Cybersecure Distributed Voltage Control of AC Microgrids

Ali Bidram
Member, IEEE
ECE Deparment
Univeristy of New Mexico
Albuquerque, New Mexico, USA
bidram@unm.edu

Lakshmisree Damodaran
Student Member, IEEE
ECE Deparment
Univeristy of New Mexico
Albuquerque, New Mexico, USA
lakshmid@unm.edu

Rafael Fierro
Fellow, IEEE
ECE Deparment
Univeristy of New Mexico
Albuquerque, New Mexico, USA
rfierro@unm.edu

***Abstract*— In this paper, the cybersecurity of distributed secondary voltage control of AC microgrids is addressed. A resilient approach is proposed to mitigate the negative impacts of cyberthreats on the voltage and reactive power control of Distributed Energy Resources (DERs). The proposed secondary voltage control is inspired by the resilient flocking of a mobile robot team. This approach utilizes a virtual time-varying communication graph in which the quality of the communication links is virtualized and determined based on the synchronization behavior of DERs. The utilized control protocols on DERs ensure that the connectivity of the virtual communication graph is above a specific resilience threshold. Once the resilience threshold is satisfied the Weighted Mean Subsequence Reduced (WMSR) algorithm is applied to satisfy voltage restoration in the presence of malicious adversaries. A typical microgrid test system including 6 DERs is simulated to verify the validity of proposed resilient control approach.**

***Index Terms*— AC microgrids, cyber-attacks, distributed control, secondary voltage control, WMSR algorithm**

I. Introduction

Microgrids are a group of interconnected loads and distributed energy resources (DERs) that act as a controllable unit [1]. They facilate the reliable integration of distributed energy resources (DERs) and are the main building block of smart grids. The main feature of microgrids that distinguishes them from conventional electric power systems is their ability to autonomously operate in the so-called islanded mode when they lose the support from an upstream grid. To cope with this requirement, microgrids utilize a hierarchical control structure which acts as the microgrid brain, oversees its reliable operation, and manages smooth transition from grid-connected to islanded mode of operation [2]. More specifically, one of the important roles of hierarchical control structure is to ensure voltage and frequency stability of microgrid subsequent to the islanding. This is achieved through the lowest hierarchy of microgrid control which is called primary control level and is locally implemented at DERs. It should be noted that primary control does not guarantee the microgrid operation at the nominal voltage and frequency values which is imperative to ensure the efficient operation of electric power equipment. This requirement is satisfied through the secondary control level that supervises primary control and operates microgrid at the nominal voltage and frequency values. The highest control hierarchy is referred as to tertiary control level which manages the active and reactive power flow between microgrid and upstream grid at the point of common coupling and satisfies the economically optimal operation of microgrid [2]. The focus of this paper is on the secondary control level with distributed control structure which has gained much attention compared to the conventional centralized structure due to its enhanced reliability, flexibility, and scalability [3]-[6].

Due to the massive deployment of computational techniques and communication infrastructure, microgrid control system is highly exposed to cyber-attacks. Cyber-attacks can aim at the individual DERs as well as the communication links among them to corrupt the data transfer [7]-[13]. Like bulk power systems, voltage and frequency stability are critical factors in the operation of microgrids. Proper control of voltage and frequency can avoid the cascading failures of microgrid components which results in the outage of power delivered to the critical customers during the emergency conditions [14]. Injecting false data to communication network or manipulating the DER controllers can disrupt the proper voltage and frequency synchronization. A cybersecure resilient distributed control must be able to adapt to tasks in the presence of unknown attacks and failures. The bulk of the research in cybersecurity of power systems focuses on the detection of attacks [7]-[12]. In [6], a trust/confidence-based control protocol is proposed to mitigate the impact of cyber-attacks on the distributed frequency control of microgrids. However, the proposed approach does not cover the synchronization and control of voltage and reactive power of DERs. In [7], a systematic approach is proposed to detect and remove attacked agents from the distributed control protocols. However, this approach depends on the high connectivity of the communication graph to ensure resilient operation of distributed control algorithms.

In this paper, a resilient distributed secondary voltage control is proposed that utilizes a virtual time-varying communication graph in which the quality of the communication links is determined based on the

This material is based upon work supported by the National Science Foundation EPSCoR Program under Award #OIA-1757207.

978-1-5386-7551-9/19/$31.00 ©2019 IEEE

synchronization behavior of DERs. The proposed secondary voltage control is inspired by the resilient flocking of the mobile robot teams proposed in [15]. DERs utilize a distributed control protocol to modify the quality of communication links and ensure that the connectivity of the communication graph is above the resilience threshold. Once the resilience threshold is satisfied the Weighted Mean Subsequence Reduced (WMSR) synchronization algorithm is applied to satisfy voltage restoration in the microgrid. Additionally, the proposed distributed voltage control shares the reactive power among DERs based on their reactive power ratings.

The rest of paper is organized as follows: Section II provides the preliminaries of graph theory. Section III discusses the conventional distributed secondary voltage control. In Section IV, the resilient distributed voltage control is presented. In Section V, a microgrid test system is simulated to verify the validity of the proposed resilient secondary voltage control. Section VI concludes the paper.

II. Preliminaries of Graph Theory

In this paper, graph theory is used to model and analyze the distributed communication network utilized to implement the microgrid secondary control. In the representative communication graph, nodes denote DERs and edges describe communication links. A graph $\mathcal{G}=(\mathcal{V},\mathcal{E},\mathcal{A})$ includes a nonempty finite set of N nodes $\mathcal{V}=\{v_1,v_2,\ldots,v_N\}$ and a set of edges $\mathcal{E}\subset\mathcal{V}\times\mathcal{V}$. The associated adjacency matrix $\mathcal{A}=[a_{ij}]\in\mathbb{R}^{N\times N}$ describes the connectivity of nodes through edges. An edge from node j to node i, denoted by (v_j,v_i), facilitates the flow of information from node *j* to node *i*. a_{ij} is the weight of edge (v_j,v_i), and $a_{ij}>0$ if $(v_j,v_i)\in\mathcal{E}$, otherwise $a_{ij}=0$. The set of neighbors of node i is denoted as $N_i=\{j\,|\,(v_j,v_i)\in\mathcal{E}\}$. The Laplacian matrix is defined as $L=D-\mathcal{A}$, where $D=\mathrm{diag}\{d_i\}\in\mathbb{R}^{N\times N}$ is the in-degree matrix with $d_i=\sum_{j\in N_i}{}' a_{ij}$ [16].

III. Conventional Distributed Secondary Voltage Control

In this section, first, the dynamic model of an inverter-based DER and primary control is elaborated. Then, the conventional distributed secondary voltage control is discussed.

A. Dynamic Model of VSC and Primary Control

The block diagram of an power electronics-based DER is shown in Fig. 1. As opposed to rotatory machine types, this type of DERs includes the dc power source, Voltage Source Converter (VSC), and the power, voltage, and current control loops [4].

The nonlinear dynamics of the *i*-th DER in a microgrid, can be written as

$$\begin{cases}\dot{\mathbf{x}}_i=\mathbf{f}_i(\mathbf{x}_i)+\mathbf{g}_i(\mathbf{x}_i)u_i\\ y_i=h_i(\mathbf{x}_i)+d_iu_i\end{cases}. \tag{1}$$

Detailed expressions for $\mathbf{f}_i(\mathbf{x}_i)$, $\mathbf{g}_i(\mathbf{x}_i)$, $h_i(\mathbf{x}_i)$, and d_i are adopted from the nonlinear model presented in [4]. The state vector is

$$\begin{aligned}\mathbf{x}_i=[&\delta_i \quad P_i \quad Q_i \quad \phi_{di} \quad \phi_{qi} \quad \gamma_{di} \quad \gamma_{qi} \quad i_{ldi} \quad i_{lqi}\\ &v_{odi} \quad v_{oqi} \quad i_{odi} \quad i_{oqi}]^T,\end{aligned} \tag{2}$$

where δ_i is the angle of *i*-th DER reference frame. P_i and Q_i are the active and reactive power of DER. v_{odi}, v_{oqi}, i_{odi}, and i_{oqi} are the direct and quadrature components of v_{oi} and i_{oi} in Fig. 1. i_{ldi} and i_{lqi} are the direct and quadrature components of LC filter current. ϕ_{di} and ϕ_{qi} are the auxiliary state variables defined for internal voltage controller and γ_{di} and γ_{qi} are the auxiliary state variables defined for internal current controller.

The nonlinear dynamics of each DER are formulated in its own *d-q* (direct-quadrature) reference frame. It is assumed that the reference frame of the *i*-th DER is rotating at the frequency of ω_i. The reference frame of one DER is considered as the common reference frame with the rotating frequency of ω_{com}. The angle of the *i*-th DER reference frame, with respect to the common reference frame, is denoted as δ_i and satisfies the following differential equation

$$\dot{\delta}_i=\omega_i-\omega_{com}. \tag{3}$$

In Fig. 1, power control block includes primary control that is implemented through the droop technique. This technique prescribes a relation between the frequency and the active power, and between the voltage magnitude and the reactive power through droop characteristics

$$\begin{cases}\omega_i=\omega_{ni}-m_{Pi}P_i\\ v_{o,magi}=V_{ni}-n_{Qi}Q_i\end{cases}, \tag{4}$$

where ω_{ni} and V_{ni} are the primary frequency and voltage control references and m_{Pi} and n_{Qi} are the active and reactive power droop coefficients, respectively [2]. The droop coefficients are chosen proportional to the active and reactive power ratings of DERs, $P_{\max i}$, $Q_{\max i}$. Doing so, one can ensure that the active and reactive power of DERs are assigned based on the active and reactive power ratings, i.e.,

$$\begin{cases}\dfrac{P_j}{P_i}=\dfrac{P_{\max j}}{P_{\max i}}=\dfrac{m_{Pi}}{m_{Pj}}\\ \dfrac{Q_j}{Q_i}=\dfrac{Q_{\max j}}{Q_{\max i}}=\dfrac{n_{Qi}}{n_{Qj}}\end{cases}. \tag{5}$$

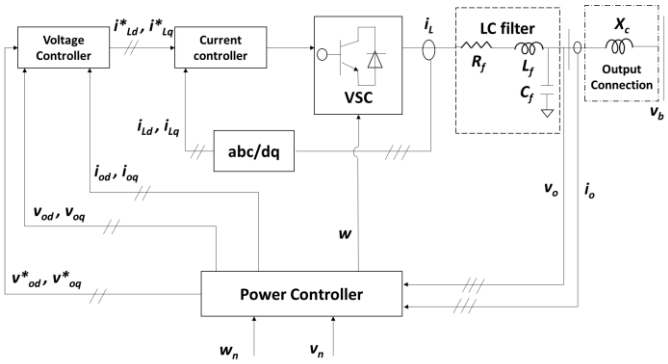


Fig. 1. An inverter-based DER power and control modules [5].

B. Distributed Secondary Voltage Control

The secondary voltage control chooses V_{ni} in (4) such that the terminal voltage magnitude of each DER synchronizes to the reference voltage, i.e., $v_{o,magi} \to V_{ref}$. Additionally, secondary voltage control should ensure that the reactive power of DERs are proportional to their reactive power ratings [5]. For the secondary voltage control, the output and input in (1) are $y_i = v_{o,magi}$ and $u_i = V_{ni}$, respectively. The reference voltage V_{ref} is equal to the nominal voltage of microgrid.

The distributed secondary voltage control is derived by differentiating the two sides of (4) and building up an auxiliary control variable for the control input V_{ni} as follows

$$\dot{V}_{ni} = \dot{V}_i + n_{Qi}\dot{Q}_i = v_{vi}, \tag{6}$$

where v_{vi} is the auxiliary control input. Equation (6) is a dynamic system for computing the control input V_{ni} from v_{vi} . The auxiliary controls are chosen based on the information of each DER and its neighbors in the communication graph and can be written as [5]

$$\begin{aligned} v_{vi} = &-c_v\Big(\sum_{j\in N_i} a_{ij}(v_{o,magi} - v_{o,magj}) + g_i(v_{o,magi} - v_{ref})\Big) \\ &-c_v\Big(\sum_{j\in N_i} a_{ij}(n_{Qi}Q_i - n_{Qj}Q_j)\Big), \end{aligned} \tag{7}$$

where $c_v \in \mathbb{R}$ is the control gain. only one DER needs the information of reference voltage. The pinning gain $g_i \geq 0$ is nonzero for the DER that has the reference voltage information.

IV. Cybersecure Distributed Secondary Voltage Control

In this section, the resilient distributed secondary voltage control of microgrids is proposed. A DER is considered to be cooperative if it can successfully apply the distributed secondary voltage control protocol in (7), and share its information with the neighboring DERs. On the other hand, a non-cooperative DER either fails to apply the distributed secondary voltage control successfully or shares malicious data with neighboring DERs on the communication graph. The non-cooperative DER might be also defective, i.e., it unintentionally measures the false local data (e.g., voltage and reactive power) due to the presence of faulty sensors. In the event of a cyber-attack, the attacker gains access to the communication nodes and manipulates the data flow on the communication graph.

A. Virtual Communication Graph Scheme

In the conventional distributed secondary control, the adjacency matrix, $\mathcal{A} = [a_{ij}] \in \mathbb{R}^{N\times N}$, is assumed to be constant, i.e., the weight of a typical communication link is a constant value. This paper, however, utilizes a time-varying communication graph in which the quality of the communication links is virtually dictated by the DERs. For this purpose, a Communication Link Quality (CLQ) function is utilized at each DER to determine the quality of the communication links between that DER and its neighbors. In this work, an exponential-based CLQ function utilizes the difference between the reference frame angle, δ_i, of DERs as a measure of the quality of the communication links among them, thus [15]

$$a_{ij} = \begin{cases} N & \left|\delta_i - \delta_j\right| < R_1 \\ 0 & \left|\delta_i - \delta_j\right| \geq R_2 \\ N \times \exp\left(\dfrac{-\gamma(\left|\delta_i - \delta_j\right| - R_1)}{R_2 - R_1}\right) & \text{otherwise,} \end{cases} \tag{8}$$

where N is the number of DERs and j denotes the neighbors of i-th DER on the communication network. R_1 denotes the threshold below which the health of communicating DERs is assumed to be guaranteed. Therefore, the quality of the communication link is set to a maximum value which in this paper is equal to the total number of DERs in the microgrid.

As the reference frame angle of neighboring DERs drift apart from each other the quality of the communication link between them decreases exponentially, until the difference between the reference frame angel of neighboring DERs is more than R_2 and the quality of the communication link is forced to zero. γ is a design parameter that can be adjusted to leverage the smoothness of the CLQ function. The CLQ function is smoother for larger γ . Equation (8) shows that if the reference frame angle between two DERs is greater than a specific value (i.e., R_2), the virtual communication graph automatically prevents the flow of information between those DERs to mitigate the risk of instability in the microgrid. It should be noted that the CLQ function is limited to the physical communication network and changes the quality of the communication links in real time only if there is a physical communication link between two DERs.

B. Mitigating the Impact of Non-cooperative DERs Using WMSR Algorithm

The WMSR algorithm objective is to mitigate the impacts of non-cooperative agents in a networked multi-agent system and achieve consensus to a weighted average value of cooperative nodes [17]-[18]. However, to ensure consensus in the presence of F non-cooperative nodes, the network must satisfy a certain connectivity requirement which is given in Theorem 1.

Definition 1 [15]: A non-trivial graph is *r*-robust if for each pair of disjoint subsets at least one of them is *r*-reachable, i.e., there is a node in that subset for which the number of edges leaving that subset from that node is greater than *r*.

Theorem 1 [17]: If a network modeled by a graph $\mathcal{G}=(\mathcal{V},\mathcal{E})$, in which the cooperative agents update their values using WMSR algorithm with parameter F, is considered, then, resilience asymptotic consensus is guaranteed if the graph is (2F+1)-robust.

The WMSR algorithm consists of two stages which are executed at each time step by each DER:

Stage 1: Each DER creates a list of voltage magnitudes received from the neighboring DERs on the communication graph, i.e., $v_{o,magj}$, $j \in N_i$, and sorts them from smallest to largest value.

Stage 2: Each DER compares the voltage magnitudes of neighboring DERs with its own voltage magnitude and updates the distributed voltage control protocol as follows: If there are F or more than F larger neighboring agent voltage magnitudes, the F largest voltage magnitudes are removed from the consensus protocol in (7). If there are fewer than F larger voltage magnitudes, all of them are removed from the consensus protocol. The same process is applied to the smaller voltage magnitudes. Doing so, the distributed voltage control protocol is updated as

$$\begin{aligned} v_{vi} = &-c_v\Big(\sum_{j\in R_{vi}} a_{ij}(v_{o,magi}-v_{o,magj})+g_i(v_{o,magi}-v_{ref})\Big) \\ &+-c_v\Big(\sum_{j\in R_{vi}} a_{ij}(n_{Qi}Q_i-n_{Qj}Q_j)\Big), \end{aligned} \tag{9}$$

where R_{vi} denotes the new set of neighbors of *i*-th DER for voltage control after the removal process.

It should be noted that WMSR algorithm guarantees resilient consensus if the graph is (2F+1)-robust. However, calculating the level of *r*-robustness is co-NP complete [19], which increases the computational burden in the presence of large number DERs with a time-varying communication graph. In [15], an alternative metric is proposed to lower-bound the value of *r*.

Theorem 2 [15]: For a graph $\mathcal{G}=(\mathcal{V},\mathcal{E})$, $\left\lfloor \frac{\lambda_2}{2} \right\rfloor$ lower-bounds *r* in a *r*-robust graph, where λ_2 is the algebraic connectivity of the graph $\mathcal{G}$.

From Theorem 2 and the connectivity requirement of WMSR algorithm, the resilient convergence can be guaranteed if the following condition is satisfied

$$\lambda_2 > 4F. \tag{10}$$

Equation (10) denotes that to ensure the resilient consensus using WMSR algorithm in the presence of F non-cooperative DERs, the algebraic connectivity of the communication graph should be larger than 4F. For this purpose, the following control protocol is proposed to ensure that (10) is satisfied before the WMSR algorithm is applied

$$\dot{\omega}_{ni} = \frac{\partial \lambda_2}{\partial \delta_i}, \tag{11}$$

where ω_{ni} is the primary frequency control reference in (4) and δ_i is the reference frame angle of *i*-th DER. The algebraic connectivity is a concave function of Laplacian matrix L which in turn is a function of the reference frame angle of DERs (See (8)). If λ_2 is unique, its derivative with respect to L can be written as [20]

$$\frac{\partial \lambda_2(L)}{\partial L} = \frac{\mathbf{V}_2\mathbf{V}_2^T}{\mathbf{V}_2^T\mathbf{V}_2}, \tag{12}$$

where $\mathbf{V}_2$ is eigen vector related to λ_2. On the other hand, L is a function of the reference frame angle of DERs according to (8). Using the chain rule, the control protocol in (11) can be written as [15]

$$\dot{\omega}_{ni} = \text{Trace}\left\{\left[\frac{\mathbf{V}_2\mathbf{V}_2^T}{\mathbf{V}_2^T\mathbf{V}_2}\right]^T\left[\frac{\partial L}{\partial \delta_i}\right]\right\}. \tag{13}$$

To implement the resilient secondary voltage control of microgrids, each DER monitors the algebraic connectivity of the virtual communication graph at each time step and compares it with $\eta\times 4F$, where η is a safety factor to ensure that algebraic connectivity has enough margin to stay above the resilient convergence threshold in (10). If the algebraic connectivity is less than $\eta\times 4F$, the algebraic connectivity control protocol in (13) is applied until the algebraic connectivity is greater than $\eta\times 4F$. If the algebraic connectivity is greater than or equal to $\eta\times 4F$, the WMSR algorithm is deployed to eliminate the non-cooperative DERs from the distributed secondary voltage control protocol as shown in (9). A graph coordinator oversees the virtual communication graph, calculates its algebraic connectivity, and shares this information with DERs to switch between the control protocol in (13) and WMSR algorithm.

V. Simulation Results

In Fig. 2, the single-line diagram of the microgrid test system is illustrated. IEEE 34 bus test feeder is slightly modified by integrating six DERs to build up the microgrid testbed. Moreover, the line parameters are averaged to transform the original IEEE 34 bus feeder to a balanced feeder. The specification of lines is provided in [21]. The specifications of the DERs and loads are summarized in Tables I and II list the specifications of the DERs and loads, respectively. The microgrid frequency is 60 Hz. The nominal line-to-line voltage is 24.9 kV. Six transformers are modelled to integrate DERs to the feeder. Each transformer has wye-wye arrangement, with 480 V/24.9 kV voltage ratings, and 400 kVA power rating. The series impedance of each transformer is 0.03 + j 0.12 pu. The communication network graph is depicted in Fig. 3. DER 1 is the only DER that knows the voltage reference value and is connected to the leader node with the pinning gain $g_1 = 1$. The parameters of CLQ function in (8) to create the virtual communication graph are as follows: R_1 is set to $\pi/50$; R_2 is set to $\pi/2$; γ is set to 5. The control gain c_v in (9) are set to 40. It is assumed that DER 6 is a non-cooperative DER and shares the constant voltage magnitude of 482 V with its neighbors on the communication graph, i.e., DER 4 and 5.

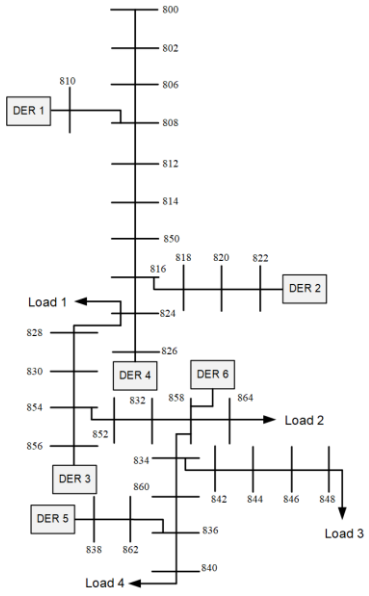


Fig. 2. IEEE 34 bus test feeder with 6 integrated DERs.

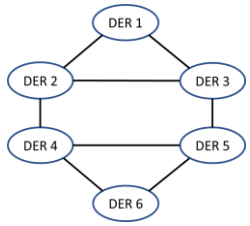


Fig. 3. Communication network architecture.

TABLE I. DER Specifications

DER 1, 2, 5 and 6		DER 3 and 4	
m_P	5.64×10^{-5}	m_P	7.5×10^{-5}
n_Q	5.2×10^{-4}	n_Q	6×10^{-4}
R_c	30 mΩ	R_c	30 mΩ
L_c	350 µH	L_c	350 µH
R_f	100 mΩ	R_f	100 mΩ
L_f	1350 µH	L_f	1350 µH
C_f	50 µF	C_f	50 µF
K_{PV}	0.1	K_{PV}	0.05
K_{IV}	420	K_{IV}	390
K_{PC}	15	K_{PC}	10.5
K_{IC}	20000	K_{IC}	16000

TABLE II. Specification of Loads

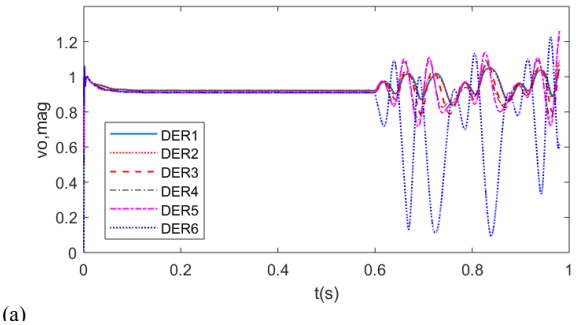
Load 1		Load 2		Load 3		Load 4	
R	1.5 Ω	R	0.5 Ω	R	1 Ω	R	0.8 Ω
X	1 Ω	X	0.5 Ω	X	1 Ω	X	0.8 Ω

Case 1: In this test case, the impact of the non-cooperative DER 6 on the performance of conventional distributed secondary voltage control in (7) is studied. The voltage magnitude of DERs and their reactive power ratios, $n_{Qi}Q_i$, before and after applying the conventional distributed voltage control under attack are shown in Fig. 4(a) and Fig. 4(b). The islanding occurs at $t = 0$ and conventional secondary voltage control is applied at $t = 0.6$ s. As seen, the conventional distributed voltage control fails to restore the voltage magnitude of DERs to the close vicinity of nominal voltage and voltage stability of microgrid is lost.

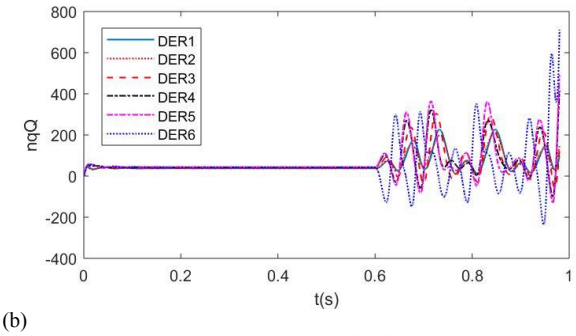
Case 2: In this test case, the validity of the proposed resilient distributed secondary voltage control is verified. Similar to Case 1, microgrid is islanded at $t = 0$ and conventional secondary voltage control is applied at $t = 0.6$ s. The resilient distributed voltage control is applied at $t = 0.65$ s. As seen in Fig. 5(a) and Fig. 5(b), after the resilient voltage control is applied, the voltage magnitude and reactive power ratio, $n_{Pi}Q_i$, of DERs converge back to a common value. The DER voltage magnitudes are restored to the close vicinity of 1 pu after $t = 1.5$ sec. Additionally, the reactive power of DERs are allocated based on their reactive power ratings.

VI. Conclusion

This paper proposes a resilient approach based on WMSR algorithm for the distributed secondary voltage control of microgrids. The methodology utilizes a time-varying virtual communication graph which dictates the quality of the communication links among DERs. The time-varying communication graph is a function of reference frame angle of DERs and is tuned up such that the algebraic connectivity of graph is always above a resilient threshold which satisfies the convergence of WMSR algorithm in the presence of non-cooperative DERs. IEEE 34-bus test feeder is simulated as a microgrid test system to verify the validity of proposed resilient control approach.

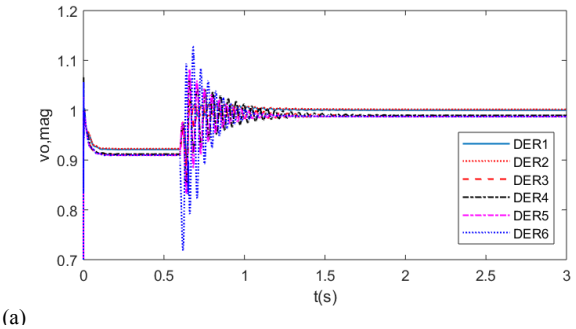


(a)

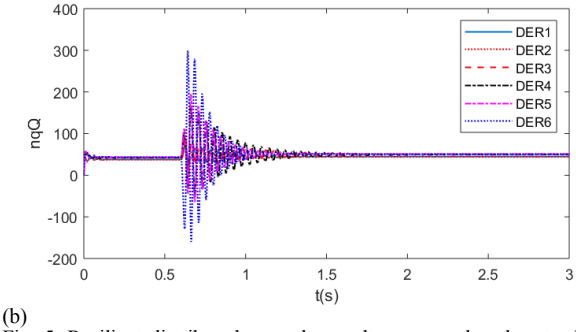


(b)

Fig. 4. Impact of attack on conventional distributed secondary voltage control: a) DER voltage magnitudes; b) DER reactive power ratios ($n_{Qi}Q_i$).



(a)



(b)

Fig. 5. Resilient distributed secondary voltage control under attack: a) DER voltage magnitudes; b) DER reactive power ratios ($n_{Qi}Q_i$).

REFERENCES

[1] D. T. Ton and M. A. Smith, "The U.S. Department of Energy's Microgrid Initiative", *Elseiveir, The Electricity Journal,* vol. 25, pp. 84-94, Oct. 2012.

[2] A. Bidram and A. Davoudi, "Hierarchical structure of microgrids control system," *IEEE Trans. Smart Grid,* vol. 3, pp. 1963-1976, Dec. 2012.

[3] M.Yazdanian and A. Mehrizi-Sani, "Distributed control techniques in microgrids," *IEEE Trans. Smart Grid,* vol. 5, pp. 2901-2909, Nov. 2014.

[4] A. Bidram, A. Davoudi, F. L. Lewis, and J. M. Guerrero, "Distributed cooperative control of microgrids using feedback linearization," *IEEE Trans. Power Syst.,* vol. 28, pp. 3462-3470, Aug. 2013.

[5] A. Bidram, A. Davoudi, and F. L. Lewis, "A Multiobjective distributed control framework for islanded AC microgrids," *IEEE Trans. Ind. Informat.,* vol. 10, pp. 1785-1798, May 2014.

[6] S. Abhinav, H. Modares, F. L. Lewis, F. Ferrese, and A. Davoudi, "Synchrony in networked microgrids under attacks," *IEEE Trans. Smart Grid,* vol. 9, no. 6, pp. 6731-6741, Nov. 2018.

[7] F. Pasqualetti, A. Bicchi, and F. Bullo, "Consensus computation inunreliable networks: A system theoretic approach," *IEEE Trans. Autom. Control*, vol. 57, pp. 90–104, Jan 2012.

[8] F. Pasqualetti, F. Dorfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Trans. Autom. Control*, vol. 58, no. 11, pp. 2715–2729, Nov 2013.

[9] Y. Huang, J. Tang, Y. Cheng, H. Li, K. A. Campbell, and Z. Han, "Realtime detection of false data injection in smart grid networks: An adaptive cusum method and analysis," *IEEE Syst. J.*, vol. 10, no. 2, pp. 532–543, June 2016.

[10] K. Manandhar, X. Cao, F. Hu, and Y. Liu, "Detection of faults and attacks including false data injection attack in smart grid using kalman filter," *IEEE Trans. Control Netw. Syst.*, vol. 1, no. 4, pp. 370–379, Dec. 2014.

[11] S. Bi and Y. J. Zhang, "Graphical methods for defense against false-data injection attacks on power system state estimation," *IEEE Trans. Smart Grid*, vol. 5, no. 3, pp. 1216–1227, May 2014.

[12] Y. Mo, R. Chabukswar, and B. Sinopoli, "Detecting integrity attacks on scada systems," *IEEE Trans. Control Syst. Technol*., vol. 22, no. 4, pp. 1396–1407, July 2014.

[13] L. Liu, M. Esmalifalak, Q. Ding, V. A. Emesih, and Z. Han, "Detecting false data injection attacks on power grid by sparse optimization," *IEEE Trans. Smart Grid*, vol. 5, pp. 612–621, March 2014.

[14] B. Schafer, D. Witthaut, M. Timme, and V. Latora, "Dynamically induced cascading failures in power grids" *Nautre Communications*, vol. 9, Article Number 1975, pp. 1–13, 2018.

[15] K. Saulnier, D. Saldana, A. Prorok, G. J. Pappas, and V. Kumar, "Resileint flocking for mobile robot teams," *IEEE Robotics and Automation letters,* vol. 2, pp. 1039-1046, Apr. 2017.

[16] Z. Qu, Cooperative control of dynamical systems: Applications to autonomous vehicles. New York: Springer-Verlag, 2009.

[17] H. Zhang and S. Sundaram, "Robustness of information diffusion algorithms to locally bounded adversaries," in *IEEE Proc. Amer. Controls Conf.*, 2012, pp. 5855–5861.

[18] H. J. LeBlanc, H. Zhang, X. Koutsoukos, and S. Sundaram, "Resilient asymptotic consensus in robust networks," *IEEE J. Sel. Areas Commun.*, vol. 31, pp. 766–781, Apr. 2013.

[19] H. Zhang, E. Fata, and S. Sundaram, "Robustness of complex networks: Reaching consensus despite adversaries," CoRR, vol. abs/1203.6119, 2012, 35 pages.

[20] E. Stump, A. Jadbabaie, and V. Kumar, "Connectivity management in mobile robot teams," in *Proc. IEEE Int. Conf. Robot. Autom*., May 2008, pp. 1525–1530.

[21] N. Mwakabuta and A. Sekar, "Comparative study of the IEEE 34 node test feeder under practical implications," in *Proc. 39th North American Power Symposium*, Sep. 2007.