran}^{(k)}\right], 0\right\}, 1\right\} \tag{6}$$

where $k_p > 0$ is a sufficiently small control gain. $\alpha_0^{(k)}$ is contained within [0, 1] so that it is attainable.

For the followers, their utilization ratios can be designed to be the weighted sum of the utilization ratios from their in-neighbors, i.e.,

$$\alpha_i^{(k+1)} = \sum_{j=0}^{n} a_{ij}^{(k)}\alpha_j^{(k)}, \quad \forall i \in \{1, \ldots, n\}, \tag{7}$$

where $a_{ij}^{(k)}$ is the corresponding entry in matrix A at the kth iteration.

Due to active power balance within the feeder, $P_{tran}^{(k)}$ can be calculated as

$$P_{tran}^{(k)} = \sum_{i=0}^{n} P_{i\max}\alpha_i^{(k)} - P_{load} - P_{loss}, \tag{8}$$

where P_{load} is the aggregated load power consumption and P_{loss} is the distribution power loss.

In practice, P_{load} is time-variant. In respect of convergence property however, P_{tran} converging to P_{ref} under a fixed P_{load} and P_{tran} tracking P_{ref} under a time-variant P_{load} is similar. Therefore, it is justified to prove the former. P_{loss} can be calculated as [18]

$$P_{loss} = \sum_{i=1}^{N-1}\sum_{j=i+1}^{N} G_{ij}\left(V_i - V_j\right)^2,$$

where G_{ij} is the conductance of power line between bus i and bus j, V_i is the voltage magnitude of bus i, and N is the total number of buses in the network. In practice, the variation of voltages at different locations of a distribution network should be maintained within a limited range so that power quality is satisfactory enough. With the introduction of DGs in distribution networks, an almost unified voltage profile can be achieved through reactive power dispatch [18]. Therefore, it follows from the expression of P_{loss} that its value is nearly a constant, which is also demonstrated by the simulations in [18].

Without considering constraint (3) (when the constraint is active, convergence of the NCS directly follows from Theorem 5.4 [11]), the dynamics of NCS can be written in a compact form as

$$0\begin{bmatrix} \alpha_0^{(k+1)} \\ \boldsymbol{\alpha}^{(k+1)} \end{bmatrix} = \begin{bmatrix} 1 - k_pP_{0\max} & -k_p\tilde{\boldsymbol{P}}_{\max}^T \\ A_1 & A_2 \end{bmatrix}\begin{bmatrix} \alpha_0^{(k)} \\ \boldsymbol{\alpha}^{(k)} \end{bmatrix} + \begin{bmatrix} k_p\left(P_{ref} + P_{load} + P_{loss}\right) \\ 0_{n\times 1} \end{bmatrix} = A_\Delta\begin{bmatrix} \alpha_0^{(k)} \\ \boldsymbol{\alpha}^{(k)} \end{bmatrix} + \boldsymbol{b}, \tag{9}$$

where $\boldsymbol{\alpha}^{(k)} = [\alpha_1^{(k)}, \ldots, \alpha_n^{(k)}]^T$, $\tilde{\boldsymbol{P}}_{\max} = [P_{1\max}, \ldots, P_{n\max}]^T$. $A_\Delta = \begin{bmatrix} 1 - k_pP_{0\max} & -k_p\tilde{\boldsymbol{P}}_{\max}^T \\ A_1 & A_2 \end{bmatrix}$ is the system matrix with $\begin{bmatrix} A_1 & A_2 \end{bmatrix} \in \mathrm{R}^{n\times(n+1)}$ being the last n rows of matrix A; $\boldsymbol{b} = \begin{bmatrix} k_p\left(P_{ref} + P_{load} + P_{loss}\right) \\ 0_{n\times 1} \end{bmatrix}$ can be regarded as a constant vector; $0_{n\times m} \in \mathrm{R}^{n\times m}$ is an all-zero matrix.

The convergence property of the discrete-time cooperative control (9) can be summarized as

Theorem 1: The cooperative control laws (5)-(7) guarantee that the DGs can asymptotically converge to the optimal solution of (1)-(3) provided that the communication network is connected.

The proof is presented in the Appendix. Note that the convergence only depends on the topology of the communication network, thus the cooperative control is robust to feeder reconfiguration.

IV. Cyber-Attacks Against Cooperative Control of VPP

When a cyber-attack is launched on a certain DG controller/communication link, it will result in the loss of information integrity or availability and consequently could fail the control objective for that DG and, if the failure propagates, for the overall system. Information availability ensures timely access to the data or functionalities, while information integrity indicates that there is no unauthorized change of information [19]. Generally, cyber-attacks can be categorized as denial-of-service (DoS) and deceptive attacks, which corrupt information availability and integrity, respectively. A DoS attack means the control command sent from a certain DG are erased, while a deceptive attack means an attacker intentionally modifies the control command in an elaborate way. Replay attacks and stealthy attacks are two particular kinds of deceptive attacks, where replay attacks make a DG controller repeatedly send the same information to its out-neighbors, while stealthy attacks can stay undetected by the monitoring system.

In this section, replay attacks are used to demonstrate the severity of cyber-attacks. Without loss of generality, let $\boldsymbol{\alpha}_M^{(k)} \equiv \boldsymbol{\alpha}_M = [\alpha_1, \ldots, \alpha_r]^T$ and $\boldsymbol{\alpha}_W^{(k)} = [\alpha_{r+1}^{(k)}, \ldots, \alpha_n^{(k)}]^T$ be the utilization ratio vectors of misbehaving and well-behaving DGs, respectively, where r is the number of misbehaving DGs.

The dynamics of the NCS can be expressed as

$$\begin{bmatrix} \alpha_0^{(k+1)} \\ \boldsymbol{\alpha}_M^{(k+1)} \\ \boldsymbol{\alpha}_W^{(k+1)} \end{bmatrix} = \begin{bmatrix} 1 - k_p P_{0\max} & -k_p \boldsymbol{P}_{M\max}^T & -k_p \boldsymbol{P}_{W\max}^T \\ 0_{r\times 1} & I_r & 0_{r\times(n-r)} \\ A_0 & A_M & A_W \end{bmatrix} \times \begin{bmatrix} \alpha_0^{(k)} \\ \boldsymbol{\alpha}_M^{(k)} \\ \boldsymbol{\alpha}_W^{(k)} \end{bmatrix} + \begin{bmatrix} k_p\left(P_{ref} + P_{load} + P_{loss}\right) \\ 0_{r\times 1} \\ 0_{(n-r)\times 1} \end{bmatrix}, \tag{10}$$

where $I_r \in \mathrm{R}^{r\times r}$ is the identity matrix, $\begin{bmatrix} A_0 & A_M & A_W \end{bmatrix}$ is the same as the last n-r rows of matrix A, $\boldsymbol{P}_{M\max} = [P_{1\max}, \ldots, P_{r\max}]^T$, and $\boldsymbol{P}_{W\max} = [P_{(r+1)\max}, \ldots, P_{n\max}]^T$.

The following lemma summarizes the property of NCS under replay attacks.

Lemma 1: Suppose that the communication network remains connected during the attack. The NCS in (10) converges to a stable point $[\alpha_0^*, (\boldsymbol{\alpha}_M^*)^T, (\boldsymbol{\alpha}_W^*)^T]^T$, which satisfies

$$\alpha_0^* = \min\{\max\{\tilde{\alpha}_0, 0\}, 1\}, \tag{11}$$

$$\boldsymbol{\alpha}_M^* = \boldsymbol{\alpha}_M, \boldsymbol{\alpha}_W^* = (I_{n-r} - A_W)^{-1}\begin{bmatrix} A_0 & A_M \end{bmatrix}\begin{bmatrix} \alpha_0^* \\ \boldsymbol{\alpha}_M \end{bmatrix}, \tag{12}$$

where $\tilde{\alpha}_0 = \frac{1}{P_{0\max}}(P_{ref}+P_{load}+P_{loss}-\boldsymbol{P}_{M\max}^T\boldsymbol{\alpha}_M-\boldsymbol{P}_{W\max}^T\boldsymbol{\alpha}_W^*)$.

In other words, the utilization ratios of the well-behaving DGs converge to the space spanned by $[\alpha_0^*, \boldsymbol{\alpha}_M^T]^T$, i.e., no consensus can be reached among the DGs.

The proof is presented in the Appendix.

Lemma 1 explains partly the incentives for carrying out a cyber-attack: when DG i deliberately increases its α_i, the other DGs converge to smaller utilization ratios. This generally brings more economic benefit to the misbehaving DG since it can generate more electricity while decrease the incomes of other DGs since they have to generate less to maintain P_{tran} to P_{ref}. Moreover, if one of the follower DG in the network is compromised so that it can randomly set its utilization ratio, this DG can maliciously make the adjustable range of P_{tran} narrow and weaken controllability of the VPP. It should be noted that the effect of a misbehaving DG on the aggregated power output of DGs $P_{aggr} = \sum_{i=0}^{n} P_i$ is mainly influenced by the topology of communication network and the corresponding adjacency matrix A. Specifically, it can be inferred

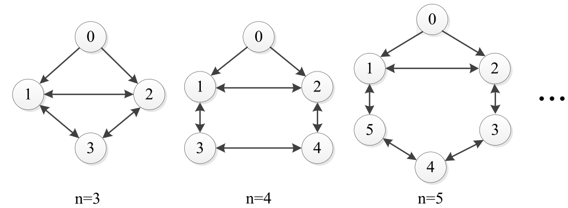

Fig. 2. Connected communication networks with different number of followers.

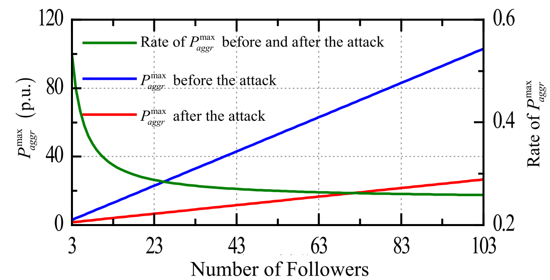

Fig. 3. $P_{aggr}^{\max}$ before and after cyber-attack on DG 1 ($\alpha_1^{(k)} \equiv 0$) with different NCS size from $n = 3$ to $n = 103$.

from (12) that a misbehaving DG has more negative effects on the NCS if it is connected to more well-behaving DGs and these DGs put more weights on the misbehaving one in the state update (7). In addition, the following example illustrates that the adjustable range of P_{aggr} can narrow more in a large-scale NCS due to possible cyber-attacks.

Consider an NCS with n followers (DGs 1 to n) which form a loop with bidirectional communication links while DG 0 (leader) directly communicates with DGs 1 and 2, as is shown in Fig. 2 for $n = 3, 4, 5$. The weights in the adjacency matrix is evenly split among the in-neighbors, i.e., $a_{ij} = 1/|N_i^{\text{in}}|$ if $j \in N_i^{\text{in}}$ and $a_{ij} = 0$ if otherwise. Assume the maximal available power of each DG is 1 p.u. Without any cyber-attack, P_{aggr} can vary from 0 to n+1 as the consensus utilization ratio α^* increases from 0 to 1, thus the maximum of P_{aggr} is $P_{aggr}^{\max} = n + 1$. However, if DG 1 misbehaves by deliberately setting $\alpha_1^{(k)} \equiv 0$, $P_{aggr}^{\max}$ decreases. The result is illustrated in Fig. 3 with different scales of NCS, which indicates that $P_{aggr}^{\max}$ is decreased by 45% when $n = 3$, while it is decreased by 75% when $n = 103$.

V. Observer Based Attack-Resilient Cooperative Control of VPP

In this section, an advanced cooperative control of VPP is proposed, which is resilient to the aforementioned cyber-attacks. Within this strategy, utilization ratios of leader and follower DGs still evolve according to (6) and (7), respectively. A distributed confidence level manager (DCLM) at each follower DG controller maintains a confidence level for each of its in-neighbors. Each DG estimates the feasible utilization ratio ranges of its in-neighbors. When a DG detects that the actual utilization ratio from a certain in-neighbor falls out of the feasible range, the DCLM decreases its confidence level, and its weight in the adjacency matrix decreases correspondingly. Consequently, the misbehaving DG is gradually marginalized

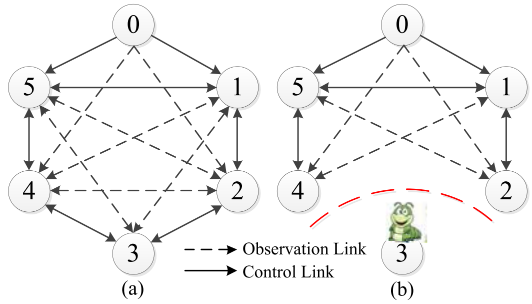

Fig. 4. Diagrams of the communication network with control and observation links (an observation link is denoted as a solid arrow if it coincides with a control link): (a) A connected communication network; (b) The network after DG 3 is isolated due to cyber-attack.

and finally isolated from the communication network, thus it cannot influence consensus of the well-behaving DGs if the remaining communication network is still connected.

It should be noted that multicast communication is generally adopted in distributed systems [15]. In this case, every DG controller always sends the same information to all its out-neighbors. Also, it can be guaranteed that the leader DG will never be compromised by means of some security methods, for example, implementing a local observer to monitor the information from the leader DG, or adopting the advanced encryption standard, etc.

A. Communication Topology Design

Detection of the misbehaving DGs comes at the expense of a redundant communication network. Specifically, the communication network can be divided into two subgraphs: the control subgraph and the observation subgraph, as illustrated in Fig. 4. It is possible that some control links overlap observation links.

The control subgraph is designed first, which mainly engages in the state update according to equations (6) and (7). The minimum requirement for the topology of the control subgraph is that it should be connected [11]. The higher its connectivity is, the faster the convergence speed is. In the rest of the paper, N_i^{in} and N_i^{out} are specifically used to indicate the in-neighbor and out-neighbor sets of DG i in the control subgraph to simplify the explanation.

Based on the control subgraph, the observation subgraph can be determined, whose responsibility is to estimate the upper and lower bounds of the utilization ratio of every in-neighboring DG. The information of the observation subgraph actually does not engage in the state update, but serves for surveillance purpose only. To this end, the topology of the observation subgraph is defined as

$$E' = \left\{ (i,j) | \forall j \in N_k^{\text{in}}, \forall i \in N_k^{\text{out}}, \forall k \in V \right\}, \tag{13}$$

i.e., for DG $k \in V$, any of its in-neighbors can communicate to any of its out-neighbors.

B. Detection of Cyber-Attacks

For any DG $i \in N_k^{\text{out}}$, it can estimate the feasible utilization ratio range of DG k with the information from the observation links provided that it can recognize set N_k^{in}. One way is that the controller of DG k should pack its utilization ratio together with the indices of N_k^{in} in the data packet and send the packet to any DG $i \in N_k^{\text{out}}$.

Consider Assumption 1 and the control law (7), any DG $i \in \{1, \ldots, n\}$ can always estimate the upper and lower bounds of the utilization ratio of its in-neighbor j in the next iteration with the information from the observation subgraph as

$$\alpha_{j\text{up}}^{(k+1)} = \eta \sum_{l \in N_j^{\text{in}} - S_j^{\max}} \alpha_l^{(k)} + \left[1 - \eta\left(\left|N_j^{\text{in}}\right| - \left|S_j^{\max}\right|\right)\right]\alpha_{j\max}^{(k)}, \tag{14}$$

$$\alpha_{j\text{low}}^{(k+1)} = \eta \sum_{l \in N_j^{\text{in}} - S_j^{\min}} \alpha_l^{(k)} + \left[1 - \eta\left(\left|N_j^{\text{in}}\right| - \left|S_j^{\min}\right|\right)\right]\alpha_{j\min}^{(k)}, \tag{15}$$

where η is the lower bound of positive entries in A as defined in Assumption 1; $\alpha_{j\max}^{(k)}$ and $\alpha_{j\min}^{(k)}$ are defined as

$$\alpha_{j\max}^{(k)} = \max\left\{\alpha_l^{(k)} \middle| \forall l \in N_j^{\text{in}}\right\}, \alpha_{j\min}^{(k)} = \min\left\{\alpha_l^{(k)} \middle| \forall l \in N_j^{\text{in}}\right\};$$

$S_{j\max}^{(k)}$ and $S_{j\min}^{(k)}$ are defined as

$$S_{j\max}^{(k)} = \left\{ l | l \in N_j^{\text{in}}, \alpha_l^{(k)} = \alpha_{j\max}^{(k)} \right\},$$
$$S_{j\min}^{(k)} = \left\{ l | l \in N_j^{\text{in}}, \alpha_l^{(k)} = \alpha_{j\min}^{(k)} \right\}.$$

If the following inequality holds

$$\alpha_{j\text{low}}^{(k)} \leq \alpha_j^{(k)} \leq \alpha_{j\text{up}}^{(k)}, \tag{16}$$

DG i considers its in-neighboring DG j to be well-behaving, where $\alpha_j^{(k)}$ is the utilization ratio received by DG i from DG j. On the contrary, if DG i does not receive information from DG j (denoted as $\alpha_j^{(k)}$ =n/a) or $\alpha_j^{(k)}$ is not within the feasible range in (16), DG j is considered to be suspicious, and the marginalization and isolation process will be activated.

It is worth noting that neighboring DGs may collude with each other to avoid from being detected by the monitoring scheme. Such kind of colluding attack happens when DG j maliciously modifies its information to others and its out-neighbors does not marginalize and isolate it on purpose. Fortunately, this kind of attack is relatively difficult to launch since it requires multiple DGs to be compromised simultaneously. How to detect a colluding attack can be the direction of our future work.

C. Marginalization and Isolation of Suspicious DGs

Motivated by [14], a DCLM is established locally for every follower DG controller. The DCLM maintains a confidence level $c_{ij}^{(k)}$ for each of its in-neighboring DG $j \in N_i^{\text{in}}$, which is initially assigned a certain integer value $c_{ij}^{(0)} = C_{ij}^0 > 0$. In every iteration, $c_{ij}^{(k)}$ evolves as

$$c_{ij}^{(k+1)} = \begin{cases} \max\left\{c_{ij}^{(k)} - 1, 0\right\} & \text{if DG } j \text{ is suspicious} \\ c_{ij}^{(k)} & \text{otherwise.} \end{cases} \tag{17}$$

When the confidence level of a certain in-neighboring DG decreases, the probability that it is misbehaving increases.

Algorithm 1: $\tilde{c}_i^{(k)}$ Calculation (DG i)

Input: $c_{ij}^{(k)}, \forall j \in N_i^{\text{in}}$

Sort $\{c_{ij}^{(k)} \big| \forall j \in N_i^{\text{in}}$ and $\alpha_j^{(k)} \neq \text{n/a}\}$ in ascending order as $\xi_{i1}^{(k)} \leq \cdots \leq \xi_{im}^{(k)}$, where $m = \left|\left\{ j | \forall j \in N_i^{\text{in}} \text{ and } \alpha_j^{(k)} \neq \text{n/a} \right\}\right|$

If $\frac{\xi_{i1}^{(k)}}{\sum_{l=1}^{m} \xi_{il}^{(k)}} \geq \eta$

  Output: $\tilde{c}_i^{(k)} = 0$

  Break;

Else

  For $(j = 2; j \leq m; j = j + 1)$

    If $\frac{\xi_{i(j-1)}^{(k)}}{\sum_{l=j-1}^{m} \xi_{il}^{(k)}} < \eta$ and $\frac{\xi_{ij}^{(k)}}{\sum_{l=j}^{m} \xi_{il}^{(k)}} \geq \eta$ (19)

      Output: $\tilde{c}_i^{(k)} = \xi_{ij}^{(k)}$

      Break;

Thus, the corresponding DG should be gradually marginalized from the communication network to decrease its influence on other DGs. To achieve this, its corresponding weight in $A^{(k)}$ can be updated in a distributed manner as

$$a_{ij}^{(k)} = \begin{cases} \dfrac{\left[c_{ij}^{(k)}\right]^+_{\tilde{c}_i^{(k)}}}{\sum_{l \in N_i^{\text{in}}, \alpha_l^{(k)} \neq \text{n/a}} \left[c_{il}^{(k)}\right]^+_{\tilde{c}_i^{(k)}}} & \text{if } \alpha_j^{(k)} \neq \text{n/a} \\ 0 & \text{otherwise,} \end{cases} \tag{18}$$

where $\tilde{c}_i^{(k)}$ is the threshold of $c_{ij}^{(k)}$ and is determined by Algorithm 1 in each iteration. Function $[x]_y^+$ is defined as

$$[x]_y^+ = \begin{cases} x & \text{if } x \geq y \\ 0 & \text{otherwise.} \end{cases}$$

Equation (18) always maintains $A^{(k)}$ to be row-stochastic. Moreover, if $c_{ij}^{(k)}$ decreases, $a_{ij}^{(k)}$ decreases correspondingly. When $c_{ij}^{(k)} < \tilde{c}_i^{(k)}$, $a_{ij}^{(k)}$ is directly set to zero, which indicates that DG j is confirmed to be misbehaving and is no longer subscribed by DG i. When a misbehaving DG is isolated from the communication network, all the communication links relevant to it are removed, as exemplified in Fig. 4. Algorithm 1 is used to find a suitable threshold value for $c_{ij}^{(k)}$ in (18) so that $a_{ij}^{(k)} \geq \eta$ if it is positive; or $a_{ij}^{(k)} = 0$ if otherwise. The logic is as follows.

When $\frac{\xi_{i1}^{(k)}}{\sum_{l=1}^{m} \xi_{il}^{(k)}} \geq \eta$, it follows from (18) by considering $\tilde{c}_i^{(k)} = 0$ that $a_{ij}^{(k)} \geq \eta$ for all $j \in N_i^{\text{in}}$ and $\alpha_j^{(k)} \neq \text{n/a}$, and $a_{ij}^{(k)} = 0$ if otherwise. When $\frac{\xi_{i1}^{(k)}}{\sum_{l=1}^{m} \xi_{il}^{(k)}} < \eta$, it can be shown that $\tilde{c}_i^{(k)} = \xi_{il}^{(k)}$ satisfying (19) is the best threshold value. Firstly, it follows from (18) that $a_{ij}^{(k)} = 0$ is satisfied for all $c_{ij}^{(k)} < \tilde{c}_i^{(k)}$ and from the second part of (19) that $a_{ij}^{(k)} \geq \eta$ for all $c_{ij}^{(k)} \geq \tilde{c}_i^{(k)}$. Secondly, $\tilde{c}_i^{(k)} = \xi_{il}^{(k)}$ is better than other options. On one hand, if $\tilde{c}_i^{(k)} \leq \xi_{i(l-1)}^{(k)}$, the first part of (19) implies that $a_{ij}^{(k)}$ corresponding to $c_{ij}^{(k)} = \xi_{i(l-1)}^{(k)}$ leads to $0 < a_{ij}^{(k)} < \eta$, which is contradictory to $\eta \leq a_{ij}^{(k)} < 1$ in Assumption 1. On the other hand, if $\tilde{c}_i^{(k)} \geq \xi_{i(l+1)}^{(k)}$, communication corresponding to $c_{ij}^{(k)} = \xi_{il}^{(k)}$ is isolated, which results in a lower connectivity. Therefore, $\tilde{c}_i^{(k)} = \xi_{il}^{(k)}$ is the best threshold value.

In addition, three remarks are given on the marginalization and isolation process.

1) When a DoS attack or a packet loss happens to certain control links, e.g., link $(i, j) \in E$, DG i treats this link as if it does not exist by setting $a_{ij}^{(k)} = 0$ in the corresponding iteration, and row stochasticity of $A^{(k)}$ is always maintained.

2) In the presence of misbehaving DGs violating (16), the time for them to be isolated is determined by both the attacks and the parameters of the attack-resilient algorithm. Generally, a misbehaving DG j can be isolated more quickly if its out-neighbor's confidence level on it, i.e., $C_{ij}^0 (\forall i \in N_j^{\text{out}})$, is relatively small and the lower bound of positive weight η is relatively large.

3) Without any misbehaving DGs, the convergence rate of the algorithm is determined by the algebraic connectivity defined as [20]

$$\phi = \sqrt{(1 - |\lambda_2| \cos \theta_2)^2 + |\lambda_2|^2 \sin^2 \theta_2},$$

where $\lambda_2 = |\lambda_2| \angle \theta_2$ is the second largest eigenvalue of the adjacency matrix $A^{(k)}$ in magnitude. A higher algebraic connectivity implies a faster convergence rate. There are two ways to improve the value of ϕ: i) adding a communication link to the control subgraph at the expense of communication [21] and ii) initially optimizing the weights in A, which is sensitive to the corresponding confidence levels as indicated by equation (18).

D. Robustness to Packet Loss

Packet loss is inevitable in an NCS. Success of communication $(i, j) \in E$ at the kth iteration can be modeled in a probabilistic manner as [10]

$$\Pr\left\{x_{ij}^{(k)} = m\right\} = \begin{cases} 1 - r_{loss} & \text{if } m = 1 \\ r_{loss} & \text{if } m = 0 \end{cases}, \tag{19}$$

where $x_{ij}^{(k)} = 1$ means no packet loss happens to link (i, j) and $x_{ij}^{(k)} = 0$ if otherwise; r_{loss} is the packet loss rate.

When packet loss happens occasionally to link $(i, j) \in E$, $c_{ij}^{(k)}$ can also decrease and eventually, the connected network will disassemble even without any cyber-attacks. To avoid this, a confidence level regain process is executed in each iteration as

$$\Pr\left\{c_{ij}^{(k)} = m\right\} = \begin{cases} r_{gain} & \text{if } m = \min\left\{c_{ij}^{(k)} + 1, C_{ij}^0\right\} \\ 1 - r_{gain} & \text{if } m = c_{ij}^{(k)}, \end{cases} \tag{20}$$

where r_{gain} is the confidence level regain rate. As long as $r_{gain} > r_{loss}$, $\Pr\{c_{ij}^{(k)} = C_{ij}^0\} = 1$ for all the well-behaving DG j.

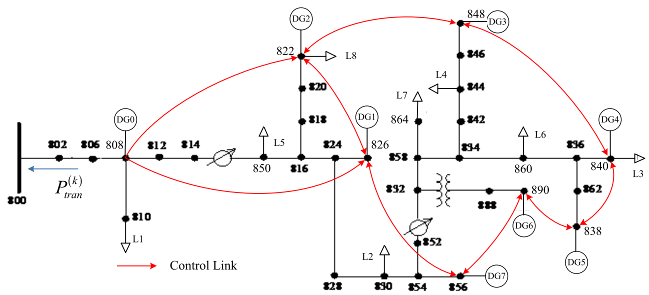

Fig. 5. Diagram of the IEEE 34-bus test feeder.

Thus, the proposed approach is also resilient to packet loss. It is worth mentioning that r_{loss} is generally small in practice (less than 5%), and a cyber-attack needs to be more frequently launched if it aims to disrupt the NCS. Therefore, the confidence level regain process cannot significantly influence the detection and isolation of misbehaving DGs.

E. Main Result

The convergence property of the proposed cooperative control strategy can be summarized as

Theorem 2: The proposed cooperative control strategy is resilient to non-colluding attacks. By isolating the DGs that violate (16), the remaining DGs can together accomplish the control objective in (1)-(3) provided that the remaining communication network is still connected.

The proof is presented in the Appendix.

It is worth noting that stealthy attacks can be launched by not violating (16). However, it is shown in the proof and by simulation that the control objective can still be accomplished only at the expense of slower convergence. It is also possible that a misbehaving agent j misreports its true in-neighbor set N_j^{in} to its out-neighbors as $\tilde{N}_j^{\text{in}} \neq N_j^{\text{in}}$. If $\tilde{N}_j^{\text{in}}$ includes any misbehaving DG, it falls into the category of colluding attack thus the misbehaving DGs stay undetected. Otherwise, $\alpha_{j\text{up}}^{(k+1)}$ and $\alpha_{j\text{low}}^{(k+1)}$ can be calculated by all its out-neighbors based on the misreported $\tilde{N}_j^{\text{in}}$ according to (14) and (15). If $\alpha_j^{(k+1)}$ from agent j falls out of this interval, agent j will be gradually isolated by its out-neighbors as in Case 1) of the proof, otherwise it follows from Case 2) of the proof that the control objective can still be accomplished.

VI. Case Studies

To validate the effectiveness of the attack-resilient cooperative control of VPP, numerical simulations are performed on the IEEE 34-bus test feeder, as shown in Fig. 5. It is connected to a transmission network with a step-up transformer at bus 800. Thus the power flow across line 802-800 is expected to be regulated to P_{ref}. The detailed parameters of the network can be found in [22]. Eight DGs (DGs 0-7) and eight loads (L1-L8) are connected to the feeder from different locations. The maximal available power of DG $i \in \{0, \dots, 7\}$ is 0.5 MW. Each load is modeled as 50% constant power and 50% constant impedance, with power consumption of

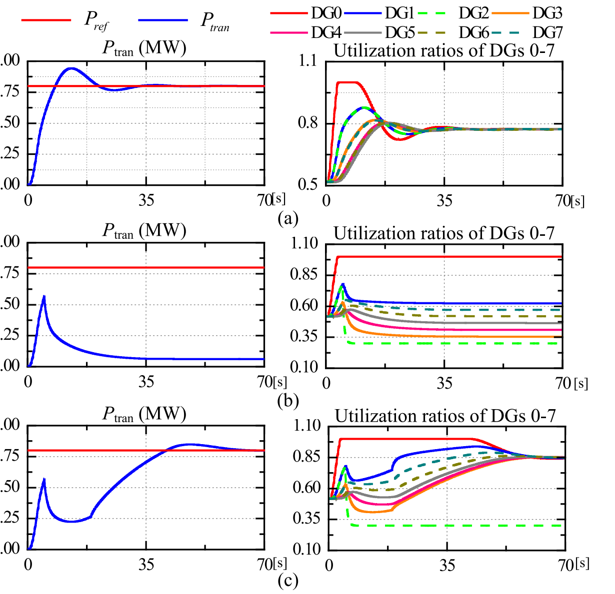

Fig. 6. Responses of the non-resilient/resilient cooperative control system with/without replay attack on DG 2: (a) Non-resilient cooperative control without replay attack, (b) Non-resilient cooperative control and (c) resilient cooperative control when DG 2 is under replay attack.

0.2 MW + 0.1 Mvar. In the attack-resilient cooperative control, the initial confidence level of each link is set to 50, thus the adjacency matrix can be initialized correspondingly according to (18). The lower bound of non-zero weight is $\eta = 0.1$ without otherwise stated. The constant gain of DG 0 is $k_p = 0.1$. The sampling period is set to $T = 0.5$ s.

A. Response of the VPP Under Replay Attack

Initially, the utilization ratio of each DG is 0.5, and the corresponding $P_{tran}^{(0)} = 0$ MW. Packet loss is not considered in this case. At $t = 0$ s, P_{ref} is set to 0.8 MW. Fig. 6 compares responses of the non-resilient/resilient cooperative control system with/without replay attack on DG 2. Fig. 6(a) shows the response of a non-resilient cooperative control system without a replay attack, which indicates that P_{tran} can track its reference value P_{ref} in about 30 s. In Fig. 6(b) and (c), a replay attack is launched on DG 2 at $t = 5$ s, which maliciously repeats $\alpha_2^{(k)} \equiv 0.3$ so as to bias the utilization ratios of other DGs. With non-resilient cooperative control [Fig. 6(b)], the utilization ratios of all the follower DGs converge to values between $\alpha_2^{(k)}$ and $\alpha_0^{(k)}$ without reaching a consensus. Also, P_{tran} fails to track P_{ref} even when $\alpha_0^{(k)}$ reaches 1 because the other DGs cannot fully utilize their capacities. In comparison, with the attack-resilient cooperative control [Fig. 6(c)], it takes about 12 s for the NCS to detect and isolate the misbehaving DG. Consequently, the well-behaving DGs can still reach a consensus. Since the misbehaving DG only has a trivial influence on the adjustable range of P_{tran}, P_{tran} successfully tracks P_{ref}. Note that it takes a longer time (about 60 s) for the well-behaving DGs to reach consensus. This is because before DG 2 is completely isolated, it prevents the follower DGs from tracking $\alpha_0^{(k)}$, and after its isolation, the

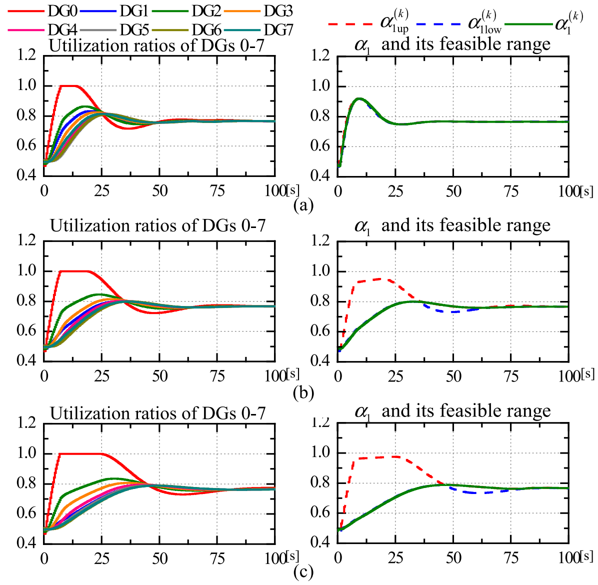

Fig. 7. Response of the VPP when DG 1 is under stealthy attack: (a) $\eta = 0.2$; (b) $\eta = 0.1$; (c) $\eta = 0.05$

connectivity of the corresponding network decreases, which also contributes to the slow convergence rate [21].

B. Response of the VPP Under Stealthy Deceptive Attack

Simulation is performed under the same initial condition as in Section VI-A. At $t = 5$ s, a stealthy attack is launched on DG 1. Intuitively, to disrupt the convergence, the attacker of DG 1 should intentionally prevent $\alpha_1^{(k)}$ from converging to $\alpha_0^{(k)}$, i.e.,

$$\alpha_1^{(k+1)} = \begin{cases} \alpha_{1\text{low}}^{(k+1)} & \text{if } \sum_{j=0}^{n} a_{1j}^{(k)} \alpha_j^{(k)} \geq \alpha_1^{(k)} \\ \alpha_{1\text{up}}^{(k+1)} & \text{otherwise.} \end{cases} \tag{21}$$

Fig. 7 compares the system responses under different η. As can be seen in the figure, equation (16) is always satisfied thus DG 1 is never suspected throughout the process. In comparison with the response of NCS without any attacks [Fig. 6(a)], the convergence rate is decreased to some extent, and it decreases even more when η is small. Specifically, the convergence time is 50 s, 63 s, and 75 s when η=0.2, 0.1 and 0.05, respectively. The reason is that as η decreases, $\alpha_{1\text{up}}^{(k)} - \alpha_{1\text{low}}^{(k)}$ increases, thus the attacker is able to adjust $\alpha_1^{(k)}$ in a wider range.

C. Response of the VPP in the Presence of Packet Loss

In this case study, the influence of packet loss is investigated. The initial condition is the same as the previous case. At $t = 60$ s, P_{ref} is changed to 0.2 MW. To highlight the effectiveness of the confidence level regain process, a rather high packet loss rate $r_{loss} = 0.2$ is selected. Fig. 8 compares the system responses with/without the confidence level regain process. Without it, the weights of $A^{(k)}$ corresponding to all the in-neighbors of each DG except itself gradually decrease to zero due to the decrease in $c_{ij}^{(k)}$. Consequently, the NCS disassembles, and no consensus in the utilization ratios can

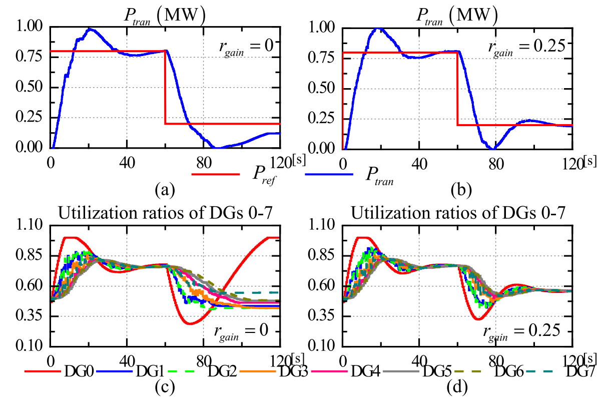

Fig. 8. Response of the VPP with the attack-resilient cooperative control ($r_{gain} = 0$ and 0.25) in the presence of packet loss: (a-b) Power flow across the transmission line (MW); (c-d) Utilization ratios of the DGs.

be reached [as shown in Fig. 8(c)]. With the confidence level regain process ($r_{gain} = 0.25$), $a_{ij}^{(k)}$ ($\forall j \in N_i^{\text{in}}$ and $\alpha_j^{(k)} \neq$ n/a) remain positive despite some fluctuation can be observed, thus the NCS remains connected and the utilization ratios finally reach a consensus value [as shown in Fig. 8(d)].

VII. Conclusion

In this paper, an attack-resilient cooperative control strategy is proposed to regulate the active power of a virtual power plant at a specific dispatch command, while maintain the utilization ratios of DGs at a consensus. With a properly designed observation subgraph, each DG can estimate the feasible utilization ratio ranges of all its in-neighbors. An in-neighbor is suspected to be misbehaving if its actual utilization ratio falls out of the feasible range. A distributed confidence level manager at each DG controller maintains confidence levels for all of its in-neighbors. The confidence level of a certain in-neighbor decreases if it is suspected. Consequently, the misbehaving in-neighbors are gradually isolated from the network. The proposed strategy is resilient to communication failure as well as various kinds of non-colluding cyber-attacks, e.g., DoS attacks and deceptive attacks. In the presence of such cyber-attacks, the well-behaving DGs can still accomplish the control objective without being misled by the misbehaving ones, which is verified through simulations of the IEEE standard 34-bus test feeder.

Appendix

Proof of Theorem 1: The system matrix of (9) is $A_\Delta = A + k_p\Delta$, which can be viewed as the adjacency matrix $A = \begin{bmatrix} 1 & 0_{1\times n} \\ A_1 & A_2 \end{bmatrix}$ perturbed via the term $k_p\Delta = k_p\begin{bmatrix} -P_{0\max} & -\tilde{\boldsymbol{P}}_{\max}^T \\ 0_{n\times 1} & 0_{n\times n} \end{bmatrix}$. The connectivity of the communication network implies that the spectrum radius of A is 1, which is also a simple eigenvalue $\lambda_1 = 1$. The rest of eigenvalues are within the open unit disk. The left and right eigenvectors corresponding to λ_1 are $\boldsymbol{\nu} = [1, 0, \ldots, 0]^T$ and $\boldsymbol{\mu} = [1, \ldots, 1]^T$, respectively. It follows from Lemma 7 in [23] that when k_p

is sufficiently small, the perturbation on λ_1 is quantified by $\boldsymbol{\nu}^T\Delta\boldsymbol{\mu} = -\sum_{i=0}^{n} P_{i\max} < 0$, thus $0<\lambda_1<1$. In addition, due to the continuity of the eigenvalues, the rest of them remain in the open unit disk when k_p is small enough. Therefore, we conclude that system (9) is asymptotically stable.

Moreover, it can be verified via steady-state analysis that

$$\alpha^* = \lim_{k\to\infty} \alpha_i^{(k)} = \min\left\{\max\left\{\frac{P_{ref} + P_{load} + P_{loss}}{\sum_{j=0}^{n} P_{j\max}}, 0\right\}, 1\right\}. \tag{22}$$

Therefore, the control objective is achieved.

Proof of Lemma 1: The stability of (10) can be characterized by the system matrix $\tilde{A}_\Delta = \tilde{A} + k_p\Delta$, where

$$\tilde{A} = \begin{bmatrix} 1 & 0_{1\times r} & 0_{1\times(n-r)} \\ 0_{r\times 1} & I_r & 0_{r\times(n-r)} \\ A_0 & A_M & A_W \end{bmatrix} \text{ and}$$
$$\Delta = -\begin{bmatrix} P_{0\max} & \boldsymbol{P}_{M\max}^T & \boldsymbol{P}_{W\max}^T \\ 0_{n\times 1} & 0_{n\times r} & 0_{n\times(n-r)} \end{bmatrix}$$

Since $\tilde{A}$ is a lower block-triangular matrix, it has $r+1$ eigenvalues $\lambda_i = 1 (i \in \{1, \ldots, r+1\})$, and the rest n-r eigenvalues lie in the open unit disk by invoking Lemma 2 in [24]. Construct matrices $V = [\boldsymbol{\nu}_1, \ldots, \boldsymbol{\nu}_{r+1}]$ and $U = [\boldsymbol{\mu}_1, \ldots, \boldsymbol{\mu}_{r+1}]$. $\boldsymbol{\nu}_i \in \mathrm{R}^{(n+1)\times 1}$ is the left eigenvector of $\tilde{A}$ and is an all-zero vector except its ith entry being 1. $\boldsymbol{\mu}_i \in \mathrm{R}^{(n+1)\times 1}$, which is the right eigenvector of $\tilde{A}$, is non-negative according to Theorem 4.8 in [11], and satisfies $V^T U = I_{r+1}$. When k_p is sufficiently small, according to Lemma 7 in [23], the perturbation on $\lambda_i = 1 (i \in \{1, \ldots, r+1\})$ is quantified by the eigenvalues of

$$V^T\Delta U = \begin{bmatrix} -\boldsymbol{P}_{\max}^T \\ 0_{r\times(n+1)} \end{bmatrix} [\boldsymbol{\mu}_1, \ldots, \boldsymbol{\mu}_{r+1}]$$
$$= \begin{bmatrix} -\boldsymbol{P}_{\max}^T\boldsymbol{\mu}_1 & \cdots & -\boldsymbol{P}_{\max}^T\boldsymbol{\mu}_{r+1} \\ 0_{r\times 1} & \cdots & 0_{r\times 1} \end{bmatrix},$$

where $\boldsymbol{P}_{\max} = [P_{0\max}, \ldots, P_{n\max}]^T$.

$V^T\Delta U$ has a simple eigenvalue $-\boldsymbol{P}_{\max}^T\boldsymbol{\mu}_1 < 0$ and an eigenvalue 0 with an algebraic multiplicity r. Therefore, when k_p is small enough, $\tilde{A}_\Delta$ has an eigenvalue 1 with an algebraic multiplicity r, while the rest of the eigenvalues are inside the open unit disk. This indicates the stability of the system. It is straightforward to verify that in the steady state, (11) and (12) hold. Also, it follows from Lemma 2 in [24] that $(I_{n-r} - A_W)^{-1}\begin{bmatrix} A_0 & A_W \end{bmatrix}$ in (12) is row-stochastic, thus the utilization ratios of the well-behaving DGs converge to the convex hull spanned by $\left[\alpha_0^*, \alpha_M^T\right]^T$.

Proof of Theorem 2: When colluding attacks are not considered, two cases need to be analyzed as follows.

Case 1) Detection criterion (16) is violated. In this case, all the misbehaving DGs that violate (16) can be detected by their out-neighbors and eventually isolated from the communication network. Since the remaining network is still connected with DG 0 as their leader, convergence of the rest of DGs directly follows Theorem 1.

Case 2) Detection criterion (16) is always satisfied, i.e., there are stealthy attacks or no attacks.

In each iteration, any misbehaving DG j can transmits $\alpha_{j\text{low}}^{(k+1)} \le \alpha_j^{(k+1)} \le \alpha_{j\text{up}}^{(k+1)}$ so as to stay undetected from its out-neighbors. Due to the continuity of cooperative control (7), there exists an equivalent set of weights $\{\tilde{a}_{jl}^{(k)} | \forall l \in N_j^{\text{in}}\}$ so that $\alpha_j^{(k+1)} = \sum_{l\in N_j^{\text{in}}} \tilde{a}_{jl}^{(k)}\alpha_l^{(k)}$. Therefore, it is equivalent that the time-invariant system (9) becomes time-varying as

$$\begin{bmatrix} \alpha_0^{(k+1)} \\ \boldsymbol{\alpha}^{(k+1)} \end{bmatrix} = A_\Delta^{(k)} \begin{bmatrix} \alpha_0^{(k)} \\ \boldsymbol{\alpha}^{(k)} \end{bmatrix} + \boldsymbol{b}, \tag{23}$$

where $A_\Delta^{(k)}$ is acquired by substituting $a_{jl}^{(k)}$ in the system matrix A_Δ in (9) with $\tilde{a}_{jl}^{(k)}$ for all $l \in N_j^{\text{in}}$, with j corresponding to any misbehaving DG that does not violate (16).

Define the error system of (23) as

$$\begin{bmatrix} \delta\alpha_0^{(k+1)} \\ \delta\boldsymbol{\alpha}^{(k+1)} \end{bmatrix} = A_\Delta^{(k)} \begin{bmatrix} \delta\alpha_0^{(k)} \\ \delta\boldsymbol{\alpha}^{(k)} \end{bmatrix}, \tag{24}$$

where $\delta\boldsymbol{\alpha}^{(k)} = \left[\alpha_1^{(k)} - \alpha^*, \ldots, \alpha_n^{(k)} - \alpha^*\right]^T$ and $\delta\alpha_0^{(k)} = \alpha_0^{(k)} - \alpha^*$. The stability of (24) can be analyzed utilizing singular perturbation: letting k_p be infinitely close to zero, it follows from Theorem 5.12 in [11] that $\delta\alpha^{(k)}$ is frozen at the quasi-steady state $[1, \ldots, 1]^T\delta\alpha_0^{(k)}$ since $\left\{A^{(k)} : k \in \mathrm{N}\right\}$ is uniformly sequentially complete. Hence, the reduced-system is

$$\begin{aligned} \delta\alpha_0^{(k+1)} &= \left(1 - k_p P_{0\max}\right)\delta\alpha_0^{(k)} - k_p\tilde{\boldsymbol{P}}_{\max}^T\delta\boldsymbol{\alpha}^{(k)} \\ &\approx \left\{1 - k_p\sum_{i=0}^{n} P_{i\max}\right\}\delta\alpha_0^{(k)}, \end{aligned}$$

which is stable since $|1 - k_p\sum_{i=0}^{n} P_{i\max}| < 1$ when k_p is sufficiently small.

REFERENCES

[1] A. M. Bouzid *et al.*, "A survey on control of electric power distributed generation systems for microgrid applications," *Renew. Sustain. Energy Rev.*, vol. 44, pp. 751–766, Apr. 2015.

[2] J. Rocabert, A. Luna, F. Blaabjerg, and P. Rodrı́guez, "Control of power converters in AC microgrids," *IEEE Trans. Power Electron.*, vol. 27, no. 11, pp. 4734–4749, Nov. 2012.

[3] D. Manz *et al.*, "The grid of the future: Ten trends that will shape the grid over the next decade," *IEEE Power Energy Mag.*, vol. 12, no. 3, pp. 26–36, May/Jun. 2014.

[4] Z. Qu and M. A. Simaan, "Modularized design for cooperative control and plug-and-play operation of networked heterogeneous systems," *Automatica*, vol. 50, no. 9, pp. 2405–2414, Sep. 2014.

[5] H. Xin, Z. Qu, J. Seuss, and A. Maknouninejad, "A self-organizing strategy for power flow control of photovoltaic generators in a distribution network," *IEEE Trans. Power Syst.*, vol. 26, no. 3, pp. 1462–1473, Aug. 2011.

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

[7] M. Guo, D. V. Dimarogonas, and K. H. Johansson, "Distributed real-time fault detection and isolation for cooperative multi-agent systems," in *Proc. Amer. Control Conf.*, Montreal, QC, Canada, Jun. 2012, pp. 5270–5275.

[8] A. Gusrialdi, Z. Qu, and M. A. Simaan, "Robust design of cooperative systems against attacks," in *Proc. Amer. Control Conf.*, Portland, OR, USA, Jun. 2014, pp. 1456–1462.

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

[10] A. D. Dominguez-Garcia, C. N. Hadjicostis, and N. H. Vaidya, "Resilient networked control of distributed energy resources," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 6, pp. 1137–1148, Jul. 2012.

[11] Z. Qu, *Cooperative Control of Dynamical Systems: Applications to Autonomous Vehicles*. New York, NY, USA: Springer, 2009.
[12] M. Zhu and S. Martinez, "On the performance analysis of resilient networked control systems under replay attacks," *IEEE Trans. Autom. Control*, vol. 59, no. 3, pp. 804–808, Mar. 2014.
[13] H. J. LeBlanc and X. D. Koutsoukos, "Low complexity resilient consensus in networked multi-agent systems with adversaries," in *Proc. 15th ACM Int. Conf. Hybrid Syst. Comput. Control*, Beijing, China, Apr. 2012, pp. 5–14.
[14] W. Zeng and M.-Y. Chow, "Resilient distributed control in the presence of misbehaving agents in networked control systems," *IEEE Trans. Cybern.*, vol. 44, no. 11, pp. 2038–2049, Nov. 2014.
[15] A. S. Tanenbaum and M. V. Steen, *Distributed Systems: Principles and Paradigms*, 2nd ed. Englewood Cliffs, NJ, USA: Prentice Hall, 2002.
[16] H. Xin, Z. Lu, Y. Liu, and D. Gan, "A center-free control strategy for the coordination of multiple photovoltaic generators," *IEEE Trans. Smart Grid*, vol. 5, no. 3, pp. 1262–1269, May 2014.
[17] H. Xin, Y. Liu, Z. Qu, and D. Gan, "Distributed control and generation estimation method for integrating high-density photovoltaic systems," *IEEE Trans. Energy Convers.*, vol. 29, no. 4, pp. 988–996, Dec. 2014.
[18] A. Maknouninejad and Z. Qu, "Realizing unified microgrid voltage profile and loss minimization: A cooperative distributed optimization and control approach," *IEEE Trans. Smart Grid*, vol. 5, no. 4, pp. 1621–1630, Jul. 2014.
[19] A. Teixeira, D. Pérez, H. Sandberg, and K. H. Johansson, "Attack models and scenarios for networked control systems," in *Proc. 1st ACM Int. Conf. High Confidence Netw. Syst.*, Beijing, China, Apr. 2012, pp. 55–64.
[20] C. Li and Z. Qu, "Distributed estimation of algebraic connectivity of directed networks," *Syst. Control Lett.*, vol. 62, no. 6, pp. 517–524, Jun. 2013.
[21] A. Gusrialdi, "Performance-oriented communication topology design for distributed control of interconnected systems," *Math. Control Signals Syst.*, vol. 25, no. 4, pp. 559–585, Aug. 2013.
[22] W. H. Kersting, "Radial distribution test feeders," *IEEE Trans. Power Syst.*, vol. 6, no. 3, pp. 975–985, Aug. 1991.
[23] K. Cai and H. Ishii, "Average consensus on general strongly connected digraphs," *Automatica*, vol. 48, no. 11, pp. 2750–2761, Nov. 2012.
[24] Z. Li, W. Ren, X. Liu, and M. Fu, "Distributed containment control of multi-agent systems with general linear dynamics in the presence of multiple leaders," *Int. J. Robust Nonlin. Control*, vol. 23, no. 5, pp. 534–547, Mar. 2013.

Yun Liu (S'14) received the B.Eng. degree (First Class Hons.) from the College of Electrical Engineering, Zhejiang University, Hangzhou, China, in 2011, where he is currently pursuing the Ph.D. degree. He was a Visiting Student with the Department of Electrical Engineering and Computer Science, University of Central Florida, Orlando, from 2014 to 2015. His research interests include power system stability analysis and distributed control of renewable energy.

Huanhai Xin (M'14) received the Ph.D. degree from the Department of Electrical Engineering, Zhejiang University, Hangzhou, China, in 2007. He is currently an Professor with the Department of Electrical Engineering, Zhejiang University. He was a Post-Doctorate in the Department of Electrical Engineering and Computer Science, University of Central Florida, from 2009 to 2010. His research interests include power system stability analysis and distributed control of renewable energy.

Zhihua Qu (M'90–SM'93–F'09) received the Ph.D. degree in electrical engineering from the Georgia Institute of Technology in 1990. Since then, he has been with the University of Central Florida (UCF), currently as a Professor and the Chair of ECE. He is the SAIC Endowed Professor of UCF. His areas of expertise are nonlinear systems and control, energy and power systems, autonomous vehicles, and robotics. In energy systems, his research covers such subjects as low-speed power generation, dynamic stability of distributed power systems, anti-islanding control and protection, distributed generation and load sharing control, distributed VAR compensation, distributed optimization, and cooperative control.

Deqiang Gan (M'96–SM'01) received the Ph.D. degree from Xi'an Jiaotong University, Xian, China, in 1994. He has been a Faculty Member with Zhejiang University, Hangzhou, China, since 2002. His employment experience includes ISO New England, Inc., Ibaraki University, the University of Central Florida, and Cornell University. His research interests include power system stability and market operations. He currently serves as an Editor of the *International Transactions on Electrical Energy Systems*.