COMMUNICATION-COGNIZANT CONTROL OF MICROGRIDS

by

SHANKAR ABHINAV

DISSERTATION

Submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy at
The University of Texas at Arlington
August 2017

Arlington, Texas

Supervising Committee:

Ali Davoudi, Supervising Professor

William E. Dillon

Ramtin Madani

Rasool Kenarangui

Ioannis D. Schizas

ABSTRACT

COMMUNICATION-COGNIZANT CONTROL OF MICROGRIDS

SHANKAR ABHINAV, Ph.D.

The University of Texas at Arlington, 2017

Supervising Professor: Ali Davoudi

The increased integration of power electronic devices, advanced software-based controllers, and communication networks has transformed the microgrid from a simple physical system into a cyber-physical system. In this work, advanced distributed control algorithms and communication network are leveraged to provide a robust control structure for AC and DC microgrids. Introduction of distributed control and communication networks in microgrids presents its own unique challenges, which has not been considered in existing literature. A noise-resilient distributed controller is proposed for synchronization of frequency and voltage in AC microgrids. Synchronization in AC microgrids is cast as an optimization problem, and solved using Alternating Direction Method of Multipliers to provide a robust distributed controller. An attack resilient controller is also proposed for AC and DC microgrids, which utilizes trust-based evaluation of neighbors to detect and mitigate attacks on communication links, sensors, actuators, and controller (hijacking). A containment based voltage regulator and consensus based load sharing regulator is also studied, to achieve voltage regulation within a bound and proportional load sharing in a DC microgrid. Extensive model based simulation for AC microgrid and Hardware-in-the-Loop verification for DC microgrid have been carried out to study the proposed controllers.

To my family.

ACKNOWLEDGEMENTS

I want to thank the National Science Foundation (Grant ECCS-1405173), U.S. Office of Naval Research (Grant N00014-14-1-0718 and N00014-17-1-2239), Defense University Research Instrumentation Program (Grant N0014-16-1-3180), Department of Electrical Engineering at UT Arlington, and Office of Graduate Studies at UT Arlington (Summer Dissertation Fellowship) for providing financial support that allowed me to pursue my doctoral research.

I would like to express my sincere gratitude to my supervising professor, Dr. Ali Davoudi, for providing me with this wonderful opportunity, and constantly motivating during this endeavor. He spent countless hours and precious energy to improve my research output. He set a high bar for quality, which inspired me to do some of my best work till date. My committee members: Dr. Dillon, Dr. Schizas, Dr. Madani and Dr. Kenarangui provided valuable comments and suggestions, which helped me improve the quality of my research work and provided ideas for new avenues of research as well. Dr. Schizas patiently sat with me and went over my derivations, and also provided me with the tools that formed the crux of my research. Dr. Modares introduced me to some innovative control concepts in the field of resilient control. Dr. Lewis helped me understand the 'big picture' in multi-agent control systems.

The administrative staff in the Department of Electrical Engineering provided valuable support. Ms. Gail Paniuski was my one stop for all queries regarding the department policy. The writing center at the library helped proofread all my manuscripts.

Seyedali Moayedi and Vahidreza Nasirian provided me with a road map on how to complete my dissertation. Ajay Yadav, Omar Beg, Tuncay Altun, Sameer Mojlish, and

were my fellow comrades in the trenches. Nuh Erdogan provided some welcome Turkish music to liven up the lab environment.

My social circle at Arlington has constantly dwindled as my PhD progressed, but one man who stuck it out was Raghavendra Sriram. He has been my source of transportation for the last four years.

I cannot express in words my gratitude to my family for their support and encouragement. My brother has always been an inspiration, due to his natural brilliance. My father gave me my first taste of engineering and got me hooked on it. My mother always had confidence in my abilities, even if I didn't.

July 24, 2017

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

1.1 Motivation

Power distribution systems are undergoing vast transformation, due to a shift in generation techniques, consumption requirements, and availability of advanced control paradigms. Integration of renewable energy sources, electronic loads, storage devices, and electrified transportation warrants the use of power electronic intensive microgrids [1, 2]. These microgrids must have the capability to operate independently of the main grid.

Control hierarchy of power-electronic intensive AC and DC microgrids [3,4] consists of three levels of control primary, secondary, and tertiary. This control hierarchy is inherited from the control architecture of the legacy grid. The primary control maintains the inverter/converter output voltage (and frequency in AC microgrids), usually through droop mechanisms [3, 4]. The secondary control provides the set-points for droop controllers [5] in the primary layer, to enforce synchronization of voltage (and frequency in AC microgrids). The tertiary controller provides the optimal set-point for the secondary controller by solving market related problems, such as the optimal power flow [6].

Conventionally centralized control has been used for secondary control in microgrids [7, 8]. Recent work in secondary control of microgrids has focused on distributed control [5, 9–19] to improve reliability. These distributed control paradigms intensively use communication to achieve the global objective of control and stability. Communication in practice always has noise, especially in the harsh operating conditions of power networks [20, 21]. The existing secondary distributed control paradigms in microgrid have assumed an ideal, noise-free communication. The secondary control objective of synchro-

nization using the existing distributed control protocols [5, 13–19], in the presence of noise cannot be guaranteed [22].

Power distribution networks have always been a target for cyber attack, incidents such as the Maroochy breach of control [23] and StuxNET worm attack on a nuclear enrichment facility [24] have well established the vulnerability of the legacy grid. Distributed control increases reliability of the microgrid due to the absence of a single point of failure. However, given the absence of a central controller to monitor the entire system, such distributed solutions are susceptible to cyber attacks, where an attacker can corrupt the information exchanged by targeting the controller, communication network, or hijacking the local control. Corrupt data in the system may lead to loss of secondary control regulation and cause instability across the network. In power systems existing research is centered around attack detection [25–30]. Attack detection and mitigation techniques are required that can prevent the attack on one part of the microgrid from causing instability across the network.

1.2 Outline

In this dissertation, distributed control algorithms and communication network are leveraged to provide a robust and resilient control structure for AC and DC microgrids. The dissertation is organized as follows:

1.2.1 Chapter 2: Distributed Noise-Resilient Synchrony of active distribution systems

1.2.1.1 Description

This chapter presents a journal paper accepted for publication in IEEE Transactions on Smart Grid. It proposes a distributed noise resilient control paradigm for voltage and frequency synchronization in inverter-based AC microgrids. Effect of noise in communi-

cation links between inverters on the synchronization process is studied. Distributed least mean-square is used to estimate the reference set point for secondary control. The proposed solution is evaluated using a modified IEEE 34-bus feeder system. An upper bound for the noise-induced deviation is analytically obtained and verified against the simulation results.

1.2.1.2 Individual Contribution

The author was the principal architect of the endeavor. The author identified the problem, theorized the solution, and executed the solution. Dr. Davoudi supervised the work and was involved from conceptualization to execution. Dr. Schizas provided insight into distributed estimation techniques and provided valuable input regarding the error bound derivation. Dr. Lewis provided valuable expertise regarding the distributed control formulation.

1.2.2 Chapter 3: Optimization-based AC microgrid synchronization

1.2.2.1 Description

This chapter presents a journal paper accepted for publication in IEEE Transactions on Industrial Informatics. The secondary control synchronization in inverter-based AC microgrids is cast as an optimization problem solved using Alternating Direction Method of Multipliers. The control and estimation problem are solved simultaneously. The proposed solution is evaluated using a modified IEEE 34-bus feeder system. An upper bound for the noise-induced deviation is analytically obtained and verified against the simulation results.

1.2.2.2 Individual Contribution

The author identified an avenue for a simplified distributed controller that solves an optimization problem. The author theorized an optimization based secondary controller

using Alternating Direction Method of Multipliers and executed the solution. Dr. Davoudi supervised the work and was involved from conceptualization to execution. Dr. Schizas provided insight into distributed estimation techniques and helped derive the error bound. Dr. Feresse provided valuable feedback and expertise regarding mean square error minimization in multi-agent systems.

1.2.3 Chapter 4: Synchrony in networked microgrids under attacks

1.2.3.1 Description

This chapter presents a journal paper accepted for publication in IEEE Transactions on Smart Grid. It proposes an attack-resilient distributed control for synchronization of inverter-based AC microgrids, by using an observed based control approach. A trust-based control protocol to mitigate attacks on communication links and hijacking of controllers is explored. The proposed solution is evaluated using a modified IEEE 34-bus feeder system.

1.2.3.2 Individual Contribution

The author conceptualized the problem, theorized the solution, and executed the solution. Dr. Davoudi supervised the work and was involved from conceptualization to execution. Dr. Modares provided insight into resilient distributed control of multi-agent systems, and provided valuable input regarding the proofs required to show vulnerability of distributed controllers to attack. Dr. Lewis provided valuable expertise regarding the distributed control formulation. Dr. Feresse provided valuable feedback and reviewed the work in detail during a presentation.

1.2.4 Chapter 4: Resilient cooperative control of DC microgrids

1.2.4.1 Description

This chapter presents a trust-based cooperative current sharing controller, that can mitigate adverse effects of attacks on communication links and hijacking controllers. The proposed controller is able to distinguish between attacks and change in loading conditions occurring naturally. The proposed solution is evaluated using Hardware in the Loop setup under different types of attack.

1.2.4.2 Individual Contribution

The author conceptualized the problem, theorized the solution, and executed the solution. Dr. Davoudi supervised the work and was involved from conceptualization to execution. Dr. Modares provided insight into resilient distributed control of multi-agent systems.

1.2.5 Chapter 5: Containment-based distributed control of DC microgrids

1.2.5.1 Description

This chapter presents a trust-based cooperative current sharing controller, that can mitigate adverse effects of attacks on communication links and hijacking controllers. The proposed controller is able to distinguish between attacks and change in loading conditions occurring naturally. The proposed solution is evaluated using Hardware in the Loop setup under different types of attack.

1.2.5.2 Individual Contribution

The author conceptualized the problem, theorized the solution, and executed the solution. Dr. Davoudi supervised the work and was involved from conceptualization to execution.

1.3 References

[1] Y. K. Chen, Y. C. Wu, C. C. Song, and Y. S. Chen, "Design and implementation of energy management system with fuzzy control for dc microgrid systems," *IEEE Trans. Power Electron.*, vol. 28, no. 4, pp. 1563–1570, Dec. 2013.

[2] D. Salomonsson, L. Soder, and A. Sannino, "An adaptive control system for a dc microgrid for data centers," *IEEE Trans. Ind. Appl.*, vol. 44, no. 6, pp. 1910–1917, Nov./Dec. 2008.

[3] D. Olivares, A. Mehrizi-Sani, A. Etemadi, C. Canizares, R. Iravani, M. Kazerani, A. Hajimiragha, O. Gomis-Bellmunt, M. Saeedifard, R. Palma-Behnke, G. Jimenez-Estevez, and N. Hatziargyriou, "Trends in microgrid control," *IEEE Trans. Smart Grid*, vol. 5, no. 4, pp. 1905–1919, July 2014.

[4] L. Che, M. Shahidehpour, A. Alabdulwahab, and Y. Al-Turki, "Hierarchical coordination of a community microgrid with AC and DC microgrids," *IEEE Trans. Smart Grid*, vol. 6, no. 6, pp. 3042–3051, Nov 2015.

[5] A. Bidram, A. Davoudi, F. Lewis, and Z. Qu, "Secondary control of microgrids based on distributed cooperative control of multi-agent systems," *IET Gener. Transmiss. Distrib.*, vol. 7, no. 8, pp. 822–831, Aug 2013.

[6] F. Dorfler, J. Simpson-Porco, and F. Bullo, "Breaking the hierarchy: Distributed control & economic optimality in microgrids," *IEEE Trans. Control Netw. Syst.*, 2015, to be published.

[7] P. Karlsson and J. Svensson, "Dc bus voltage control for a distributed power system," *IEEE Transactions on Power Electronics*, vol. 18, no. 6, pp. 1405–1412, Nov 2003.

[8] J. A. P. Lopes, C. L. Moreira, and A. G. Madureira, "Defining control strategies for microgrids islanded operation," *IEEE Transactions on Power Systems*, vol. 21, no. 2, pp. 916–924, May 2006.

[9] F. Guo, C. Wen, J. Mao, and Y. D. Song, "Distributed secondary voltage and frequency restoration control of droop-controlled inverter-based microgrids," *IEEE Trans. Ind. Electron.*, vol. 62, no. 7, pp. 4355–4364, July 2015.

[10] F. Guo, C. Wen, J. Mao, J. Chen, and Y.-D. Song, "Distributed cooperative secondary control for voltage unbalance compensation in an islanded microgrid," *IEEE Trans. Ind. Informat.*, vol. 11, no. 5, pp. 1078–1088, Oct 2015.

[11] A. Vaccaro, V. Loia, G. Formato, P. Wall, and V. Terzija, "A self-organizing architecture for decentralized smart microgrids synchronization, control, and monitoring," *IEEE Trans. Ind. Informat.*, vol. 11, no. 1, pp. 289–298, Feb 2015.

[12] M. Tahir and S. Mazumder, "Self-triggered communication enabled control of distributed generation in microgrids," *IEEE Trans. Ind. Informat.*, vol. 11, no. 2, pp. 441–449, April 2015.

[13] A. Bidram, A. Davoudi, and F. Lewis, "A multiobjective distributed control framework for islanded AC microgrids," *IEEE Trans. Ind. Informat.*, vol. 10, no. 3, pp. 1785–1798, Aug 2014.

[14] G. Wen, G. Hu, J. Hu, X. Shi, and G. Chen, "Frequency regulation of source-grid-load systems: A compound control strategy," *IEEE Trans. Ind. Informat.*, vol. 12, no. 1, pp. 69–78, Feb 2016.

[15] J. Schiffer, T. Seel, J. Raisch, and T. Sezi, "Voltage stability and reactive power sharing in inverter-based microgrids with consensus-based distributed voltage control," *IEEE Trans. Control Syst. Technol.*, vol. 24, no. 1, pp. 96–109, Jan 2016.

[16] J. Simpson-Porco, Q. Shafiee, F. Dorfler, J. Vasquez, J. Guerrero, and F. Bullo, "Secondary frequency and voltage control of islanded microgrids via distributed averaging," *IEEE Trans. Ind. Electron.*, vol. 62, no. 11, pp. 7025–7038, Nov 2015.

[17] Q. Shafiee, J. M. Guerrero, and J. C. Vasquez, "Distributed secondary control for islanded microgrids: A novel approach," *IEEE Trans. Power Electron.*, vol. 29, no. 2, pp. 1018–1031, Feb 2014.

[18] Q. Shafiee, C. Stefanovic, T. Dragicevic, P. Popovski, J. C. Vasquez, and J. M. Guerrero, "Robust networked control scheme for distributed secondary control of islanded microgrids," *IEEE Trans. Ind. Electron.*, vol. 61, no. 10, pp. 5363–5374, Oct 2014.

[19] Q. Shafiee, V. Nasirian, J. C. Vasquez, J. M. Guerrero, and A. Davoudi, "A multi-functional fully distributed control framework for ac microgrids," *IEEE Trans. Smart Grid*, 2016, to be published.

[20] V. C. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, and G. P. Hancke, "Smart grid technologies: Communication technologies and standards," *IEEE Trans. Ind. Informat.*, vol. 7, no. 4, pp. 529–539, Nov 2011.

[21] H. Meng, Y. L. Guan, and S. Chen, "Modeling and analysis of noise effects on broadband power-line communications," *IEEE Trans. Power Del.*, vol. 20, no. 2, pp. 630–637, April 2005.

[22] L. Xiao, S. Boyd, and S.-J. Kim, "Distributed average consensus with least-mean-square deviation," *J. Parallel Distrib. Comput.*, vol. 67, no. 1, pp. 33 – 46, Jan 2007.

[23] J. Slay and M. Miller, *Lessons Learned from the Maroochy Water Breach*. Boston, MA: Springer US, 2008, pp. 73–82.

[24] J. P. Farwell and R. Rohozinski, "Stuxnet and the future of cyber war," *Survival*, vol. 53, no. 1, pp. 23–40, 2011.

[25] F. Pasqualetti, A. Bicchi, and F. Bullo, "Consensus computation in unreliable networks: A system theoretic approach," *IEEE Trans. Autom. Control*, vol. 57, no. 1, pp. 90–104, Jan 2012.

[26] 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.

[27] 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.

[28] Y. Huang, J. Tang, Y. Cheng, H. Li, K. A. Campbell, and Z. Han, "Real-time 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.

[29] 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.

[30] 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, no. 2, pp. 612–621, March 2014.

CHAPTER 2

DISTRIBUTED NOISE-RESILIENT NETWORKED SYNCHRONY OF ACTIVE DISTRIBUTION SYSTEMS[1]

Authors: S. Abhinav, I. D. Schizas, F. Lewis, and A. Davoudi.

Reprinted, with permission from all the co-authors.

Journal: IEEE Transactions on Smart Grid (in press),

DOI: 10.1109/TSG.2016.2569602

[1]Used with permission of the publisher, 2017. In reference to IEEE copyrighted material which is used with permission in this thesis, the IEEE does not endorse any of the University of Texas at Arlington's (UTA) products or services. Internal or personal use of this material is permitted. If interested in reprinting/republishing IEEE copyrighted material for advertising or promotional purposes or for creating new collective works for resale or redistribution, please go to $http$: $//www.ieee.org/publications_standards/publications/rights/rights_link.html$ to learn how to obtain a License from RightsLink.

Distributed Noise-resilient Networked Synchrony of Active Distribution Systems

Shankar Abhinav, *Graduate Student Member, IEEE,*
Ioannis D. Schizas, *Member, IEEE* Frank L. Lewis, *Fellow, IEEE,*
and Ali Davoudi, *Senior Member, IEEE*

Abstract

This paper proposes a distributed noise resilient control technique for voltage and frequency synchronization in inverter-based AC microgrids. Existing cooperative control techniques assume ideal communication among inverters. The effect of additive noise in communication links among inverters, and between the reference signal and inverters, on the synchronization process, is studied. Distributed least mean-square solutions estimate the reference set points, and a local least mean-square algorithm estimates neighboring inverter frequencies and voltages. The efficacy of the proposed solution, for an islanded microgrid test system under the additive noise in reference communication links and links connecting neighboring inverters, is evaluated for a modified IEEE 34-bus feeder system. An upper bound for the noise-induced deviation in the consensus parameter is analytically derived and verified by the simulated testbed.

Index Terms

The work has been supported in part by the National Science Foundation under Grant ECCS-1405173, CCF-1218079, and by the U.S. Office of Naval Research under Grant N00014-14-1-0718.

Authors are with Electrical Engineering Department, the University of Texas at Arlington, TX 76019 USA (phone: 817-272-1374; fax: 817-272-2253; e-mail: (shankar.abhinav@mavs.uta.edu, schizas@uta.edu, lewis@uta.edu, and davoudi@uta.edu).

AC microgrids, cooperative control, distributed control, distributed estimation, noise, secondary control.

NOMENCLATURE

$\mathbf{A}$	Adjacency matrix of the communication graph.
$\mathbf{L}$	Laplacian matrix of the communication graph.
g_i	Pinning gain associate with inverter i.
$\mathbf{G}$	Diagonal matrix of pinning gains.
$\mathbf{x}_i$	State vector for dynamics of inverter i.
ω_i	Output frequency of inverter i.
V_i	Output voltage of inverter i.
ω_{ref}	Reference frequency.
v_{ref}	Reference voltage.
ω_{ni}	Frequency set point in droop control of inverter i.
V_{ni}	Voltage set point in droop control of inverter i.
e_{vi}	Voltage error term in cooperative secondary control for inverter i.
e_{ω_i}	Voltage error term in cooperative secondary control for inverter i.
r_{ref_i}	Noise in link between reference and inverter i.
r_{ij}	Noise in link between inverter i and inverter j.
$\bar{\omega}_{\text{ref},i}$	Local estimate of reference frequency at inverter i.
$\bar{\omega}_j$	Local estimate of inverter j frequency at inverter i.
$\mathbf{R}_i$	Noise parameter associated with the communication links in between inverters.
$\mathbf{R}_o$	Noise parameter associated with the communication links between inverters and the reference.
σ^2	Noise variance.

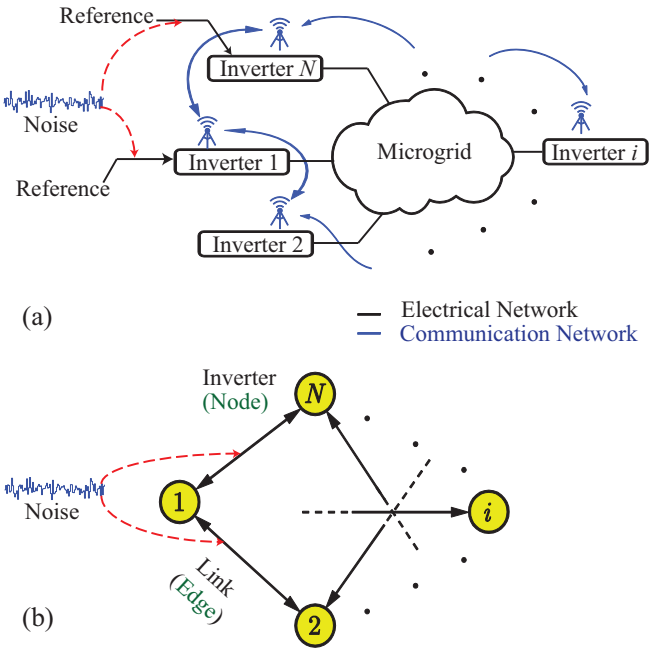

Fig. 1. Incorporating communication noise in distributed control of AC microgrids: a) Multi-inverter AC microgrids; b) Graphical representation of information exchange among inverters.

I. Introduction

Autonomous inverter-interfaced AC microgrids are finite-inertia power systems that are islanded (isolated) from the main grid. In a microgrid control hierarchy [1]–[3], the primary control maintains the inverter output voltage and frequency, usually through droop mechanisms at each inverter. The secondary control ensures synchrony of voltage and frequency variables among inverters by setting the set points for the primary control. The conventional centralized secondary control [4]–[6] requires point-to-point communication, exposes a single point-of-failure, and increases complexity. Alternatively, distributed control strategies are inspired by spatially-dispersed microgrids, and utilize a sparse communication network to exchange information among inverters [7]–[11], as seen in Fig. 1.

Existing distributed control paradigms assume an ideal, noise-free communication among inverters. In practice, the communication channels will be corrupted by addi-

tive noise [12]. For example, in wireless communications, an additive noise will be generated in the receiver front end and surrounding noise picked up by the antenna. Environmental causes, e.g., rain, can also introduce noise in to communication channels. The additive noise associated with electronic components and amplifiers at the receiver end is classified as thermal noise and statistically modeled as Gaussian in nature [12]. Without loss of generality, in this paper, noise is considered to be zero mean white Gaussian. Consensus on the desired set point is not warranted in the presence of noise [13]. Noise could especially disrupt the frequency synchronization. Given the nominal threshold of $\pm$ 0.05 Hz on frequency deviation [14], small deviation can adversely affect the sensitive electronics loads, while larger deviations can lead to circulating currents and, can potentially, destabilize the microgrid.

The effect of noise and distributed estimators for a noisy multi-agent system have been studied in [15], [16]. ADMM is an iterative algorithm to solve convex minimization problems that combines decomposability of dual descent with the faster convergence property of the method of multipliers. The distributed least mean-squares algorithm (DLMS) method is adopted in this paper in contrast to other distributed estimation approaches [17], [18], as it offers robustness and fast convergence rates, and relies on a single-hop communication among agents [19], [20]. The initial work of the authors in [21] had considered the communication noise only in the reference signal linked to the leader inverter (i.e., the pinned reference link). This paper generalizes the concept and considers additive communication noise in all the communication links among all inverters. The effect of additive communication noise is reduced by incorporating a distributed estimation technique in secondary cooperative control. It uses the same communication topology employed in the cooperative control for decentralized estimation in the presence of noisy data. The DLMS algorithm is used to estimate the reference set points, and a local LMS algorithm estimates the neighboring inverter frequency and

voltage.

This paper is organized as follows. Section II provides preliminaries of graph theory. Cooperative control of inverter-based microgrid are presented in Section III. In Section IV, a distributed scheme estimates the reference and neighbor's signals corrupted with an additive noise. An upper bound on the noise-induced deviation from the consensus value is obtained in section V. Case studies, using a 34-bus IEEE feeder network augmented with six inverters, are presented in Section VI. The conclusion is drawn in Section VII.

II. Preliminary of Graph Theory

The communication network among inverters $1, 2...N$ is represented by a graph $Gr = (O, E)$, as shown in Fig. 1(b). $O = \{o_1, o_2, ..., o_n\}$ is a set of n nodes or vertices corresponding to each inverter. E is a set of edges or arcs, where each edge from o_i to o_j is denoted by (o_i, o_j). N_i is the set of inverters providing information to inverter i, also referred to as its neighbors. The graph can be represented by an adjacency matrix $\mathbf{A} = [a_{ij}]$, with weights $a_{ij} > 0$ if $(o_i, o_j) \epsilon E$, otherwise $a_{ij} = 0$. The diagonal in-degree matrix is defined as $\mathbf{D} = \mathrm{diag}\{N_i\}$.

The graph Laplacian matrix, $\mathbf{L} = \mathbf{D} - \mathbf{A}$, includes distributed system properties, e.g., the convergence rate. A path from node i to node j is a sequence of edges $(o_i, o_k), (o_k, o_l), ..., (o_m, o_j)$. A graph is said to have a spanning tree, if there is a root node with a path from that node to every other node in the graph. If a graph has a spanning tree which implies that the communication graph is connected, the Laplacian matrix eigenvalue $\lambda_1 = 0$ is a simple eigenvalue [22]. The solution to $\mathrm{L}\boldsymbol{\omega} = \mathbf{0}$ can be written as $\boldsymbol{\omega} = c\underline{\mathbf{1}}$, where c is a constant. Thus, synchronization is guaranteed as long as the communication graph has a spanning tree.

A leader node can be connected to some nodes (at least to one root node) by unidirectional edges. The nodes connected to the leader node and the corresponding connecting edges are called pinned nodes and pinning edges, respectively. A gain is

assigned to each pinning edge, e.g., g_i is the pinning gain from the leader to the node i. The pinning gain is zero for an unpinned node. The pinning gain matrix is $\mathbf{G} = \mathrm{diag}\{g_i\}$.

III. Cooperative Control of AC Microgrids

A. Dynamic Modeling of Inverters

In this section, the nonlinear large-signal inverter model is explored. Moreover, preliminaries of cooperative control strategy for the secondary control of AC microgrids is presented, assuming ideal communication among inverters. This drawback is addressed in the next section. Figure 2 shows the block diagram of inverter-based AC microgrids. The dynamics of DC bus voltage and switching harmonics are usually neglected [23], [24]. The large-signal dynamical model of an inverter, with internal control loops, is adopted from [24]

$$\begin{cases} \dfrac{\mathrm{d}\mathbf{x}_i}{\mathrm{d}t} = f_i(x_i) + g(x_i)u_i \\ \mathbf{y}_i = h_i(x_i) \end{cases}, \tag{1}$$

where the state vector is

$$\mathbf{x}_i = \left[\delta_i, P_i, Q_i, \phi_{di}, \phi_{qi}, \gamma_{di}, \gamma_{qi}, i_{ldi}, i_{lqi}, v_{odi}, v_{oqi}, i_{odi}, i_{oqi}\right]. \tag{2}$$

The reference frame of one inverter is considered as the common reference frame ω_{com}. The angle of other inverters, ω, is found from

$$\frac{\mathrm{d}\delta_i}{\mathrm{d}t} = \omega - \omega_{\mathrm{com}}. \tag{3}$$

The inductive load dynamics are modeled as

$$\begin{cases} \frac{\mathrm{d}i_{load,d}}{\mathrm{d}t} = -\frac{R_{load}}{L_{load}} i_{load,d} + \omega i_{load,q} + \frac{1}{L_{load}} v_{bd} \\ \frac{\mathrm{d}i_{load,q}}{\mathrm{d}t} = -\frac{R_{load}}{L_{load}} i_{load,q} - \omega i_{load,d} + \frac{1}{L_{load}} v_{bq} \end{cases}. \tag{4}$$

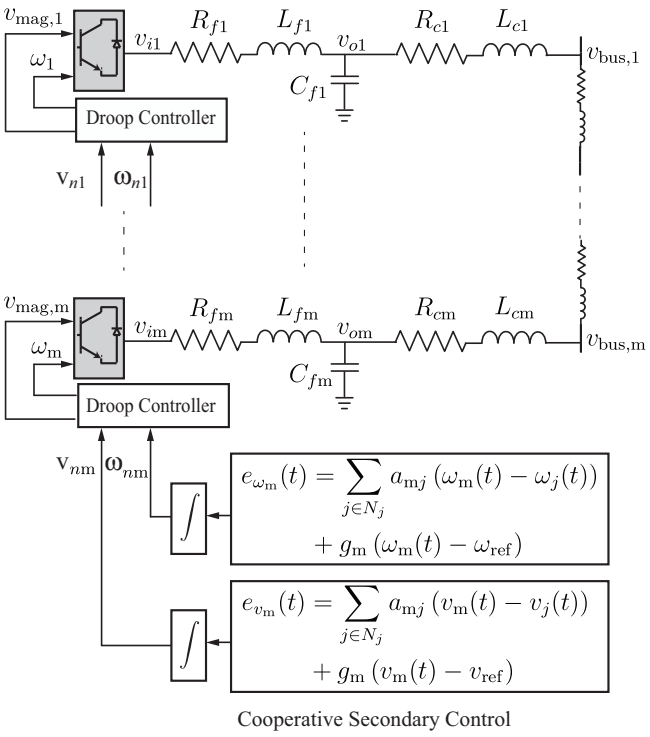

Fig. 2. Cooperative control of inverter-based microgrids.

The equations (1)-(3) represent the dynamic modeling of the inverter and inductive loads used for analysis and simulation purposes.

B. Cooperative Control of AC Microgrids

Decentralized droop techniques are conventionally employed for the primary control assuming inductive power distribution networks

$$\begin{cases} \omega_i = \omega_{ni} - m_{pi} P_i \\ v_{\mathrm{mag},i} = V_{ni} - n_{qi} Q_i \end{cases}, \tag{5}$$

where $v_{\mathrm{mag},i}$ and ω_i are the reference voltage and frequency provided for the internal control loops. ω_{ni} and V_{ni} are the set points for the primary control in (5). P_i and Q_i are the inverters' active and reactive powers. m_{pi} and n_{qi} are the droop coefficients evaluated based on the inverter ratings.

The secondary control provides ω_{ni} and V_{ni} in (5), to synchronize the terminal voltages and frequencies of each inverter to the reference values. This can be achieved by each inverter exchanging data only with its neighbors on a communication graph. The voltage error term is obtained by cooperation among inverters based on [9], [24] to update V_{ni}

$$e_{vi}(t) = \sum_{j \in N_i} \left(v_i(t) - v_j(t)\right) + g_i \left(v_i(t) - v_{\text{ref}}\right), \tag{6}$$

where v_i and v_j are the voltages of the inverters i and j, neighboring on the graph. To ensure consensus, some inverters are pinned with reference values. The pinning gain $g_i \geqslant 0$ is the weight of the edge connecting inverter i with the reference v_{ref}. Likewise, the cooperative frequency control law to update ω_{ni} based on [9], [24] is

$$e_{\omega_i}(t) = \sum_{j \in N_i} \left(\omega_i(t) - \omega_j(t)\right) + g_i \left(\omega_i(t) - \omega_{\text{ref}}\right), \tag{7}$$

where ω_i and ω_j are the frequencies of inverters i and j on the graph. The pinning gain is non-zero for the inverters connected to the reference frequency ω_{ref}. The overall block diagram of the distributed cooperative control is shown in Fig. 2. This cooperative secondary control ensures synchronization of inverter frequencies and output voltages to the reference set points, but assumes ideal communication and neglects the inevitable presence of noise in the communication channels.

IV. Distributed Noise Reduction

In this section, a fully distributed approach is proposed to estimate parameters communicated for the secondary control between the neighboring inverters, as well as the pinned inverters and the reference signals.

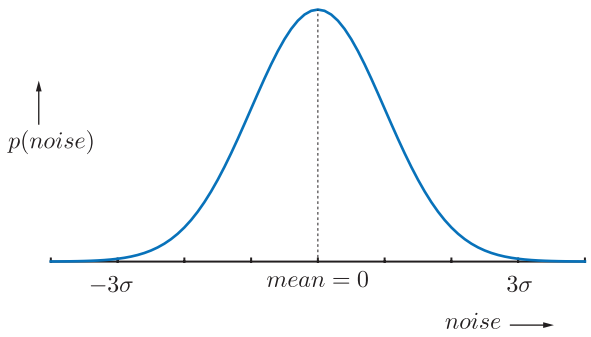

Fig. 3. Probability distribution function of noise (white gaussian).

A. *Communication Noise*

The pinning and communication links among inverters are assumed to be corrupted by noise that is zero-mean Gaussian. The probability distribution function of this noise signal with variance σ^2 is shown in Fig. 3 and given by

$$p(noise) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left(-\frac{noise^2}{2\sigma^2}\right). \tag{8}$$

The proposed algorithm is general and not restricted by the noise type. However, to streamline the analytics, the noise is considered to be zero-mean. Otherwise, methods such as sample averaging [25] can render the noise zero mean. The links between the pinned inverter i and the leader node has a zero-mean additive noise $r_{ref_i}(t)$, with a covariance $\mathrm{C}_{r_o} := \mathrm{E}[r_{\mathrm{ref},i}(t) r_{\mathrm{ref},i}(t)^T]$, received at inverter i. The corrupted reference frequency and voltage signals for the pinned inverters are

$$\begin{cases} \omega_{\mathrm{ref},i}(t) = \omega_{\mathrm{ref}} + r_{\mathrm{ref},i}(t) \\ v_{\mathrm{ref},i}(t) = v_{\mathrm{ref}} + r_{\mathrm{ref},i}(t). \end{cases} \tag{9}$$

The communication links among inverters have a zero-mean additive noise $r_{ij}(t)$, with a covariance $\mathrm{C}_{r_{ij}} := \mathrm{E}[r_{ij}(t) r_{ij}(t)^T]$, received at the inverter j from the inverter i. The corrupted reference frequency and voltage signals are

$$\begin{cases} \omega_{ij}(t) = \omega_i + r_{ij}(t) \\ v_{ij}(t) = v_i + r_{ij}(t). \end{cases} \tag{10}$$

B. Signal Estimation Under Noisy Communications

In presence of communication noise, synchronization of voltage and frequency terms might not be properly achieved. Fully-distributed estimation techniques [19], [20] are modified to address the presence of additive noise. The presence of noise in communicated frequency terms is considered; the same discussion can be extended to the voltage terms. The frequency reference set point is communicated to pinned inverters. These local reference set points $\omega_{\mathrm{ref},1}, \omega_{\mathrm{ref},2}, ..., \omega_{\mathrm{ref,N}}$ are corrupted by the additive noise. For synchronization of inverter frequencies, it is necessary to estimate the reference frequency set points from the corrupted local frequency set points using a LMS estimator. The centralized LMS estimator is given by

$$\begin{aligned} \hat{\omega}_{\mathrm{ref}}(t) &= \arg\min_{\bar{\omega}_{\mathrm{ref}}} \mathrm{E}[||\omega_{\mathrm{ref}}(t) - \bar{\omega}_{\mathrm{ref}}||^2] \\ &= \arg\min_{\bar{\omega}_{\mathrm{ref}}} \sum_{i=1}^{N} \mathrm{E}[(\omega_{\mathrm{ref},i}(t) - \bar{\omega}_{\mathrm{ref}})^2], \end{aligned} \tag{11}$$

where $\mathrm{E}[||\omega_{\mathrm{ref}}(t) - \bar{\omega}_{\mathrm{ref}}||^2]$ is the estimate of the mean-square error. The distorted and estimated reference frequencies are denoted by $\omega_{\mathrm{ref}}(t)$ and $\bar{\omega}_{\mathrm{ref}}$, respectively.

A distributed solution can be formulated, using local optimization and distributed implementation of (11). The global variable $\bar{\omega}_{\mathrm{ref}}$ is replaced by its local estimates $\bar{\omega}_{\mathrm{ref},1}, \bar{\omega}_{\mathrm{ref},2}, ..., \bar{\omega}_{\mathrm{ref,N}}$. A separable formulation, that adheres to the communication graph connectivity, is

$$\begin{aligned} \{\hat{\omega}_{\mathrm{ref},i}(t)\}_{i=1}^{N} = \arg\min_{\bar{\omega}_{\mathrm{ref},i}} & \sum_{i=1}^{N} \mathrm{E}[(\omega_{\mathrm{ref},i}(t) - \bar{\omega}_{\mathrm{ref},i})^2] \\ & \text{subject to } \bar{\omega}_{\mathrm{ref},i} = \bar{\omega}_{\mathrm{ref},j}, i \in N, j \in N_i \end{aligned} \tag{12}$$

where $\bar{\omega}_{\mathrm{ref},i}$ and $\bar{\omega}_{\mathrm{ref},j}$ are the local estimates of reference frequency at inverters i and j, respectively. If the communication graph is connected, the constraints $\bar{\omega}_{\mathrm{ref},i} = \bar{\omega}_{\mathrm{ref},j}$ in (12) impose consensus on the local reference frequency estimates. We solve (12) in a distributed manner using the Alternating Direction Method of Multipliers (ADMM) [26]. To facilitate application of ADMM, auxiliary variables s replace the constraints in (12) with

$$\bar{\omega}_{\mathrm{ref},i} = s_i \ ; \ \bar{\omega}_{\mathrm{ref},j} = s_j, i \in N, j \in N_i \tag{13}$$

Lagrange multipliers $[a, b] := a_i^j, b_i^j$, and the auxiliary variables, are used to form a quadratic Lagrangian function

$$\begin{aligned}\mathcal{L}[\bar{\omega}_{\mathrm{ref}}, s, a, b] &= \sum_{i=1}^{N} \mathrm{E}[(\omega_{\mathrm{ref},i}(t) - \bar{\omega}_{\mathrm{ref},i})^2] \\ &+ \sum_{i=1}^{N} \sum_{j \in N_i} \left[(a_i^j)^T(\bar{\omega}_{\mathrm{ref},i} - s_i) + (b_i^j)^T(\bar{\omega}_{\mathrm{ref},i} - s_j)\right] \\ &+ \sum_{i=1}^{N} \sum_{j \in N_i} \frac{c}{2} \left[||\bar{\omega}_{\mathrm{ref},i} - s_i||^2 + ||\bar{\omega}_{\mathrm{ref},i} - s_j||^2\right],\end{aligned} \tag{14}$$

where $c > 0$ is a penalty coefficient.

ADMM is an iterative process that updates the multipliers, local frequency estimates, and auxiliary variables at each time instant. It has been shown in [20] that auxiliary variables can be eliminated. The ADMM results in two updates of the Lagrange multipliers and the local reference frequency estimate, (15) and (16), at each time instant. Lagrange multipliers are

$$a_i^j(t) = a_i^j(t-1) + \frac{c}{2}\left(\bar{\omega}_{\mathrm{ref},i}(t) - \bar{\omega}_{\mathrm{ref},j}(t)\right). \tag{15}$$

The local reference frequency estimate, $\bar{\omega}_{\mathrm{ref,i}}$, is

$$\begin{aligned}\bar{\omega}_{\mathrm{ref},i}(t+1) = \underset{\bar{\omega}_{\mathrm{ref},i}}{\arg\min} \mathrm{E}[(\omega_{\mathrm{ref},i}(t) - \bar{\omega}_{\mathrm{ref},i})^2] \\ + \sum_{j \in N_j} \left(a_i^j(t) - a_j^i(t)\right) \bar{\omega}_{\mathrm{ref},i} \\ + c \sum_{j \in N_j} ||\bar{\omega}_{\mathrm{ref},i}(t) - \frac{1}{2}\left(\bar{\omega}_{\mathrm{ref},i}(t) + \bar{\omega}_{\mathrm{ref},j}(t)\right)||^2. \end{aligned} \tag{16}$$

The update of local reference frequency estimate, for every recursion, is

$$\begin{aligned}\bar{\omega}_{\mathrm{ref},i}(t+1) = \bar{\omega}_{\mathrm{ref},i}(t) + \mu[2\left(\omega_{\mathrm{ref},i}(t+1) - \bar{\omega}_{\mathrm{ref},i}(t)\right) \\ - \sum_{j \in N_j} \left(a_i^j(t) - a_j^i(t)\right) \\ - c \sum_{j \in N_j} \left(\bar{\omega}_{\mathrm{ref},i}(t) - \bar{\omega}_{\mathrm{ref},j}(t)\right)] \end{aligned} \tag{17}$$

where μ is the update step-size. The noise can be accounted for by incorporating communication noise η_i^j and $\bar{\eta}_i^j$, which corrupts the Lagrange multipliers and the local reference frequency estimates of the neighboring inverter, respectively. The Lagrange multiplier and local reference frequency estimate, in presence of communication noise, are given by (18), (19).

$$a_i^j(t) = a_i^j(t-1) + \frac{c}{2}\left(\bar{\omega}_{\mathrm{ref},i}(t) - \left(\bar{\omega}_{\mathrm{ref},j}(t) + \eta_i^j\right)\right) \tag{18}$$

$$\begin{aligned}\bar{\omega}_{\mathrm{ref},i}(t+1) = \bar{\omega}_{\mathrm{ref},i}(t) + \mu[2\left(\omega_{\mathrm{ref},i}(t+1) - \bar{\omega}_{\mathrm{ref},i}(t)\right) \\ - \sum_{j \in N_j} \left(a_i^j(t) - \left(a_j^i(t) + \bar{\eta}_i^j\right)\right) \\ - c \sum_{j \in N_j} \left(\bar{\omega}_{\mathrm{ref},i}(t) - \left(\bar{\omega}_{\mathrm{ref},j}(t) + \eta_i^j\right)\right)]. \end{aligned} \tag{19}$$

The DLMS algorithm to estimate the reference frequency has to find the local Lagrange

multiplier using (18), and update the local reference frequency estimate using (19). Each inverter communicates its reference frequency estimate and the Lagrange multiplier to its neighbors. The stability of DLMS algorithm has been studied in [20]. The local frequencies communicated to neighbors are corrupted due to the presence of noise in the neighboring communication links. A local LMS algorithm can estimate the frequencies of neighboring inverters at each inverter i. The distorted and estimated inverter frequencies are denoted by $\omega_j(t)$ and $\bar{\omega}_j$, respectively. The LMS estimator at every inverter i for the neighboring inverters $j \in N_i$ frequencies is obtained by minimizing

$$\hat{\omega}_j(t) = \arg\min_{\bar{\omega}_j} \mathrm{E}[||\omega_j(t) - \bar{\omega}_j||^2] \ \forall j \in N_i, \tag{20}$$

where $\mathrm{E}[||\omega_j(t) - \bar{\omega}_j||]$ is the mean-square error. The frequency estimate update, for every recursion, is

$$\bar{\omega}_j(t+1) = \bar{\omega}_j(t) + \mu\left(\omega_j(t+1) - \bar{\omega}_j(t)\right), \tag{21}$$

where μ is the step size for the updates. This approach is detailed in Algorithm 1. A similar algorithm can be used in tandem for the secondary control of inverter voltages.

Algorithm 1 Secondary Control Augmented with Estimation

Initialize $a_i^i(-1)$ and $\bar{\omega}_{\mathrm{ref},i}$
for $t = 0, 1...$ **do**
  Transmit $\bar{\omega}_{\mathrm{ref},i}(t)$ and $\omega_i(t)$ to neighbors
  Update $a_i^i(t)$ using (18)
  Transmit $a_i^i(t)$ to neighbors
  Update $\bar{\omega}_{\mathrm{ref},i}(t+1)$ using (19)
  Estimate $\bar{\omega}_j(t+1)$ using (21)
  Update $\omega_i(t+2)$ by substituting $\bar{\omega}_{\mathrm{ref},i}(t+1)$ and $\bar{\omega}_j(t+1)$ in place of $\omega_{\mathrm{ref}}(t)$ and $\omega_j(t)$ in (7)
end for

V. Noise-induced Bound on Frequency Deviation

To assess the robustness of the proposed method to additive noise levels in communication links, an upper error bound, on the deviation of local frequency estimates

---

$$
\begin{aligned}
||\mathbf{Error}(t+\Delta t)||^2 \leqslant & \,||\left(\mathbf{I}-\mathbf{T}\right)^t \boldsymbol{\omega}(0) + \sum_{k=0}^{t-1}\left(\mathbf{I}-\mathbf{T}\right)^t \mathbf{T}\boldsymbol{\omega}_{\mathrm{ref}_0} - \boldsymbol{\omega}_{\mathrm{ref}_0}||^2 \\
& + ||\sum_{k=0}^{t-1}\left(\mathbf{I}-\mathbf{T}\right)^k \Delta t \mathbf{R}_i(t-k\Delta t)|| + ||\sum_{k=0}^{t-1}\left(\mathbf{I}-\mathbf{T}\right)^k \Delta t \\
& \mathbf{R}_o(t-k\Delta t)||^2 + 2||\left(\mathbf{I}-\mathbf{T}\right)^t \boldsymbol{\omega}(0) + \sum_{k=0}^{t-1}\left(\mathbf{I}-\mathbf{T}\right)^t \mathbf{T}\boldsymbol{\omega}_{\mathrm{ref}_0} - \boldsymbol{\omega}_{\mathrm{ref}_0}|| \\
& ||\sum_{k=0}^{t-1}\left(\mathbf{I}-\mathbf{T}\right)^k \Delta t \mathbf{R}_i(t-k\Delta t)|| + 2||\left(\mathbf{I}-\mathbf{T}\right)^t \boldsymbol{\omega}(0) \\
& + \sum_{k=0}^{t-1}\left(\mathbf{I}-\mathbf{T}\right)^t \mathbf{T}\boldsymbol{\omega}_{\mathrm{ref}_0} - \boldsymbol{\omega}_{\mathrm{ref}_0}||||\sum_{k=0}^{t-1}\left(\mathbf{I}-\mathbf{T}\right)^k \Delta t \mathbf{R}_o(t-k\Delta t)|| \\
& + 2||\sum_{k=0}^{t-1}\left(\mathbf{I}-\mathbf{T}\right)^k \Delta t \mathbf{R}_i(t-k\Delta t)||||\sum_{k=0}^{t-1}\left(\mathbf{I}-\mathbf{T}\right)^k \Delta t \mathbf{R}_o(t-k\Delta t)||
\end{aligned}
\tag{26}
$$

$$
\begin{aligned}
\mathrm{E}[||\mathbf{Error}(t+\Delta t)||^2] \leqslant & \,||\left(\mathbf{I}-\mathbf{T}\right)^t \boldsymbol{\omega}(0) \\
& + \sum_{k=0}^{t-1}\left(\mathbf{I}-\mathbf{T}\right)^t \mathbf{T}\boldsymbol{\omega}_{\mathrm{ref}_0} - \boldsymbol{\omega}_{\mathrm{ref}_0}||^2 + ||\sum_{k=0}^{t-1}\left(\mathbf{I}-\mathbf{T}\right)^k \Delta t \mathbf{R}_{i,\max}||^2 \\
& + ||\sum_{k=0}^{t-1}\left(\mathbf{I}-\mathbf{T}\right)^k \Delta t \mathbf{R}_{o,\max}||^2 + 2||\left(\mathbf{I}-\mathbf{T}\right)^t \boldsymbol{\omega}(0) + \sum_{k=0}^{t-1}\left(\mathbf{I}-\mathbf{T}\right)^t \\
& \mathbf{T}\boldsymbol{\omega}_{\mathrm{ref}_0} - \boldsymbol{\omega}_{\mathrm{ref}_0}||||\sum_{k=0}^{t-1}\left(\mathbf{I}-\mathbf{T}\right)^k \Delta t \mathbf{R}_{i,\max}|| + 2||\left(\mathbf{I}-\mathbf{T}\right)^t \boldsymbol{\omega}(0) \\
& + \sum_{k=0}^{t-1}\left(\mathbf{I}-\mathbf{T}\right)^t \mathbf{T}\boldsymbol{\omega}_{\mathrm{ref}_0} - \boldsymbol{\omega}_{\mathrm{ref}_0}||||\sum_{k=0}^{t-1}\left(\mathbf{I}-\mathbf{T}\right)^k \Delta t \mathbf{R}_{o,\max}|| \\
& + 2||\sum_{k=0}^{t-1}\left(\mathbf{I}-\mathbf{T}\right)^k \Delta t \mathbf{R}_{i,\max}||||\sum_{k=0}^{t-1}\left(\mathbf{I}-\mathbf{T}\right)^k \Delta t \mathbf{R}_{o,\max}||
\end{aligned}
\tag{27}
$$

from their reference values, is derived. The error bound has been analytically derived a priori, to provide designer and operator with knowledge about the effect of noise prior to controller implementation and microgrid deployment. As a metric to measure error, we consider the mean-square error, $\mathrm{E}[||\boldsymbol{\omega}(t) - \boldsymbol{\omega}_{\mathrm{ref}}||^2]$, a standard performance index used in estimation.

The secondary cooperative frequency control, under additive noise in communication (and pinned reference) links, is

$$\dot{\omega}_i(t) = \sum_{j \in N_i} a_{ij} \left(\omega'_{ji}(t) - \omega_i(t)\right) + g_i \left(\omega'_{refi} - \omega_i(t)\right), \tag{22}$$

where $\omega'_{ji}(t) = \omega_j(t) + r_{ji}(t)$ and $\omega'_{refi}(t) = \omega_{ref_0}(t) + r_{\mathrm{ref},i}(t)$. $\omega_j(t)$ is the frequency of inverter j , ω_{ref_0} is the reference frequency, and $r_{ji}(t)$ and $r_{\mathrm{ref},i}(t)$ are noise components. Expanding (22), one has

$$\begin{aligned} \dot{\omega}_i(t) = & \sum_{j \in N_i} a_{ij} \left(\omega_j(t) - \omega_i(t)\right) + g_i \left(\omega_{ref_0} - \omega_i(t)\right) \\ & + \sum_{j \in N_i} a_{ij} r_{ji}(t) + g_i r_{\mathrm{ref},i}(t). \end{aligned} \tag{23}$$

This can be written in the vector form as

$$\dot{\boldsymbol{\omega}}(t) = -(\mathbf{L} + \mathbf{G})(\boldsymbol{\omega}(t) - \boldsymbol{\omega}_{\mathrm{ref}_0}) + \mathbf{R}_i(t) + \mathbf{R}_o(t), \tag{24}$$

where the graph Laplacian matrix is $\mathbf{L} = \mathbf{D} - \mathbf{A}$, and the diagonal matrix of pinning gains is $\mathbf{G} = \mathrm{diag}(g_i)$. $\mathbf{R}_i = [a_{ij} \times r_{ji}(t)]$ and $\mathbf{R}_o = [g_i \times r_{\mathrm{ref},i}(t)]$ contain the noise parameters and their associated adjacency and pinned gains. The inverter frequencies,

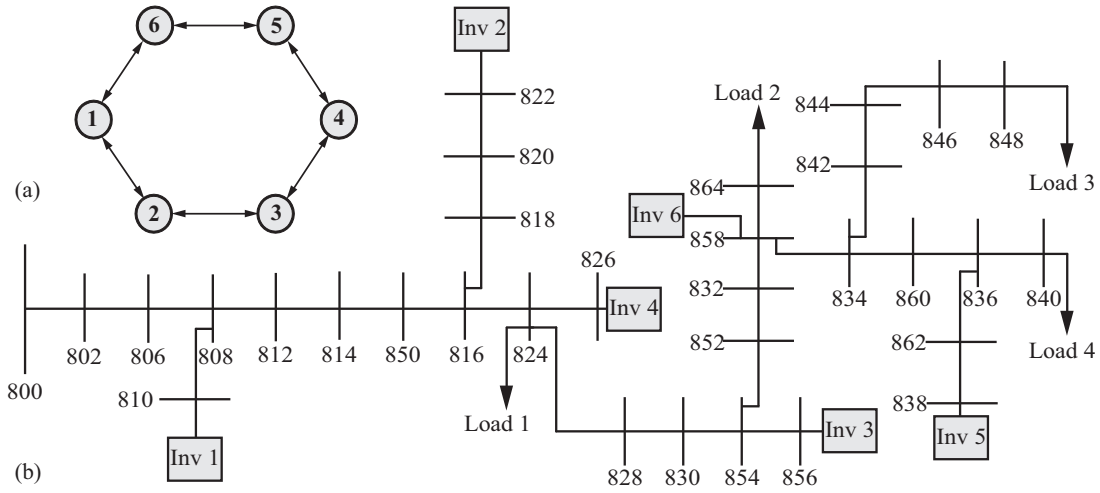

Fig. 4. (a) Topology of the communication network among inverters. (b) IEEE standard 34-bus feeder system augmented with six inverters.

at time $t + \Delta t$, is

$$\begin{aligned}\boldsymbol{\omega}(t+\Delta t) &= \boldsymbol{\omega}(t) + \Delta t[-\left(\mathbf{L}+\mathbf{G}\right)\left(\boldsymbol{\omega}(t) - \boldsymbol{\omega}_{\mathrm{ref}_0}\right) \\ &+ \mathbf{R}_i(t) + \mathbf{R}_o(t)] \\ &= \left[\mathbf{I} - \Delta t\left(\mathbf{L}+\mathbf{G}\right)\right]\boldsymbol{\omega}(t) + \Delta t\left(\mathbf{L}+\mathbf{G}\right)\boldsymbol{\omega}_{\mathrm{ref}_0} \\ &+ \Delta t\left[\mathbf{R}_i(t) + \mathbf{R}_o(t)\right]. \end{aligned} \tag{25}$$

To further simplify, let $\mathbf{T} = \Delta t\,(\mathbf{L} + \mathbf{G})$. By expanding (25), one has

$$\begin{aligned}
\boldsymbol{\omega}(t+\Delta t) &= (\mathbf{I}-\mathbf{T})\,\boldsymbol{\omega}(t) + \mathbf{T}\boldsymbol{\omega}_{\mathrm{ref}_0} + \Delta t\,[\mathbf{R}_i(t) + \mathbf{R}_o(t)] \\
&= (\mathbf{I}-\mathbf{T})^2\,\omega_{\mathbf{i}}(t-\Delta t) + (\mathbf{I}-\mathbf{T})\,\mathbf{T}\boldsymbol{\omega}_{\mathrm{ref}_0} \\
&+ (\mathbf{I}-\mathbf{T})\,\Delta t\,[\mathbf{R}_i(t-\Delta t) + \mathbf{R}_o(t-\Delta t)] \\
&+ \mathbf{T}\boldsymbol{\omega}_{\mathrm{ref}_0} + \Delta t\,[\mathbf{R}_i(t) + \mathbf{R}_o(t)] \\
&= (\mathbf{I}-\mathbf{T})^t\,\boldsymbol{\omega}(0) + \sum_{k=0}^{t-1}(\mathbf{I}-\mathbf{T})^t\,\mathbf{T}\boldsymbol{\omega}_{\mathrm{ref}_0} \\
&+ \sum_{k=0}^{t-1}(\mathbf{I}-\mathbf{T})^k\,\Delta t\,[\mathbf{R}_i(t-k\Delta t) + \mathbf{R}_o(t-k\Delta t)]\,. \qquad (28)
\end{aligned}$$

The control objective is to synchronize all the frequencies to the reference value. The frequency error is

$$\begin{aligned}
\mathbf{Error}(t+\Delta t) &= \boldsymbol{\omega}(t+\Delta t) - \boldsymbol{\omega}_{\mathrm{ref}_0} \\
&= (\mathbf{I}-\mathbf{T})^t\,\boldsymbol{\omega}(0) + \sum_{k=0}^{t-1}(\mathbf{I}-\mathbf{T})^t\,\mathbf{T}\boldsymbol{\omega}_{\mathrm{ref}_0} - \boldsymbol{\omega}_{\mathrm{ref}_0} \\
&+ \sum_{k=0}^{t-1}(\mathbf{I}-\mathbf{T})^k\,\Delta t\,[\mathbf{R}_i(t-k\Delta t) + \mathbf{R}_o(t-k\Delta t)]\,, \qquad (29)
\end{aligned}$$

where $\mathbf{T} = \Delta t\,(\mathbf{L} + \mathbf{G})$, the graph Laplacian matrix is $\mathbf{L} = \mathbf{D} - \mathbf{A}$, and the diagonal matrix of pinning gains is $\mathbf{G} = \mathrm{diag}(g_i)$. The vectors $\mathbf{R}_i = [a_{ij} \times r_{ji}(t)]$ and $\mathbf{R}_o = [g_i \times r_{\mathrm{ref},i}(t)]$ account for the system noise. Taking norm-two on both sides of (29) leads to

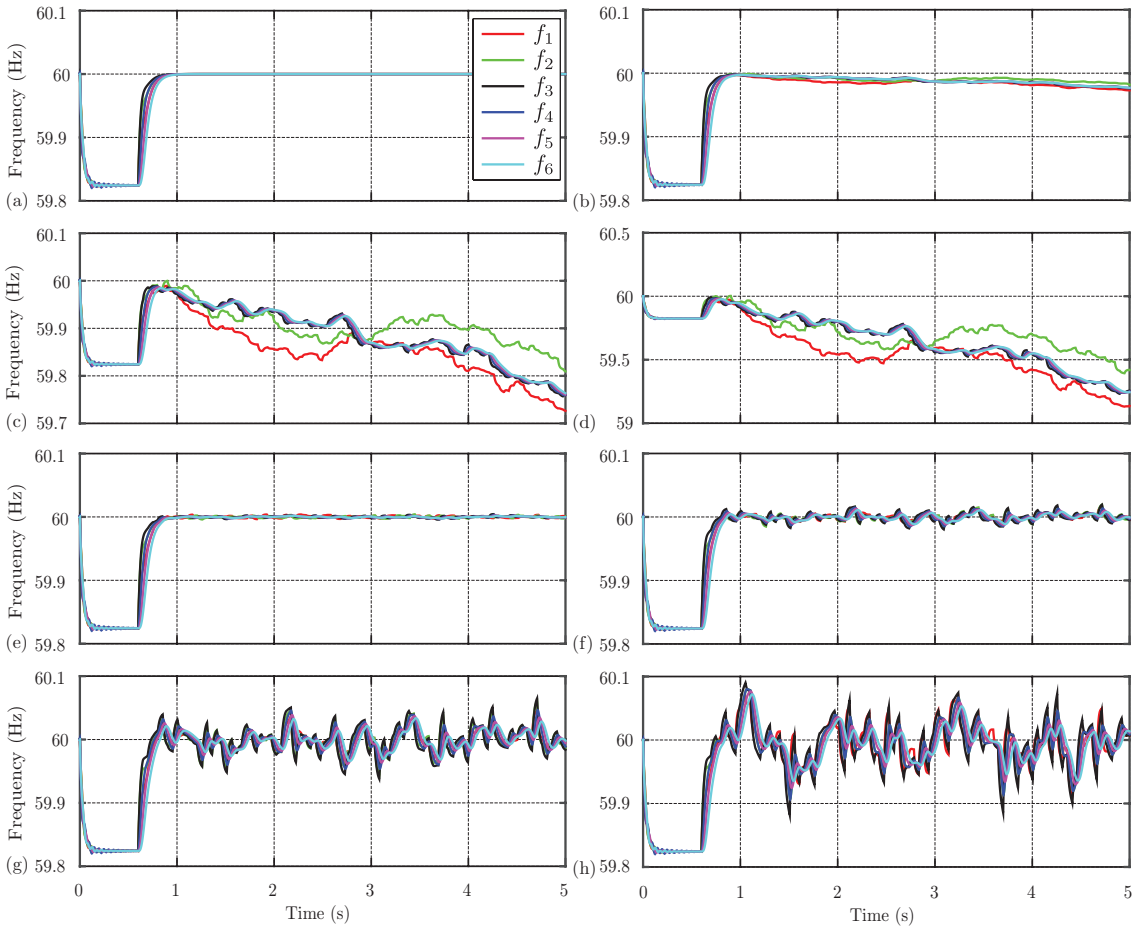

Fig. 5. Frequency synchronization in presence of noise: (a) Inverter frequencies under ideal conditions (no noise); (b) Inverter frequencies with noise $\sigma^2 = 10^{-4}$;(c) Inverter frequencies with noise $\sigma^2 = 10^{-2}$; (d) Inverter frequencies with noise $\sigma^2 = 0.1$; (e) Inverter frequencies with noise $\sigma^2 = 10^{-4}$ with DLMS algorithm; (f) Inverter frequencies with noise $\sigma^2 = 10^{-2}$ with DLMS algorithm; (g) Inverter frequencies with noise $\sigma^2 = 0.1$ with DLMS algorithm; (h) Inverter frequencies with noise $\sigma^2 = 0.1$ with DLMS algorithm, when the links between inverters 2 and 3 and the reference and inverter 2 fail.

$$
\begin{aligned}
||\mathbf{Error}(t+\Delta t)|| &= || \left(\mathbf{I}-\mathbf{T}\right)^t \boldsymbol{\omega}(0) + \sum_{k=0}^{t-1} \left(\mathbf{I}-\mathbf{T}\right)^t \mathbf{T}\boldsymbol{\omega}_{\mathrm{ref}_0} \\
&- \boldsymbol{\omega}_{\mathrm{ref}_0} + \sum_{k=0}^{t-1} \left(\mathbf{I}-\mathbf{T}\right)^k \Delta t \left[\mathbf{R}_i(t-k\Delta t) + \mathbf{R}_o(t-k\Delta t)\right] || \\
&\leqslant || \left(\mathbf{I}-\mathbf{T}\right)^t \boldsymbol{\omega}(0) + \sum_{k=0}^{t-1} \left(\mathbf{I}-\mathbf{T}\right)^t \mathbf{T}\boldsymbol{\omega}_{\mathrm{ref}_0} - \boldsymbol{\omega}_{\mathrm{ref}_0} || \\
&+ || \sum_{k=0}^{t-1} \left(\mathbf{I}-\mathbf{T}\right)^k \Delta t \mathbf{R}_i(t-k\Delta t) || \\
&+ || \sum_{k=0}^{t-1} \left(\mathbf{I}-\mathbf{T}\right)^k \Delta t \mathbf{R}_o(t-k\Delta t) ||. \qquad (30)
\end{aligned}
$$

By taking squares on both sides and expanding, we get (26). By considering expectation of the error, Since R_i and R_o are bounded and uncorrelated [20], the expectation of errors is given in (27). Taking the limit on both sides of (27) as $t \rightarrow \infty$, and since $\lim_{t\rightarrow\infty} (\mathbf{I} - \mathbf{T})^t = 0$ and $\lim_{t\rightarrow\infty} \sum_{k=0}^{t-1} (\mathbf{I} - \mathbf{T})^t \mathbf{T}\boldsymbol{\omega}_{\mathrm{ref}_0} = \boldsymbol{\omega}_{\mathrm{ref}_0}$, the mean-square deviation becomes

$$\begin{aligned}
&\lim_{t\rightarrow\infty} E[||\mathbf{Error}(t+\Delta t)||^2] \leqslant ||\mathbf{T}^{-1}\Delta t||^2 ||\mathbf{R}_{i,\max}||^2 \\
&+ ||\mathbf{T}^{-1}\Delta t||^2 ||\mathbf{R}_{o,\max}||^2 \\
&+ 2||\mathbf{T}^{-1}\Delta t|| ||\mathbf{R}_{i,\max}|| ||\mathbf{T}^{-1}\Delta t|| ||\mathbf{R}_{o,\max}||. \qquad (31)
\end{aligned}$$

The upper bound for $\mathbf{R}_{i,\max}$ can be obtained by using the maximum covariance of the noise associated with the neighboring communication links, $r_{i,\max}$, and weights of the adjacency matrix, $\mathbf{R}_{i,\max} = [a_{ij} \times r_{i,\max}]$. In a practical setting, the covariance can usually be estimated based on the data available for different communication strategies [27]–[29]. It can be shown that $\mathbf{R}_o$ is bounded ([20]-section 5.2). The expression for the upper bound of mean-square deviation for the DLMS algorithm, $\mathbf{R}_{o,\max}$, can be obtained similarly [20]. The upper bound on voltage error cannot be similarly defined since, as opposed to the frequency being a global variable which is consistent throughout the microgrid, inverter voltages should be different to allow reactive power sharing [9].

VI. Case Studies

The performance of the proposed control method is evaluated for different noise levels in a communication network of an islanded microgrid. Figure 4 illustrates a single-line diagram of a modified 34-bus test feeder [30], augmented with six inverters. The feeder is connected to the main grid at bus 800. The feeder is converted to a balanced feeder by averaging the line parameters given in [30]. The load impedances are load 1 : $1.5 + j1\ \Omega$, load 2 : $0.5 + j0.5\ \Omega$, load 3 : $1 + j1\ \Omega$, and load 4 :

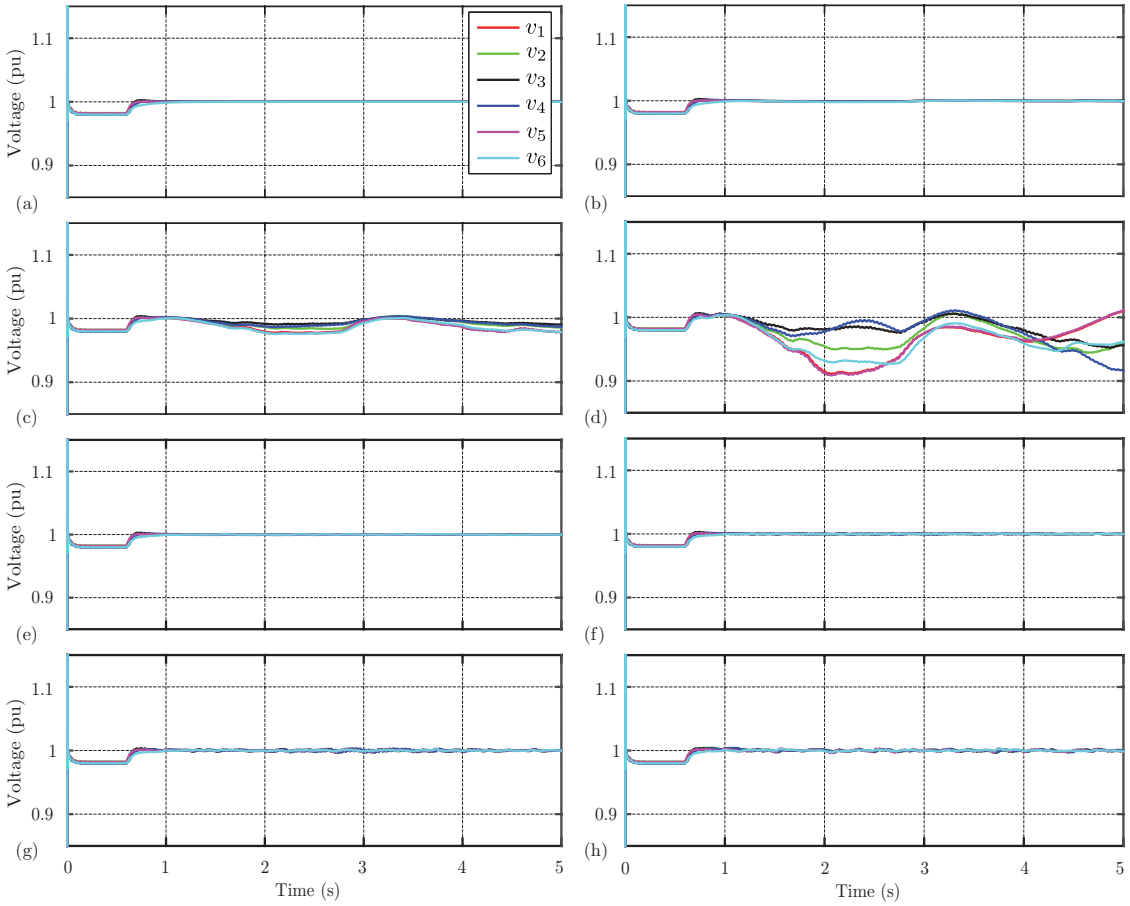

Fig. 6. Voltage synchronization in the presence of noise: (a) Inverter output voltage under ideal conditions (no noise); (b) Inverter output voltage with noise $\sigma^2 = 10^{-4}$;(c) Inverter output voltage with noise $\sigma^2 = 10^{-2}$; (d) Inverter output voltage with noise $\sigma^2 = 0.1$; (e) Inverter output voltage with noise $\sigma^2 = 10^{-4}$ with DLMS algorithm; (f) Inverter output voltage with noise $\sigma^2 = 10^{-2}$ with DLMS algorithm; (g) Inverter output voltage with noise $\sigma^2 = 0.1$ with DLMS algorithm; (h) Inverter output voltage with noise $\sigma^2 = 10^{-2}$ with DLMS algorithm, when the link failure occurs between inverter 2 and 3, and between the reference and inverter 2.

$0.8 + j0.8\ \Omega$. The inverter specifications are given in the Appendix. Each inverter is modeled by a 13-order dynamic system as described in (2), and the secondary control is implemented, in a distributed fashion, using (6) and (7). Loads have been modeled using a second-order dynamic model in (4). The nominal frequency and line-to-line voltage are 60 Hz and 24.9 kV, respectively. The inverters are connected to the feeder through Y-Y 480V/24.9 kV, 400 kVA transformers with a series impedance of $0.03 + j0.12$ p.u. Each inverter can communicate only with other inverters neighboring on a communication

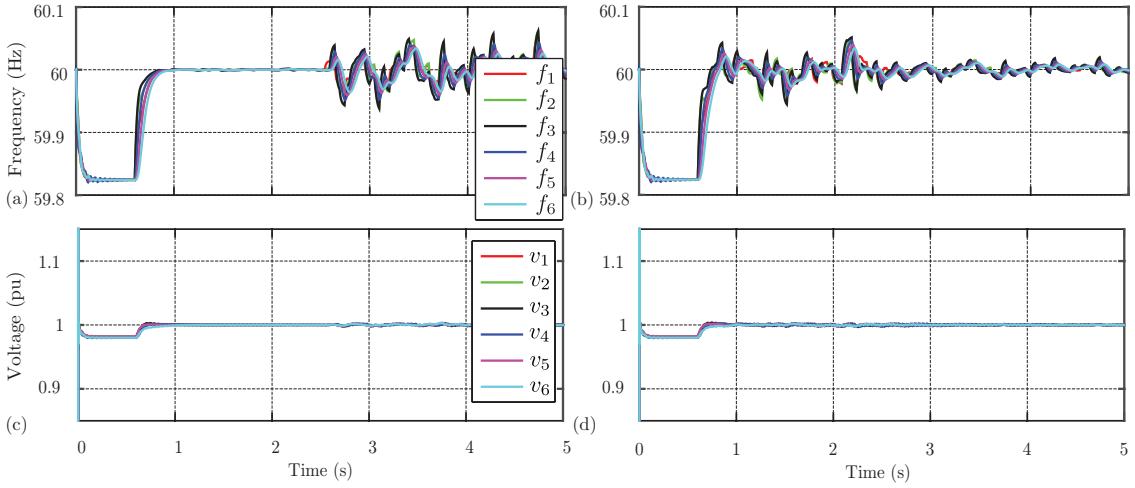

Fig. 7. Synchronization in the presence of varying noise levels: (a) Inverter frequencies when noise changes from $\sigma^2 = 10^{-4}$ to $\sigma^2 = 0.1$ at $t = 2.5$ s with DLMS algorithm ; (b) Inverter frequencies when noise changes from $\sigma^2 = 0.1$ to $\sigma^2 = 10^{-2}$ at $t = 2.5$ s with DLMS algorithm ; (c) Inverter output voltage when noise changes from $\sigma^2 = 10^{-4}$ to $\sigma^2 = 0.1$ at $t = 2.5$ s with DLMS algorithm ; (d) Inverter output voltage when noise changes from $\sigma^2 = 0.1$ to $\sigma^2 = 10^{-2}$ at $t = 2.5$ s with DLMS algorithm.

graph as shown in Fig. 4(a). Each inverter communicates its frequency, output voltage, estimated reference frequency, estimated reference voltage, and Lagrange multipliers to its neighbors. Inverters 1, 2, and 3 are pinned (receive reference signal) with pinning gains $g_1 = g_2 = g_3 = 1$. It is assumed that the noise in neighboring communication links and pinned reference links are the same.

The reference frequency and voltage for the secondary control are set to 60 Hz and 1 p.u, respectively. The test feeder is islanded from the main grid at $t = 0$ s. The cooperative secondary control is intentionally activated at $t = 0.7$ s. Under ideal conditions (no noise in the reference signal), as seen in Fig. 5(a) and Fig. 6(a), the frequency and voltage synchronize to the desired levels of $f = 60$ Hz and $V = 1$ p.u., respectively. Figures 5(b) and 5(c) show when reference links and communication links include noise with $\sigma^2 = 10^{-4}$ (variance) and $\sigma^2 = 10^{-2}$ respectively, the inverter frequencies do not synchronize in Fig. 5(c). The variance of $\sigma^2 = 10^{-2}$ implies a deviation of ± 0.3Hz ($\pm 3\sigma$) in the frequency communicated. When the reference and

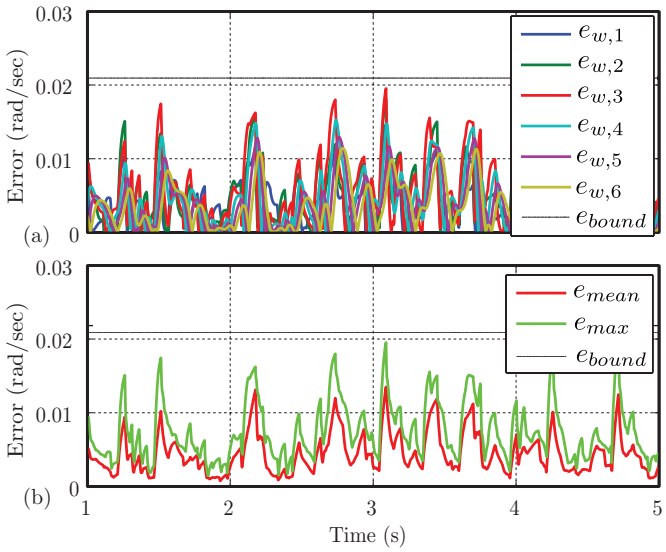

Fig. 8. Error levels in frequency terms: (a) Error in inverter frequencies with noise $\sigma^2 = 10^{-2}$; (b) Maximum and mean error with noise $\sigma^2 = 10^{-2}$. The theoretical upper error bound for the associated noise level is shown.

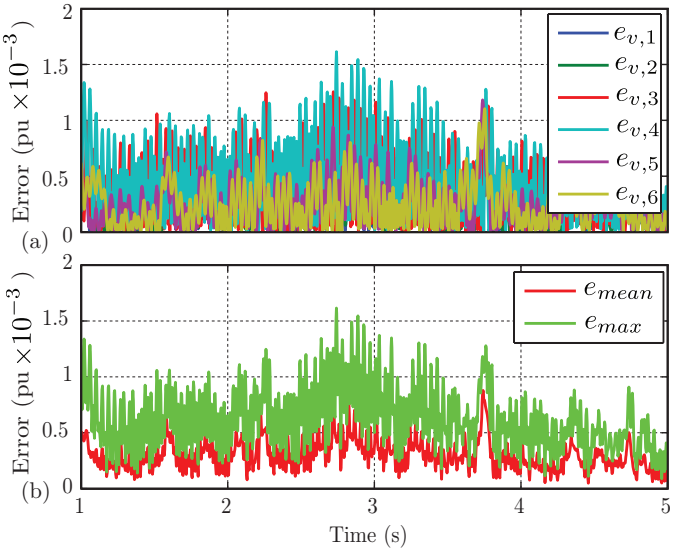

Fig. 9. Error levels in voltage terms: (a) Error in inverter's voltage with noise $\sigma^2 = 10^{-2}$; (b) Maximum and mean error with noise $\sigma^2 = 10^{-2}$.

communication links are corrupted with noises with $\sigma^2 = 0.1$, as seen in Fig. 5(d), the distortion in inverter frequencies increases even further.

Secondary frequency control is augmented with estimation as described in Algorithm 1, with $\mu = 0.05$. A similar strategy is adopted for the secondary voltage control. The

inverter frequencies, when embedded DLMS algorithms are considered in the secondary control, are shown in Figs. 5(e), (f), and (g) for noise levels of $\sigma^2 = 10^{-4}$, $\sigma^2 = 10^{-2}$, and $\sigma^2 = 0.1$, respectively. The inverter voltages are shown in Figs. 6(e), (f), and (g) for the noise levels of $\sigma^2 = 10^{-4}$, $\sigma^2 = 10^{-2}$, and $\sigma^2 = 0.1$, respectively. The inverter frequencies and voltages are synchronized within acceptable limits for the different noise levels. This is less effective for increased noise levels but, even for the noise level of $\sigma^2 = 0.1$, the frequencies and voltages are still within an acceptable range.

The performance of the proposed control algorithm augmented with estimation is studied under a link failure scenario in Figs. 5(h) and 6(h) with functioning links corrupted with noise signals with $\sigma^2 = 0.1$. Figures 5(h) and 6(h) show the output frequency and voltage when the link between inverters 2 and 3, and the link between the reference and inverter 2, fail. It can be seen that frequency and voltage terms synchronize given the presence of spanning tree in the communication graph topology, but the error due to noise is elevated but within acceptable limits. The controller performance, under various noise conditions, is studied in Fig. 7. Figures 7(a) and 7(c) show the output frequency and voltage when corrupted with noises with $\sigma^2 = 10^{-4}$ (variance) for $t < 2.5$ s, and $\sigma^2 = 0.1$ (variance) for $t > 2.5$ s. Figures 7(b) and 7(d) show the output frequency and voltage when corrupted with noises with $\sigma^2 = 0.1$ (variance) for $t < 2.5$ s, and $\sigma^2 = 10^{-2}$ (variance) for $t > 2.5$ s.

The upper error bound in frequency is calculated with noise levels of $\sigma^2 = 10^{-2}$ in the reference and neighboring communication links. It is shown in Fig. 8 that the error in frequency obtained for each individual inverter is within the error bound derived in Section V. The microgrid system is simulated with 100 Monte Carlo runs and the error observed in frequencies is compared with the upper error bound in Fig. 8. The algorithm robustness can also be inferred as even with a variance $\sigma^2 = 10^{-2}$ indicating a deviation of ± 0.3Hz, while the error is less than 0.03. The upper bound of voltage

error cannot be similarly defined, as inverter voltages should be inherently different to ensure reactive power sharing. As seen from Fig. 9, the voltage deviations are also low. The error in voltage and frequency for a noise level of $\sigma^2 = 10^{-2}$, observed in Figs. 6 and 8, respectively, is low and permissible in a practical scenario.

VII. Conclusion

This paper explores the noise-resilient synchronization of multi-inverter AC microgrids. The effect of different noise levels in the communication links on the secondary control of inverter frequency and voltage is evaluated. The performance of distributed noise reduction technique is evaluated for different noise levels in reference communication links and links connecting neighboring inverters. An expression for the upper error bound, due to the noise corruption, is derived. Error bound less than 0.03Hz for the communication noise deviation up to $\pm 0.3\text{Hz}$ is verified using a modified 34-bus IEEE feeder test system.

Appendix

TABLE I
Inverter Specifications

	Inverter 1,2,4&5		**Inverter 3&6**	
Output Connector	R_c	0.03Ω	R_c	0.03Ω
	L_c	$0.35mH$	R_c	0.35mH
LC Filter	R_f	0.1Ω	R_f	0.1Ω
	L_f	1.35mH	L_f	1.35mH
	C_f	$50\mu\text{F}$	C_f	$50\mu\text{F}$

References

[1] A. Bidram and A. Davoudi, "Hierarchical structure of microgrids control system," *IEEE Transactions on Smart Grid*, vol. 3, no. 4, pp. 1963–1976, Dec 2012.

TABLE II
CONTROLLER SPECIFICATIONS

	Inverter 1,2,4&5		**Inverter 3&6**	
Droop Gains	m_p	5.64×10^{-5}	m_p	7.5×10^{-5}
	n_q	5.2×10^{-4}	n_q	6×10^{-4}

[2] D. Olivares, A. Mehrizi-Sani, A. Etemadi, C. Canizares, R. Iravani, M. Kazerani, A. Hajimiragha, O. Gomis-Bellmunt, M. Saeedifard, R. Palma-Behnke, G. Jimenez-Estevez, and N. Hatziargyriou, "Trends in microgrid control," *IEEE Transactions on Smart Grid*, vol. 5, no. 4, pp. 1905–1919, July 2014.

[3] L. Che, M. Shahidehpour, A. Alabdulwahab, and Y. Al-Turki, "Hierarchical coordination of a community microgrid with AC and DC microgrids," *IEEE Transactions on Smart Grid*, vol. 6, no. 6, pp. 3042–3051, Nov 2015.

[4] M. Savaghebi, A. Jalilian, J. Vasquez, and J. Guerrero, "Secondary control scheme for voltage unbalance compensation in an islanded droop-controlled microgrid," *IEEE Transactions on Smart Grid*, vol. 3, no. 2, pp. 797–807, June 2012.

[5] A. Mehrizi-Sani and R. Iravani, "Constrained potential function-based control of microgrids for improved dynamic performance," *IEEE Transactions on Smart Grid*, vol. 3, no. 4, pp. 1885–1892, Dec 2012.

[6] C. Ahumada, R. Cardenas, D. Saez, and J. Guerrero, "Secondary control strategies for frequency restoration in islanded microgrids with consideration of communication delays," *IEEE Transactions on Smart Grid*, 2015, to be published.

[7] S. Cady, A. Dominguez-Garcia, and C. Hadjicostis, "A distributed generation control architecture for islanded AC microgrids," *IEEE Transactions on Control Systems Technology*, vol. 23, no. 5, pp. 1717–1735, Sept 2015.

[8] A. Bidram, A. Davoudi, F. Lewis, and J. Guerrero, "Distributed cooperative secondary control of microgrids using feedback linearization," *IEEE Transactions on Power Systems*, vol. 28, no. 3, pp. 3462–3470, Aug 2013.

[9] J. Simpson-Porco, Q. Shafiee, F. Dorfler, J. Vasquez, J. Guerrero, and F. Bullo, "Secondary frequency and voltage control of islanded microgrids via distributed averaging," *IEEE Transactions on Industrial Electronics*, vol. 62, no. 11, pp. 7025–7038, Nov 2015.

[10] J. Schiffer, T. Seel, J. Raisch, and T. Sezi, "Voltage stability and reactive power sharing in inverter-based microgrids with consensus-based distributed voltage control," *IEEE Transactions on Control Systems Technology*, 2015, to be published.

[11] F. Dorfler, J. Simpson-Porco, and F. Bullo, "Breaking the hierarchy: Distributed control & economic optimality in microgrids," *IEEE Transactions on Control of Network Systems*, 2015, to be published.

[12] J. G. Proakis, *Digital Communications*. New York: McGraw-Hill, 1995.

[13] L. Xiao, S. Boyd, and S.-J. Kim, "Distributed average consensus with least-mean-square deviation," *Journal*

of Parallel and Distributed Computing, vol. 67, no. 1, pp. 33 – 46, Jan 2007.

[14] M. A. Hanley, "Frequency instability problems in north american interconnections," National Energy Technology Laboratory Report, Tech. Rep. DOE/NETL-2011/1473, May 2011.

[15] J. Hu and G. Feng, "Distributed tracking control of leader-follower multi-agent systems under noisy measurement," *Automatica*, vol. 46, no. 8, pp. 1382 – 1387, Aug 2010.

[16] Y. Hong, G. Chen, and L. Bushnell, "Distributed observers design for leader-following control of multi-agent networks," *Automatica*, vol. 44, no. 3, pp. 846 – 850, March 2008.

[17] L. Xiao and S. Boyd, "Fast linear iterations for distributed averaging," *Systems & Control Letters*, vol. 53, no. 1, pp. 65 – 78, Sep 2004.

[18] F. Cattivelli and A. Sayed, "Diffusion LMS strategies for distributed estimation," *IEEE Transactions on Signal Processing*, vol. 58, no. 3, pp. 1035–1048, March 2010.

[19] I. Schizas, G. Giannakis, S. Roumeliotis, and A. Ribeiro, "Consensus in ad hoc wsns with noisy links Part II: Distributed estimation and smoothing of random signals," *IEEE Transactions on Signal Processing*, vol. 56, no. 4, pp. 1650–1666, April 2008.

[20] G. Mateos, I. D. Schizas, and G. B. Giannakis, "Performance analysis of the consensus-based distributed LMS algorithm," *EURASIP Journal on Advances in Signal Processing*, vol. 2009, no. 68, pp. 1–19, 2009.

[21] S. Abhinav, I. Schizas, and A. Davoudi, "Noise-resilient synchrony of AC microgrids," in *Resilience Week (RWS)*, 2015, pp. 1–6.

[22] R. Olfati-Saber and R. Murray, "Consensus problems in networks of agents with switching topology and time-delays," *IEEE Transactions on Automatic Control*, vol. 49, no. 9, pp. 1520–1533, Sept 2004.

[23] N. Pogaku, M. Prodanovic, and T. Green, "Modeling, analysis and testing of autonomous operation of an inverter-based microgrid," *IEEE Transactions on Power Electronics*, vol. 22, no. 2, pp. 613–625, March 2007.

[24] A. Bidram, F. Lewis, and A. Davoudi, "Distributed control systems for small-scale power networks: Using multiagent cooperative control theory," *IEEE Control Systems*, vol. 34, no. 6, pp. 56–77, Dec 2014.

[25] R. G. Gallager, *Principles of digital communication*. Cambridge University Press, 2008.

[26] D. P. Bertsekas and J. N. Tsitsiklis, *Parallel and Distributed Computation: Numerical Methods*. Prentice-Hall, Inc., 1989.

[27] T. T. Cai, C.-H. Zhang, H. H. Zhou *et al.*, "Optimal rates of convergence for covariance matrix estimation," *Ann. Stat.*, vol. 38, no. 4, pp. 2118–2144, 2010.

[28] G. A. M. M. and G. L. Stuber, "Joint EM channel and covariance estimation with sufficient-statistic chip combining for a SIMO MC-CDMA antijam system," in *Proc. IEEE Wireless Commun. Netw.*, Las Vegas, NV, USA, March 2008, pp. 1131–1136.

[29] E. Conte, A. D. Maio, and G. Ricci, "Recursive estimation of the covariance matrix of a compound-gaussian process and its application to adaptive CFAR detection," *IEEE Trans. Signal Process.*, vol. 50, no. 8, pp. 1908–1915, Aug 2002.

[30] N. Mwakabuta and A. Sekar, "Comparative study of the IEEE 34 node test feeder under practical simplifications," in *39th North American Power Symposium*, 2007, pp. 484–491.

CHAPTER 3

OPTIMIZATION-BASED AC MICROGRID SYNCHRONIZATION[1]

Authors: S. Abhinav, I. D. Schizas, F. Ferrese, and A. Davoudi.

Reprinted, with permission from all the co-authors.

Journal: IEEE Transactions on Industrial Informatics (in press),

DOI: 10.1109/TII.2017.2702623

[1]Used with permission of the publisher, 2017. In reference to IEEE copyrighted material which is used with permission in this thesis, the IEEE does not endorse any of the University of Texas at Arlington's (UTA) products or services. Internal or personal use of this material is permitted. If interested in reprinting/republishing IEEE copyrighted material for advertising or promotional purposes or for creating new collective works for resale or redistribution, please go to $http$: $//www.ieee.org/publications_standards/publications/rights/rights_link.html$ to learn how to obtain a License from RightsLink.

Optimization-based AC Microgrid Synchronization

Shankar Abhinav, *Graduate Student Member, IEEE,*
Ioannis D. Schizas, *Member, IEEE* Frank Ferrese, *Senior Member, IEEE,*
and Ali Davoudi, *Senior Member, IEEE*

Abstract

This paper casts the synchronization phenomena in inverter-based AC microgrids as an optimization problem solved using Alternating Direction Method of Multipliers (ADMM). Existing cooperative control techniques are based on the standard voting protocols in multi-agent systems, and assume ideal communication among inverters. Alternatively, this paper presents a recursive algorithm to restore synchronization in voltage and frequency using ADMM, which results in a more robust secondary control even in the presence of noise. The performance of the control algorithm, for an islanded microgrid test system with additive noise in communication links broadcasting reference signals and communication links connecting neighboring inverters, is evaluated for a modified IEEE 34-bus feeder system. An upper bound for the deviation due to communication noise from the reference set point is analytically derived and verified by the simulated microgrid test system.

Index Terms

This material is based upon research supported in part by the U.S. Office of Naval Research under award number N00014-14-1-0718, and by the National Science Foundation under Grant ECCS-1405173.

S. Abhinav, I. D. Schizas, and A. Davoudi are with Electrical Engineering Department, the University of Texas at Arlington, TX 76019 USA (e-mail: {shankar.abhinav, schizas, davoudi}@uta.edu).

F. Ferrese is with the Naval Surface Warfare Center, Philadelphia, PA 19112 USA (e-mail: frank.ferrese@navy.mil).

AC microgrids, distributed control, distributed estimation, noise, optimization, secondary control.

I. Introduction

In the control hierarchy of multi-inverter AC microgrids [1], [2], the primary control maintains the inverter output voltage and frequency, usually through droop mechanisms. The secondary control ensures inverters' synchrony by providing the setpoints for droop controllers in the primary layer [3]. The tertiary controller solves the optimal power flow [4], and provides the optimal set-point for the secondary controller. In [5], model-predictive control has been used for centralized secondary frequency control. The latest secondary control paradigms are focused on the distributed control of networked microgrids (Fig. 1) [3], [6]–[16], where inverters exchange information on a sparse communication network, and assume an ideal, noise-free communication. Such network-centric approaches rely heavily on the communication among inverters, and are vulnerable to link fallacies such as additive noise and link failure.

Some communication technologies, such as Zigbee and power line communication [17], [18], can be corrupted by noise in a harsh microgrid environment. The noise in communication links is associated with electronic components and amplifiers at the receiver end (e.g., thermal noise [19]). In [20], the effect of uncertainty due to noise in automatic generation control has been explored. Automatic generation control of the legacy grid is analogous to the secondary control of inverters in microgrids. Destabilizing effects of communication noise on microgrids have been studied in [21]. Synchronization to the desired setpoints, using neighbor-based voting protocols, cannot be guaranteed in the presence of noise [22]. On the other hand, these neighbor-based consensus protocols are essential to existing distributed secondary control paradigms [3], [10]–[16]. While the effect of communication delay on distributed control of microgrids

has been investigated [14]–[16], [23], robust distributed secondary control methods are warranted to mitigate the effect of communication noise.

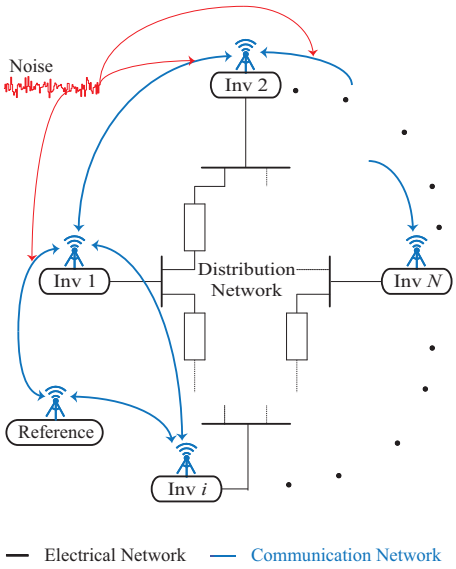

Fig. 1. Inverter-populated networked AC microgrids with communication noise.

In this paper, the secondary-level synchronization objective is cast as a constrained optimization problem, and solved in a distributed fashion by using Alternating Direction Method of Multipliers (ADMM). ADMM is an iterative algorithm to solve convex minimization problems that combines decomposability of dual descent with the faster convergence property of the method multipliers [24]. The synchronization objective is split into minimizing the estimated error between the reference frequency/voltage and the inverter frequency/voltage, while subjected to the constraint that the inverter frequency/voltage must be equal to the neighboring inverter frequencies/voltages. Inverters communicate on a sparse, and non-ideal, communication network. The salient contribution of the paper are:

- The control formulation is fully distributed and inherently robust to noise. In contrast to the existing average consensus methods [10], the controller formulation includes higher-order terms that makes it more robust to disturbances.

- An upper bound for the noise-induced deviation in the output frequency is analytically derived.
- Comprehensive case studies investigate the effect of link failure and time-varying communication topologies in the presence of noise.

This paper is organized as follows: Section II provides preliminaries of graph theory and physical microgrid systems. Section III presents inverter synchrony using cooperative control and ADMM-based secondary controller, and analytics for noise-induced deviations. Section IV presents case studies, using a 34-bus IEEE feeder network augmented with six inverters. The conclusion is drawn in Section V.

II. Modeling Framework

A. Graph Theory

The communication topology connecting inverters $1, 2...N$ can be represented by a graph $Gr = (O, E)$. $O = \{o_1, o_2, ..., o_N\}$ is a set of N nodes corresponding to individual inverter. E is a set of edges or communication links, where each edge from o_i to o_j is denoted by (o_i, o_j). N_i is the set of inverters connected to inverter i on the communication topology, also referred to as its neighbors. The graph can be represented by an adjacency matrix $\mathbf{A} = [a_{ij}]$, with weights $a_{ij} > 0$ if $(o_i, o_j)\epsilon E$, otherwise $a_{ij} = 0$. The diagonal in-degree matrix is defined as $\mathbf{D} = \mathrm{diag}\{N_i\}$. The graph Laplacian matrix is $\mathbf{L} = \mathbf{D} - \mathbf{A}$. The convergence rate depends on the second eigenvalue (Fiedler value λ_2) of the graph Laplacian matrix L. A graph is said to have a spanning tree, if there is a root node with a path from that node to every other node in the graph. Synchronization is guaranteed as long as the communication graph has a spanning tree [25]. A leader node is connected to a few inverters (at least to one root inverter) by unidirectional links. The inverters connected to the leader node and the corresponding edges are called pinned inverters and pinning edges, respectively. g_i is the pinning gain from the leader to the

inverter i. The pinning gain is zero for an unpinned inverter. The pinning gain matrix is given by $\mathbf{G} = \mathrm{diag}\{g_i\}$.

B. Inverter and Power Distribution Network Dynamics

Each *inverter system* consists of a DC power source, inverter bridge, power sharing controller, output filter, connector, and voltage and current controllers, as shown in Fig. 2 and [3], [26]. The non-linear dynamics of each inverter are formulated in its own direct-quadrature(d-q) reference frame. Each inverter's reference frame is related to a common reference frame

$$\dot{\delta}_i = \omega_i - \omega_{com} \tag{1}$$

where δ_i is the angle of rotation of the inverter i reference frame. ω_i and ω_{com} are the frequencies of inverter i and the common reference frame. In practice, inverter frequency can be measured using phase-locked loops (PLL). Interested readers are directed to [14], [27]–[29] for a more detailed discussion of PLL. In this paper, frequency is obtained by solving the state-space description of an inverter.

The primary control provides the voltage reference to the voltage controller and operating frequency to the inverter bridge. The primary controller is discussed in detail in the next sub-section. It employs a power calculator block to calculate the instantaneous active and reactive powers, and obtaining their average by passing them through a low-pass filter. Instantaneous powers are calculated at inverter's terminals

$$\begin{cases} \mathrm{p}_i = (v_{odi} i_{odi} + v_{oqi} i_{oqi}) \\ \mathrm{q}_i = (v_{oqi} i_{odi} - v_{odi} i_{oqi}) \end{cases}, \tag{2}$$

where v_{odi} and v_{oqi} are the direct and quadrature components of the output voltage, while i_{odi} and i_{oqi} are the direct and quadrature components of the output current of inverter i. p_i and q_i are the instantaneous active and reactive powers. The average active

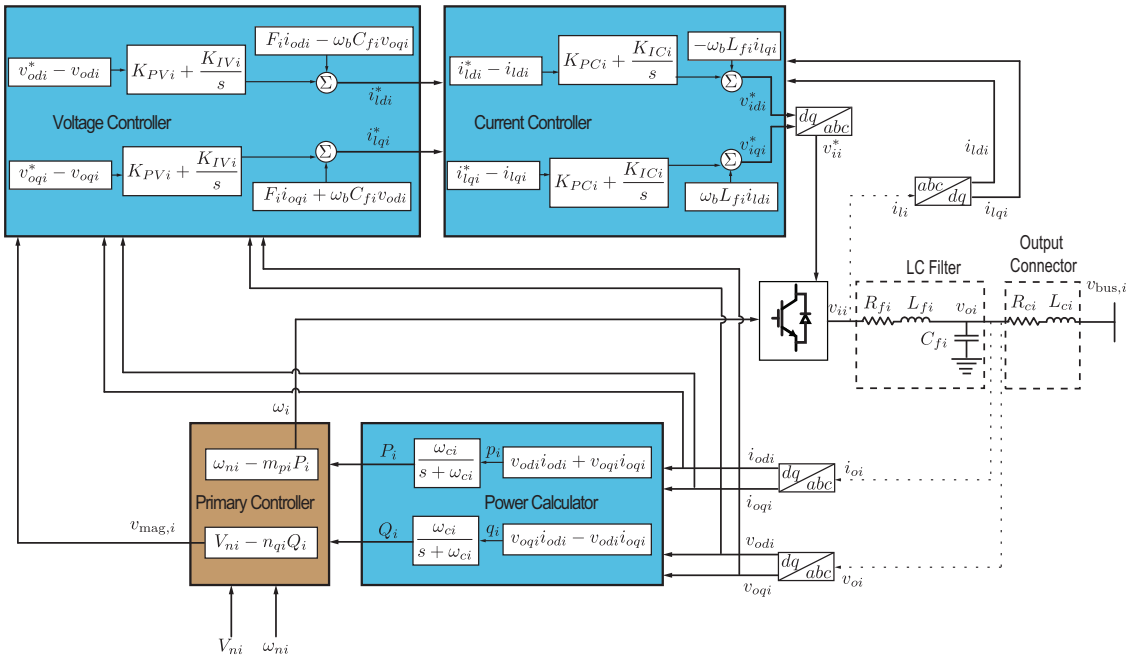

Fig. 2. Control block diagram of inverter i.

and reactive powers can be expressed as

$$\begin{cases} \mathrm{P}_i = \frac{\omega_{ci}}{s+\omega_{ci}}\ p_i \\ \mathrm{Q}_i = \frac{\omega_{ci}}{s+\omega_{ci}}\ q_i \end{cases}, \tag{3}$$

where ω_{ci} is the cut-off frequency of the low-pass filter used to measure power. P_i and Q_i are the active and reactive powers measured at inverter i.

The power controller dynamics can be given by

$$\begin{cases} \dfrac{\mathrm{d}P_i}{\mathrm{d}t} = -\omega_{ci}P_i + \omega_{ci}(v_{odi}i_{odi} + v_{oqi}i_{oqi}) \\ \dfrac{\mathrm{d}Q_i}{\mathrm{d}t} = -\omega_{ci}Q_i + \omega_{ci}(v_{oqi}i_{odi} - v_{odi}i_{oqi}) \end{cases}, \tag{4}$$

The voltage controller dynamics are

$$\begin{cases} \dot{\phi}_{di} = v^*_{odi} - v_{odi}, \\ \dot{\phi}_{qi} = v^*_{oqi} - v_{oqi}, \\ i^*_{ldi} = F_i i_{odi} - \omega_b C_{fi} v_{oqi} + K_{PVi}(v^*_{odi} - v_{odi}) + K_{IVi}\phi_{di}, \\ i^*_{lqi} = F_i i_{oqi} + \omega_b C_{fi} v_{odi} + K_{PVi}(v^*_{oqi} - v_{oq,i}) + K_{IVi}\phi_{qi} \end{cases} \tag{5}$$

where ϕ_{di} and ϕ_{qi} are the state variables of the PI controller used to implement the voltage controller. ω_b is the nominal angular frequency. The current controller dynamics are

$$\begin{cases} \dot{\gamma}_{di} = i^*_{ldi} - i_{ldi}, \\ \dot{\gamma}_{qi} = i^*_{lqi} - i_{lqi}, \\ v^*_{idi} = -\omega_b L_{fi} i_{lqi} + K_{PCi}(i^*_{ldi} - i_{ldi}) + K_{ICi}\gamma_{di}, \\ v^*_{iqi} = \omega_b L_{fi} i_{ldi} + K_{PCi}(i^*_{lqi} - i_{lq,i}) + K_{ICi}\gamma_{qi} \end{cases} \tag{6}$$

where γ_{di} and γ_{qi} are the state variables of the PI controller used to implement the current controller. i_{ldi} and i_{lqi} are the direct and quadrature components of current measured at the output filter. The output LC filter and connector dynamics are

$$\begin{cases} \dot{i}_{ldi} = -\frac{R_{fi}}{L_{fi}} i_{ldi} + \omega_i i_{lqi} + \frac{1}{L_{fi}} v_{idi} - \frac{1}{L_{fi}} v_{odi}, \\ \dot{i}_{lqi} = -\frac{R_{fi}}{L_{fi}} i_{lqi} - \omega_i i_{ldi} + \frac{1}{L_{fi}} v_{iqi} - \frac{1}{L_{fi}} v_{oqi}, \\ \dot{v}_{odi} = \omega_i v_{oqi} + \frac{1}{C_{fi}} i_{ldi} - \frac{1}{C_{fi}} i_{odi}, \\ \dot{v}_{oqi} = -\omega_i v_{odi} + \frac{1}{C_{fi}} i_{lqi} - \frac{1}{C_{fi}} i_{oqi}, \\ \dot{i}_{odi} = -\frac{R_{ci}}{L_{ci}} i_{odi} + \omega_i i_{oqi} + \frac{1}{L_{ci}} v_{odi} - \frac{1}{L_{ci}} v_{bdi}, \\ \dot{i}_{oqi} = -\frac{R_{ci}}{L_{ci}} i_{oqi} - \omega_i i_{odi} + \frac{1}{L_{ci}} v_{oqi} - \frac{1}{L_{ci}} v_{bqi} \end{cases} \tag{7}$$

The large-signal dynamical model of an inverter, with internal control loops, is adopted from [3], [26]

$$\begin{cases} \dfrac{\mathrm{d}\mathbf{x}_i}{\mathrm{d}t} = f_i(x_i) + g(x_i)u_i \\ \mathbf{y}_i = h_i(x_i) \end{cases}, \tag{8}$$

where the state vector is

$$\mathbf{x}_i = \left[\delta_i, P_i, Q_i, \phi_{di}, \phi_{qi}, \gamma_{di}, \gamma_{qi}, i_{ldi}, i_{lqi}, v_{odi}, v_{oqi}, i_{odi}, i_{oqi}\right]. \tag{9}$$

The dynamics of inverter's inductive load is given by

$$\begin{cases} \frac{\mathrm{d}i_{load,d}}{\mathrm{d}t} = -\frac{R_{load}}{L_{load}} i_{load,d} + \omega i_{load,q} + \frac{1}{L_{load}} v_{bd} \\ \frac{\mathrm{d}i_{load,q}}{\mathrm{d}t} = -\frac{R_{load}}{L_{load}} i_{load,q} - \omega i_{load,d} + \frac{1}{L_{load}} v_{bq} \end{cases}, \tag{10}$$

The detailed expressions of (8,9,10) can be found in [3], [26]. The active and reactive power flow between the inverter i and the distribution network at bus i is given by

$$\begin{cases} P_i = \frac{v_{\mathrm{mag},i} v_{\mathrm{bus},i} sin(\alpha_i - (\theta_i - \beta_i))}{Z_i} - \frac{v_{\mathrm{bus},i}^2 cos(\delta_i)}{Z_i} \\ Q_i = \frac{v_{\mathrm{mag},i} v_{\mathrm{bus},i} cos(\alpha_i - (\theta_i - \beta_i))}{Z_i} - \frac{v_{\mathrm{bus},i}^2 sin(\delta_i)}{Z_i} \end{cases}, \tag{11}$$

where $Z_i \angle \alpha_i$ is the combined impedance of the output filter and connector. $v_{\mathrm{mag},i}$ is the i^{th} output inverter voltage, and $v_{\mathrm{bus},i} \angle \beta_i$ is the i^{th} bus voltage. Assuming the line impedance is purely inductive $\alpha_i = 90^o$, and the phase difference between inverter voltage and bus voltage is small. Active and reactive power injections at bus i by inverter i become

$$\begin{cases} P_i = \frac{v_{\mathrm{mag},i} v_{\mathrm{bus},i} sin(\theta_i - \beta_i)}{Z_i} \\ Q_i = \frac{v_{\mathrm{mag},i} v_{\mathrm{bus},i} cos(\theta_i - \beta_i)}{Z_i} - \frac{v_{\mathrm{bus},i}^2}{Z_i} \end{cases}, \tag{12}$$

This leads to linear relationships for (P_i, ω_i) and (Q_i, v_i), used in droop mechanisms.

III. INVERTER SYNCHRONIZATION

A. Primary Control

Decentralized droop techniques are conventionally adopted for the primary control by linearizing the relationships in (P_i, ω_i) and (Q_i, v_i) in (12),

$$\begin{cases} \omega_i = \omega_{ni} - m_{pi} P_i \\ v_{\mathrm{mag},i} = V_{ni} - n_{qi} Q_i \end{cases}, \tag{13}$$

$v_{\mathrm{mag},i}$ and ω_i are the reference voltage and frequency provided for the internal control loops. P_i and Q_i are the inverters' active and reactive powers. m_{pi} and n_{qi} are the droop coefficients obtained based on the inverter ratings. ω_{ni} and V_{ni} are the setpoints for the primary controllers in (13).

The primary control provides the voltage reference for the inverter voltage controller and the operating frequency ω_i to the inverter bridge. The references for the voltage controller are set as

$$\begin{cases} v^*_{odi} = v_{\mathrm{mag},i} \\ v^*_{oqi} = 0 \end{cases}. \tag{14}$$

B. Cooperative Secondary Controller

Droop control techniques lead to a deviation of voltage and frequency from their reference setpoints. The secondary control provides setpoints ω_{ni} and V_{ni} for the primary controller in (13) to synchronize and restore the inverters' voltages and frequencies to their reference values. Secondary control can be achieved in a distributed fashion by each inverter exchanging data only with its neighbors on the communication graph [3], [10], [13]–[15]. To obtain the control input ω_{ni}, auxiliary control input u_i is set as

$$u_i = \dot{\omega}_i \tag{15}$$

The cooperative frequency control based on [10], [13], using the relative measured information of inverters neighboring on the communication graph and leader is

$$e_{\omega_i}(t) = \sum_{j \in N_i} a_{ij} \left(\omega_i(t) - \omega_j(t)\right) + g_i \left(\omega_i(t) - \omega_{\text{ref}}\right), \tag{16}$$

where ω_i and ω_j are the frequencies of inverters i and j. N_i is the set of inverters neighboring inverter i on the communication graph. The pining gain, g_i, is non-zero for the inverters connected to the reference frequency, ω_{ref}.

The auxiliary control input u_i at inverter i is given by

$$u_i(t) = -c_\omega e_{\omega_i}(t), \tag{17}$$

where $c_\omega \in \mathbb{R}$ is a coupling gain. The secondary control setpoint for primary control, ω_{ni}, is given by

$$\omega_{ni} = \int \left(u_i + m_{pi}\dot{P}_i\right) \mathrm{d}t, \tag{18}$$

where $\dot{P}_i$ is given by (4). A similar approach has been used for the cooperative secondary voltage control [3]. If the communication link between two inverters is corrupted due to natural noise in communication channel or external false data injection, the controller receives corrupted frequency information. This can be modeled by

$$\omega_i^j = \omega_i + \eta_i, \tag{19}$$

where ω_i^j is the frequency of inverter i communicated to inverter j, and η_i is noise. Synchronization to the desired setpoint ω_{ref} using cooperative control law cannot be guaranteed in the presence of noise [22].

C. ADMM-based Distributed Optimization

In this subsection, a fully distributed approach for the secondary control of microgrid using an ADMM-based secondary controller is proposed. ADMM method offers robust-

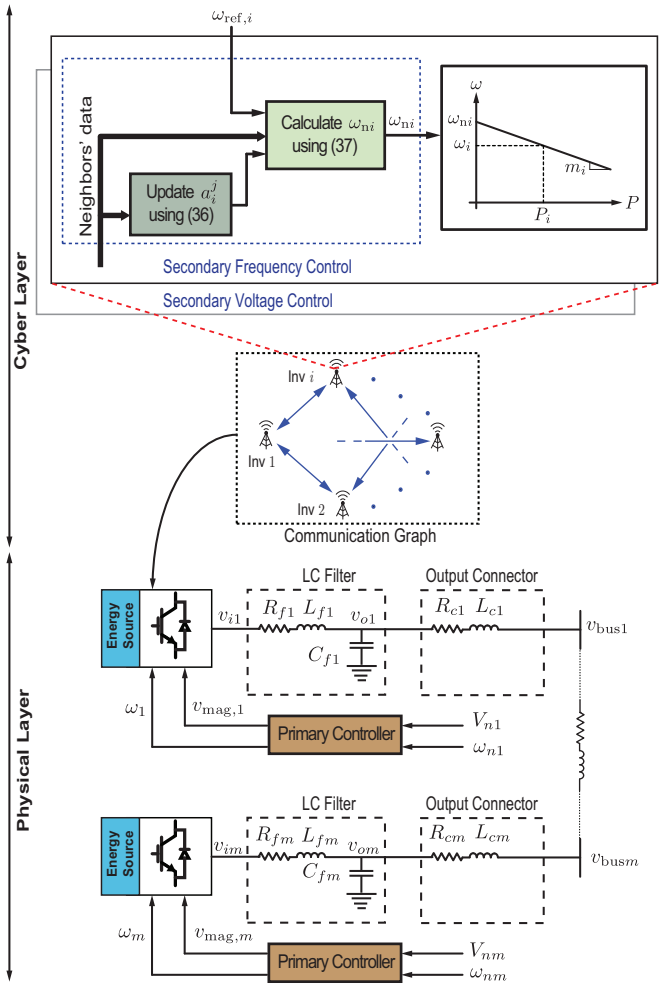

Fig. 3. ADMM-based control of inverter-based microgrids.

ness in the presence of noise, and fast convergence rates as it is a second-order method. In frequency synchronization, the control objective is $\omega_1 = \omega_2 = ... = \omega_N = \omega_{\text{ref}}$ [3]. One can then write

$$\omega_{\text{n,ref},i} = \omega_{\text{ref},i} + m_i P_i, \tag{20}$$

which represents the local frequency setpoint required at inverter i to ensure $\omega_i = \omega_{\text{ref}}$. The synchronization objective will then be cast as a constrained optimization problem and solved in a distributed fashion using ADMM, based on inverter interactions with their neighbors on a sparse communication graph. The convex constrained optimization

problem, in terms of the local frequency setpoints, is given as

$$\{\hat{\omega}_{\mathrm{n}i}(t)\}_{i=1}^{N} = \arg\min_{\omega_{\mathrm{n}}} \sum_{i=1}^{N} \mathrm{E}[g_i \left(\omega_{\mathrm{n,ref},i}(t) - \omega_{\mathrm{n}i}\right)^2],$$
$$\text{subject to } \omega_i = \omega_j, i \in N, j \in N_i \tag{21}$$

$g_i = 1$ if inverter i is pinned; Otherwise, $g_i = 0$. One can modify the constraints in (21) to $\omega_{\mathrm{n}i} - m_i P_i = \omega_{\mathrm{n}j} - m_j P_j$. Then, auxiliary variables ψ replace these constraints with

$$\omega_{\mathrm{n}i} - m_i P_i = \psi_i^j \ ; \ \omega_{\mathrm{n}j} - m_j P_j = \psi_i^j, i \in N, j \in N_i. \tag{22}$$

To form a quadratic Lagrangian function, multipliers associated with constraints are defined. The ADMM consists of iteratively updating the (i) multipliers, (ii) frequency setpoints and (iii) auxiliary variables to solve (21). This is detailed below:

The Lagrange multipliers $[a, b] := a_i^j, b_i^j$, associated with the auxiliary variables in (22), form a quadratic Lagrangian function

$$\begin{aligned}
\mathcal{L}[\omega_{\mathrm{n}}, \psi, a, b] &= \sum_{i=1}^{N} \mathrm{E}[g_i \left(\omega_{\mathrm{n,ref},i}(t+1) - \omega_{\mathrm{n}i}\right)^2] \\
&+ \sum_{i=1}^{N} \sum_{j \in N_i} \big[(a_i^j)^T(\omega_{\mathrm{n}i} - m_i P_i - \psi_i^j) \\
&+ (b_i^j)^T(\omega_{\mathrm{n}i} - m_i P_i - \psi_j^i)\big] \\
&+ \sum_{i=1}^{N} \sum_{j \in N_i} \frac{c}{2} \big[||\omega_{\mathrm{n}i} - m_i P_i - \psi_i^j||^2 \\
&+ ||\omega_{\mathrm{n}i} - m_i P_i - \psi_j^i||^2\big],
\end{aligned} \tag{23}$$

where $c > 0$ is the penalty coefficient. Multipliers are updated as

$$a_i^j(t) = a_i^j(t-1) + c\left(\omega_{\mathrm{n}i}(t) - m_i P_i - \psi_i^j(t)\right). \tag{24}$$

$$b_i^j(t) = b_i^j(t-1) + c\left(\omega_{\mathrm{n}i}(t) - m_i P_i - \psi_j^i(t)\right). \tag{25}$$

The frequency setpoints are updated as

$$\omega_{\mathrm{n}}(t+1) = \arg\min_{\omega_{\mathrm{n}}} \mathcal{L}[\omega_{\mathrm{n}}, \psi(t), a(t), b(t)]. \tag{26}$$

Auxiliary variables are updated as

$$\psi(t+1) = \arg\min_{\psi} \mathcal{L}[\omega_{\mathrm{n}}(t+1), \psi, a(t), b(t)]. \tag{27}$$

To be solved locally, (27) can be decoupled into

$$\begin{aligned}
\psi_i^j(t+1) = \arg\min_{\psi_i^j} \Big[& -\left[a_i^j(t) + b_j^i(t)\right]^T \psi_i^j \\
& + \frac{c}{2}\left[||\omega_{\mathrm{n}i}(t+1) - m_i P_i - \psi_i^j||^2\right. \\
& \left. + ||\omega_{\mathrm{n}j}(t+1) - m_j P_j - \psi_i^j||^2\right]\Big] \\
= & \frac{1}{2c}\left[a_i^j(t) + b_j^i(t)\right]^T \\
& + \frac{1}{2}\left[\omega_{\mathrm{n}i}(t+1) - m_i P_i + \omega_{\mathrm{n}j}(t+1) - m_j P_j\right].
\end{aligned} \tag{28}$$

To eliminate the auxiliary variables from (24) and (25), let $a_i^j(-1) = -b_j^i(-1)$. Then, $a_i^j(t) = -b_j^i(t)$. Thus, (28) becomes $\psi_i^j(t+1) = \frac{1}{2}\left[\omega_{\mathrm{n}i}(t+1) - m_i P_i + \omega_{\mathrm{n}j}(t+1) - m_j P_j\right]$. Substituting this in (24) leads to

$$a_i^j(t) = a_i^j(t-1) + \frac{c}{2}\left[(\omega_{\mathrm{n}i}(t) - m_i P_i) - (\omega_{\mathrm{n}j}(t) - m_j P_j)\right]. \tag{29}$$

Thus, the auxiliary variables are eliminated from the multiplier updates. The opti-

mization problem (26) can be decoupled as

$$\begin{aligned}\omega_{\mathrm{n}i}(t+1) = \arg\min_{\omega_{\mathrm{n}i}} \Bigg[& \mathrm{E}[g_i\left(\omega_{\mathrm{n,ref},i}(t+1) - \omega_{\mathrm{n}i}\right)^2] \\ & + \sum_{j\in N_i} \left[a_i^j(t) + b_i^j(t)\right]^T \left(\omega_{\mathrm{n}i} - m_i P_i\right) \\ & + \sum_{j\in N_i} \frac{c}{2} \left[||\omega_{\mathrm{n}i} - m_i P_i - \psi_i^j(t)||^2 \right. \\ & \left. + ||\omega_{\mathrm{n}i} - m_i P_i - \psi_j^i(t)||^2\right] \Bigg]. \end{aligned} \tag{30}$$

Using $a_i^j(t) = -b_i^j(t)$, $\psi_i^j(t) = \psi_j^i(t)$ in (30)

$$\begin{aligned}\omega_{\mathrm{n}i}(t+1) = \arg\min_{\omega_{\mathrm{n}i}} \Bigg[& \mathrm{E}[g_i\left(\omega_{\mathrm{n,ref},i}(t+1) - \omega_{\mathrm{n}i}\right)^2] \\ & + \sum_{j\in N_i} \left[a_i^j(t) + b_i^j(t)\right]^T \left(\omega_{\mathrm{n}i} - m_i P_i\right) \\ & + \sum_{j\in N_i} c \left[||\omega_{\mathrm{n}i} - m_i P_i - \psi_i^j(t)||^2\right] \Bigg] \\ = \arg\min_{\omega_{\mathrm{n}i}} \Bigg[& \mathrm{E}\left[g_i\left(\omega_{\mathrm{n,ref},i}(t+1) - \omega_{\mathrm{n}i}\right)^2\right] \\ & + \sum_{j\in N_i} \left[a_i^j(t) - a_j^i(t)\right]^T \left(\omega_{\mathrm{n}i} - m_i P_i\right) \\ & + c \sum_{j\in N_i} \left(||\left(\omega_{\mathrm{n}i} - m_i P_i\right) \right. \\ & \left. - \frac{1}{2}\left(\omega_{\mathrm{n}i}(t) - m_i P_i + \omega_{\mathrm{n}j}(t) - m_j P_j\right)||^2\right) \Bigg]. \end{aligned} \tag{31}$$

The unconstrained minimization problem in (31) is convex, and the first-order differentiation is a sufficient optimality condition [24]. By setting the gradient, with respect to $\omega_{\mathrm{n}i}$, to zero

$$\mathrm{E}\Bigg[-2g_i\left(\omega_{\mathrm{n,ref},i}(t+1)-\omega_{\mathrm{n}i}\right)+\sum_{j\in N_i}\left[a_i^j(t)-a_j^i(t)\right] + 2c\Bigg[\left(\omega_{\mathrm{n}i}-m_iP_i\right)-\frac{1}{2}\left(\omega_{\mathrm{n}i}(t)-m_iP_i+\omega_{\mathrm{n}j}(t) -m_jP_j\right)\Bigg]\Bigg]=0. \tag{32}$$

The proposed recursion to update the frequency setpoint is

$$\begin{aligned}\omega_{\mathrm{n}i}(t+1)=\omega_{\mathrm{n}i}(t)+\mu\Bigg[&2g_i\Big(\omega_{\mathrm{n,ref},i}(t+1)-\omega_{\mathrm{n}i}(t)\Big)\\ &-\sum_{j\in N_j}\left(a_i^j(t)-a_j^i(t)\right)\\ &-c\sum_{j\in N_j}\Big(\left(\omega_{\mathrm{n}i}(t)-m_iP_i\right)-\left(\omega_{\mathrm{n}j}(t)-m_jP_j\right)\Big)\Bigg]\end{aligned} \tag{33}$$

μ is a constant step size.

D. Communication Impact on ADMM-based Distributed Optimization

Communication links are subject to failure and noise. ADMM-based optimization updates can be modified to account for noise and communication for analysis. Accounting for the additive noise corrupting the neighbor information, the multiplier update and the frequency setpoint update can be rewritten as

$$a_i^j(t)=a_i^j(t-1)+\frac{c}{2}\left[\left(\omega_{\mathrm{n}i}(t)-m_iP_i\right)-\left(\omega_{\mathrm{n}j}(t) -m_jP_j+\eta_\omega\right)\right], \tag{34}$$

$$\omega_{\mathrm{n}i}(t+1) = \omega_{\mathrm{n}i}(t) + \mu\Bigg[2g_i\Big(\omega_{\mathrm{n,ref},i}(t+1) - \omega_{\mathrm{n}i}(t) + \eta_{\omega_{\mathrm{ref}}}\Big) - \sum_{j\in N_j}\left(a_i^j(t) - a_j^i(t) + \eta_a\right) - c\sum_{j\in N_j}\Big(\left(\omega_{\mathrm{n}i}(t) - m_iP_i\right) - \left(\omega_{\mathrm{n}j}(t) - m_jP_j + \eta_\omega\right)\Big)\Bigg], \tag{35}$$

where $\eta_{\omega_{\mathrm{ref}}}$ is the additive noise in the reference signal, η_a is the additive noise in the multiplier signal, and η_ω is the noise in the neighbor frequency.

The communication links between inverters are subject to the potential failure. The multiplier update and the local frequency setpoint update can be modified to take communication link failure into account

$$a_i^j(t) = a_i^j(t-1) + \frac{c}{2}\left[\left(\omega_{\mathrm{n}i}(t) - m_iP_i\right) - l_{ij}\left(\omega_{\mathrm{n}j}(t) - m_jP_j + \eta_\omega\right)\right], \tag{36}$$

$$\omega_{\mathrm{n}i}(t+1) = \omega_{\mathrm{n}i}(t) + \mu\Bigg[2g_i\Big(\omega_{\mathrm{n,ref},i}(t+1) - \omega_{\mathrm{n}i}(t) + \eta_{\omega_{\mathrm{ref}}}\Big) - \sum_{j\in N_j}\left(a_i^j(t) - l_{ij}(a_j^i(t) + \eta_a)\right) - c\sum_{j\in N_j}\Big(\left(\omega_{\mathrm{n}i}(t) - m_iP_i\right) - l_{ij}\left(\omega_{\mathrm{n}j}(t) - m_jP_j + \eta_\omega\right)\Big)\Bigg], \tag{37}$$

where $\eta_{\omega_{\mathrm{ref}}}$ is the additive noise in the reference signal, η_a is the additive noise in the multiplier signal, and η_ω is the noise in neighbor frequency, $l_{ij} = 0$ indicates communication link failure between inverters i and j, and $l_{ij} = 1$ indicates an operational communication link. The communication links between inverters are subject to

a potential failure.

The overall ADMM-based synchronization of AC microgrids is presented in Fig. 3, and summarized in Algorithm 1. Secondary voltage control can be performed in tandem by using a similar algorithm.

Algorithm 1 Secondary Control of Frequency using ADMM

Initialize $a_i^j(-1)$.
for $t = 0, 1...$ **do**
  Inverter i transmits $\omega_{\mathrm{n},i}(t)$ and $\omega_i(t)$ to neighbors N_i.
  Inverter i updates $a_i^j(t)$ using (36).
  Inverter i transmits $a_i^j(t)$ to neighbors.
  Inverter i updates $\omega_{\mathrm{n},i}(t+1)$ using (37).
end for

E. Performance Analysis

To assess the performance of the Algorithm 1 in terms of output frequencies, (37) is rewritten in terms of ω_i instead of $\omega_{\mathrm{n}i}$

$$\omega_i(t+1) = \omega_i(t) + \mu \Bigg[2g_i \left(\omega_{\mathrm{ref},i}(t+1) - \omega_i(t) + \eta_{\mathrm{ref}}\right) - \sum_{j \in N_j} \left(a_i^j(t) - l_{ij}(a_j^i(t) + \eta_a)\right) - c \sum_{j \in N_j} \left(\omega_i(t) - l_{ij}(\omega_j(t) + \eta_\omega)\right) \Bigg], \tag{38}$$

which is similar to the estimate update in ([30]-section 3.1). It can be ascertained from [30] that, in the absence of noise ω_i converges to ω_{ref}.

An upper bound on the deviation of the output frequency from the reference value is analytically derived, following an approach similar to [30]. The noise in the communication links is assumed to be zero mean Gaussian in nature. Mean-square error (MSE) is considered to evaluate error

$$\mathbf{MSE}(t) = \mathrm{E}[||\boldsymbol{\omega}(t) - \boldsymbol{\omega}_{\mathrm{ref}}||^2], \tag{39}$$

where $\boldsymbol{\omega} = [\omega_1\ \omega_2\ ...\ \omega_N]^T$ and $\boldsymbol{\omega}_{\mathrm{ref}} = \underline{\mathbf{1}}\omega_{\mathrm{ref}}$.

Local frequency error is $\{\mathbf{y}_{1,i}(t) := \omega_i(t) - \omega_{\mathrm{ref}}\}_{i=1}^N$ and the multiplier error is $\{\mathbf{y}_{2,i}(t) := \sum_{j\in N_j}(a_i^j(t-1) - l_{ij}a_j^i(t-1))\}_{i=1}^N$. The global state vector, capturing the dynamics of the control algorithm for frequency, is defined as $\mathbf{y}(t) =: [\mathbf{y}_1^T(t)\ \mathbf{y}_2^T(t)]^T = [\mathbf{y}_{1,1}^T(t)...\mathbf{y}_{1,N}^T(t)\ \mathbf{y}_{2,1}^T(t)...\mathbf{y}_{2,N}^T(t)]^T$. To capture the effect of noise on the pinned reference communicated among inverters, noise vectors are defined as $\boldsymbol{\eta}_{\omega_{\mathrm{ref}}}(t) := 2\mu[\eta_{\omega_{\mathrm{ref}},1}(t)...\eta_{\omega_{\mathrm{ref}},N}(t)]^T$ and $\boldsymbol{\eta}_a := [\eta_{a,1}^T(t)...\eta_{a,N}^T(t)]^N$, where $\eta_{a,i} =: \sum_{j\in N_i}\eta_{a,i}^j(t)$ is the accumulated communication noise at inverter i due to reception of all required multipliers at time t, and covariance is $\mathbf{R}_{\boldsymbol{\eta}_a} := \mathrm{E}[\boldsymbol{\eta}_a(t)\boldsymbol{\eta}_a^T(t)]$. The receiver noise corrupting the local neighbor inverter frequency $\boldsymbol{\eta}_\omega(t) := [\{\eta_{\omega,j}^1(t)\}_{j\in N_1}...\{\eta_{\omega,j}^N(t)\}_{j\in N_N}]^T$, and covariance is $\mathbf{R}_{\boldsymbol{\eta}_\omega} := \mathrm{E}[\boldsymbol{\eta}_\omega(t)\boldsymbol{\eta}_\omega^T(t)]$.

The local mean-square error at each inverter, at time instant t, can be defined as

$$\mathrm{MSE}_i(t) = \mathrm{E}[||\mathbf{y}_{1,i}(t)||^2]. \tag{40}$$

If $\mathbf{R}_{\mathbf{y}_{1,i}}(t) := \mathrm{E}[\mathbf{y}_{1,i}\mathbf{y}_{1,i}^T(t)]$ is the local covariance matrix at inverter i, then $\mathrm{MSE}_i(t) = \mathbf{tr}[\mathbf{R}_{\mathbf{y}_{1,i}}(t)]$. The global mean-square error at time t is given by $\mathbf{MSE}(t) = \frac{1}{N}\sum_{i\in N}\mathbf{tr}[\mathbf{R}_y(t)]_{11,i}$. Thus, the upper bound for the mean-square deviation in the steady state from [30] can be used

$$\mathbf{MSE}(\infty) = \frac{1}{N}\sum_{i\in N}\mathbf{tr}\left[\mathbf{R}_y(\infty)\right]_{11,i}. \tag{41}$$

$\mathbf{R}_y$ is the state covariance matrix, and its expression can be obtained from ([30]-section 5.2). It has also been shown in [30] that $\mathbf{MSE}(\infty)$ is bounded and stable.

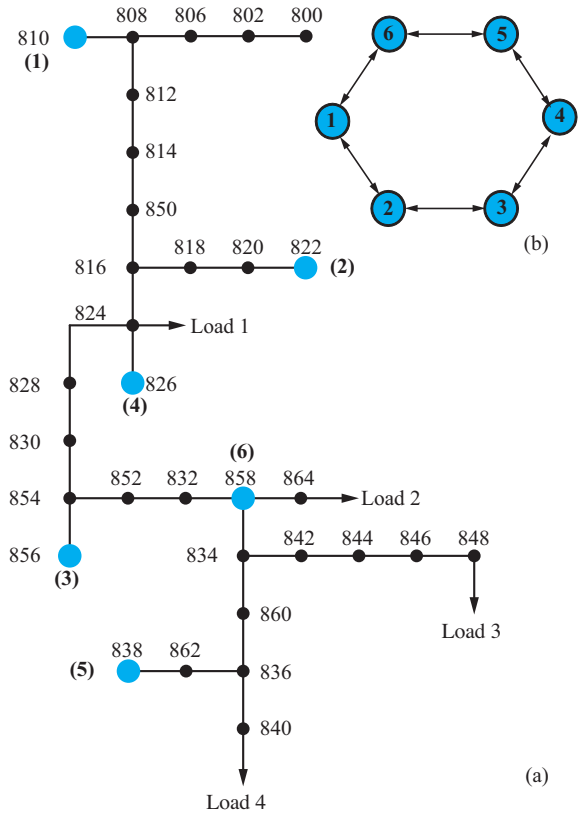

Fig. 4. (a) IEEE standard 34-bus feeder system augmented with six inverters;(b) Topology of the communication network among inverters.

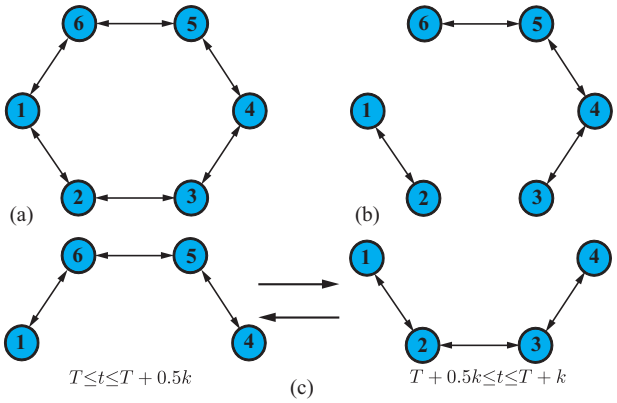

Fig. 5. Communication Topologies: (a) Ring communication; (b) Links between inverters 1 and 6 as well as 2 and 3 fail; (c) Time-varying topology: Communication graph switches between the two topologies every 0.5 s.

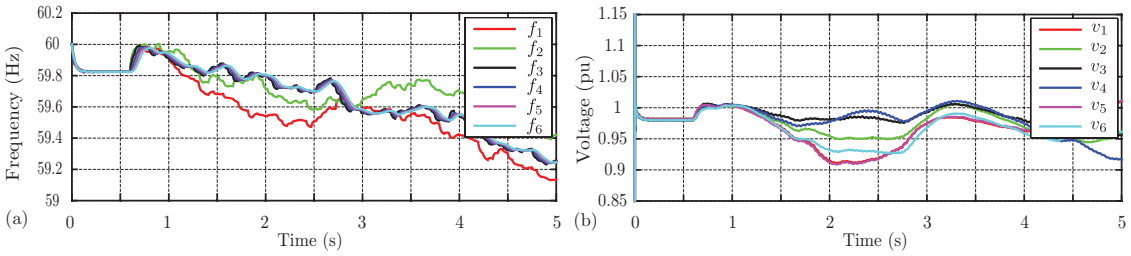

Fig. 6. Conventional controller fails for the noise levels of $\sigma^2 = 0.1$.

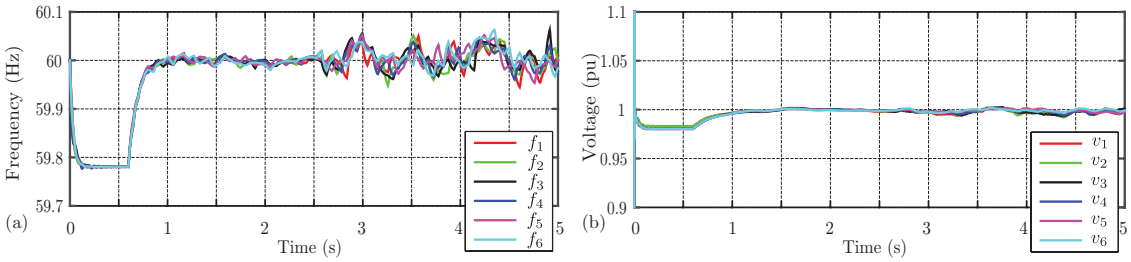

Fig. 7. Case A: (a),(b) Inverter frequencies and voltages when there is communication noise with $\sigma^2 = 10^{-2}$ for $t < 2.5$ s and $\sigma^2 = 0.1$ for $t > 2.5$ s.

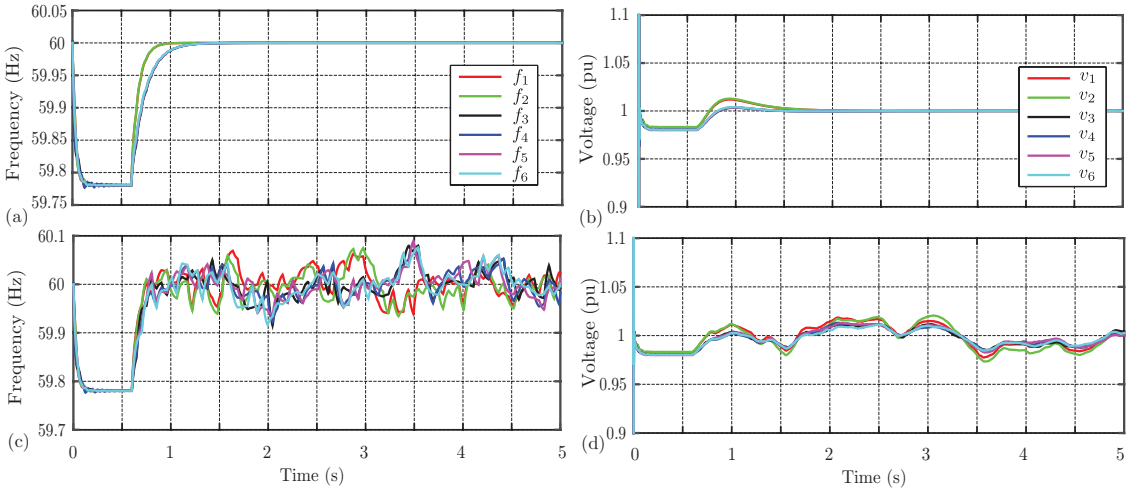

Fig. 8. Case B (Link failure): (a),(b) Inverter frequencies and voltages under ideal conditions (no noise) when the link between inverter 1 and 6 is down; (c),(d) Inverter frequencies and voltages with noise $\sigma^2 = 0.1$ when links between inverters 1 and 6, and 2 and 3, are down.

IV. Case Studies

The distributed ADMM-based secondary controller performance is evaluated for an islanded microgrid. A single-line diagram of a modified 34-bus test feeder, augmented

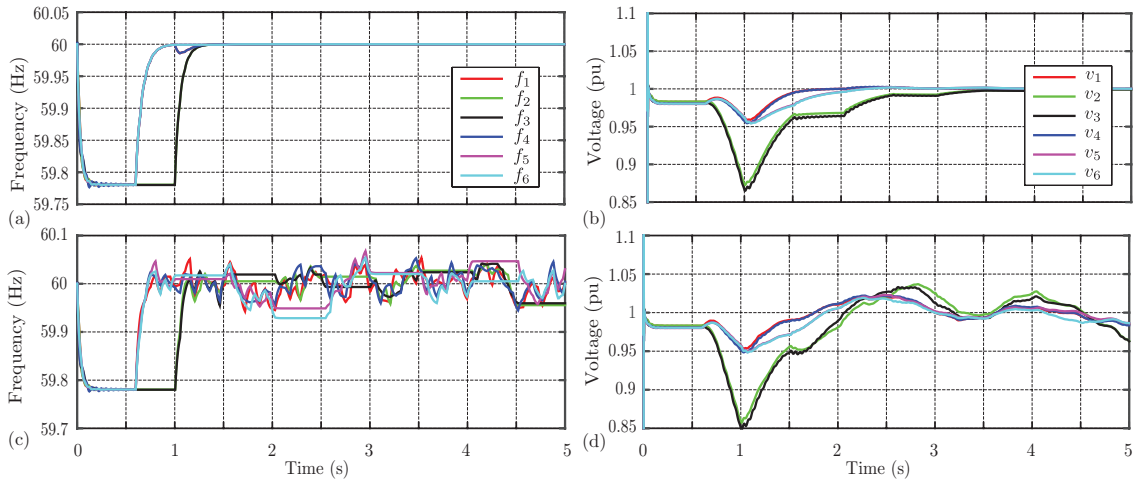

Fig. 9. Case C (Time-varying graph): (a),(b) Inverter frequencies and voltages under ideal conditions (no noise); (c),(d) Inverter frequencies and voltages when there is communication noise with $\sigma^2 = 0.1$.

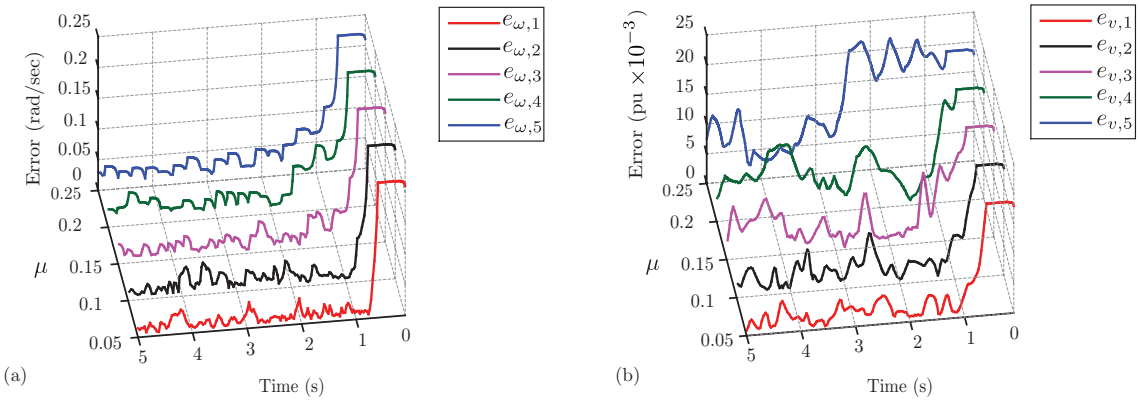

Fig. 10. Case D (Effect of varying update step size μ): (a) Error in frequency; (b) Error in voltage.

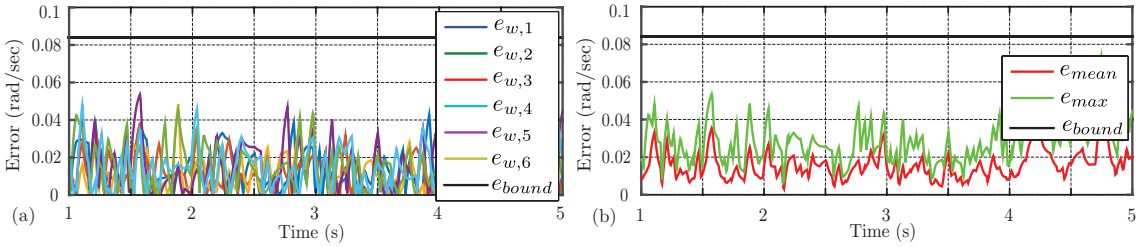

Fig. 11. Error in inverter frequencies with noise $\sigma^2 = 0.1$. The theoretical upper error bound for the corresponding noise levels is shown.

with six inverters is shown in Fig. 4. The test feeder is connected to the main grid at bus 800. The specifications for the line parameters are given in [31]. The load specifications

are load $1: 2.64 + j1.74$ p.u., load $2: 0.87 + j0.87$ p.u., load $3: 1.74 + j1.74$ p.u., and load $4: 1.39 + j1.39$ p.u.. The inverter droop specifications are summarized in Table I. Each inverter comprises of a LC filter with $R_f = 0.17$ p.u., $X_{Lf} = 0.89$ p.u. and $X_{Cf} = 92.1$ p.u., and output connector with $R_c = 0.052$ p.u., and $X_{Lc} = 0.23$ p.u., using a base of 400 kVA. The nominal frequency and line-to-line voltage are set to 60 Hz and 24.9 kV, respectively. The inverters are connected to the test feeder through a Y-Y 480V/24.9 kV, 400 kVA transformer with a series impedance of $0.03 + j0.12$ p.u. Every inverter communicates its frequency, output voltage, and Lagrange multipliers to its neighboring inverters through the communication graph (Fig. 5(a)). Inverters 1, 2, and 3 receive reference signal (pinned) with pinning gains $g_1 = g_2 = g_3 = 1$. The test feeder is islanded from the main grid at $t = 0$ s. The secondary control is activated at $t = 0.7$ s. Figures 6(a) and 6(b) show the conventional controller performance when communication links between the neighboring inverters and the reference node are corrupted with noise with $\sigma^2 = 0.1$ (variance), clearly leading to loss of synchrony.

We consider three cases to evaluate the performance of the proposed controller. In *Case A*, inverters 1 and 4 are pinned with $g_1 = g_4 = 1$. Figures 7(a) and 7(b) show the output frequency and voltage when communication links between the neighboring inverters and the reference node include variable noise with $\sigma^2 = 10^{-2}$ (variance) for $t < 2.5$ s, and $\sigma^2 = 0.1$ (variance) for $t > 2.5$ s. It can be observed that inverter frequencies and voltages are synchronized within acceptable limits. The variance of $\sigma^2 = 0.1$ implies a deviation of ± 0.95 ($\pm 3\sigma$) in the communicated frequency term.

In *Case B*, inverters 1 and 4 are pinned with gains $g_1 = g_4 = 1$. Figures 8(a) and 8(b) show the output frequency and voltage under ideal conditions when the communication links between inverters 1 and 6, and inverters 2 and 3, are down (Fig. 5(b)). The time taken for synchronization increases. Figures 8(c) and (d) show the output frequency and voltage when links between inverters 6 and 1, and inverters 2 and 3, are down, when

communication links between the neighboring inverters and the reference node includes noise with $\sigma^2 = 0.1$. Even in the presence of link failures and noise, frequencies and voltages are synchronized within acceptable limits as long as there exists a path from the reference to each inverter. In this case, the communication graph splits into two as shown in Fig. 5(b), each containing a pinned inverter (1 and 4).

In *Case C*, a time-varying periodic communication graph shown in Fig. 5(c) is employed. As seen in Figs. 9(a) and 9(b), under ideal conditions, frequency and voltage synchronize to the desired $f = 60$ Hz and $V = 1$ p.u. As long as the union of the time-varying graphs has a spanning tree, synchrony is achieved eventually. Figures 9(c) and 9(d) show the output frequency and voltage when communication links between the neighboring inverters and the reference node include noise with $\sigma^2 = 0.1$ (variance). As seen, the error associated with noise under a time-varying graph increases, thus switching time between topologies must be smaller (currently 0.5 s) to ensure proper synchronization.

In *Case D*, inverters 1 and 4 are pinned with gains $g_1 = g_4 = 1$. The effect of μ in (37) on the frequency and voltage error is studied. μ is varied from 0.05 to 0.25, in steps of 0.05, and the mean frequency and voltage errors are plotted in Figs. 10(a) and 10(b). As μ increases, the time taken for synchrony initially decreases, but the steady-state error increases.

The upper error bounds in frequency terms are calculated with the noise level of $\sigma^2 = 0.1$ in the communication links between the neighboring inverters and the reference node. It is shown in Figs. 11 (a) and (b) that the error in individual frequency and the maximum error in frequency are within the bound obtained in Section III. The robustness of the proposed control can be deduced, even with noise in communication links with a variance $\sigma^2 = 0.1$ indicating a deviation of ± 0.95, the error in frequency is less than 0.08. The upper bound on output voltage error cannot be similarly defined, as inverter

output voltages should be slightly different to allow reactive power sharing. However, as seen in Fig. 10(b), the voltage deviations due to communication noise are quite low.

TABLE I
INVERTER DROOP SPECIFICATIONS

	Inverter 1,2,4&5		**Inverter 3&6**	
Droop Gains	m_p	5.64×10^{-5}	m_p	7.5×10^{-5}
	n_q	5.2×10^{-4}	n_q	6×10^{-4}

V. CONCLUDING REMARKS

This paper revisits the synchronization phenomena in multi-inverter AC microgrids as a distributed convex constrained optimization problem. This problem was solved in a distributed fashion by using an iterative ADMM method. The proposed algorithm is inherently robust to noise and makes use of a sparse communication network. The controller performance was evaluated for different noise levels in communication links connecting neighboring inverters and the reference node. An expression for the upper error bound induced by noise was established. The efficacy of the proposed controller, with link failures and time-varying communication topologies, was evaluated using a modified 34-bus IEEE feeder test system.

REFERENCES

[1] D. Olivares, A. Mehrizi-Sani, A. Etemadi, C. Canizares, R. Iravani, M. Kazerani, A. Hajimiragha, O. Gomis-Bellmunt, M. Saeedifard, R. Palma-Behnke, G. Jimenez-Estevez, and N. Hatziargyriou, "Trends in microgrid control," *IEEE Trans. Smart Grid*, vol. 5, no. 4, pp. 1905–1919, July 2014.

[2] L. Che, M. Shahidehpour, A. Alabdulwahab, and Y. Al-Turki, "Hierarchical coordination of a community microgrid with AC and DC microgrids," *IEEE Trans. Smart Grid*, vol. 6, no. 6, pp. 3042–3051, Nov 2015.

[3] A. Bidram, A. Davoudi, F. Lewis, and Z. Qu, "Secondary control of microgrids based on distributed cooperative control of multi-agent systems," *IET Gener. Transmiss. Distrib.*, vol. 7, no. 8, pp. 822–831, Aug 2013.

[4] F. Dorfler, J. Simpson-Porco, and F. Bullo, "Breaking the hierarchy: Distributed control and economic optimality in microgrids," *IEEE Trans. Control Netw. Syst.*, vol. 3, no. 3, pp. 241–253, Sept 2016.

[5] C. Ahumada, R. Crdenas, D. Sez, and J. M. Guerrero, "Secondary control strategies for frequency restoration in islanded microgrids with consideration of communication delays," *IEEE Trans. Smart Grid*, vol. 7, no. 3, pp. 1430–1441, May 2016.

[6] F. Guo, C. Wen, J. Mao, and Y. D. Song, "Distributed secondary voltage and frequency restoration control of droop-controlled inverter-based microgrids," *IEEE Trans. Ind. Electron.*, vol. 62, no. 7, pp. 4355–4364, July 2015.

[7] F. Guo, C. Wen, J. Mao, J. Chen, and Y.-D. Song, "Distributed cooperative secondary control for voltage unbalance compensation in an islanded microgrid," *IEEE Trans. Ind. Informat.*, vol. 11, no. 5, pp. 1078–1088, Oct 2015.

[8] A. Vaccaro, V. Loia, G. Formato, P. Wall, and V. Terzija, "A self-organizing architecture for decentralized smart microgrids synchronization, control, and monitoring," *IEEE Trans. Ind. Informat.*, vol. 11, no. 1, pp. 289–298, Feb 2015.

[9] M. Tahir and S. Mazumder, "Self-triggered communication enabled control of distributed generation in microgrids," *IEEE Trans. Ind. Informat.*, vol. 11, no. 2, pp. 441–449, April 2015.

[10] A. Bidram, A. Davoudi, and F. Lewis, "A multiobjective distributed control framework for islanded AC microgrids," *IEEE Trans. Ind. Informat.*, vol. 10, no. 3, pp. 1785–1798, Aug 2014.

[11] G. Wen, G. Hu, J. Hu, X. Shi, and G. Chen, "Frequency regulation of source-grid-load systems: A compound control strategy," *IEEE Trans. Ind. Informat.*, vol. 12, no. 1, pp. 69–78, Feb 2016.

[12] J. Schiffer, T. Seel, J. Raisch, and T. Sezi, "Voltage stability and reactive power sharing in inverter-based microgrids with consensus-based distributed voltage control," *IEEE Trans. Control Syst. Technol.*, vol. 24, no. 1, pp. 96–109, Jan 2016.

[13] J. Simpson-Porco, Q. Shafiee, F. Dorfler, J. Vasquez, J. Guerrero, and F. Bullo, "Secondary frequency and voltage control of islanded microgrids via distributed averaging," *IEEE Trans. Ind. Electron.*, vol. 62, no. 11, pp. 7025–7038, Nov 2015.

[14] Q. Shafiee, J. M. Guerrero, and J. C. Vasquez, "Distributed secondary control for islanded microgrids: A novel approach," *IEEE Trans. Power Electron.*, vol. 29, no. 2, pp. 1018–1031, Feb 2014.

[15] Q. Shafiee, C. Stefanovic, T. Dragicevic, P. Popovski, J. C. Vasquez, and J. M. Guerrero, "Robust networked control scheme for distributed secondary control of islanded microgrids," *IEEE Trans. Ind. Electron.*, vol. 61, no. 10, pp. 5363–5374, Oct 2014.

[16] Q. Shafiee, V. Nasirian, J. C. Vasquez, J. M. Guerrero, and A. Davoudi, "A multi-functional fully distributed control framework for ac microgrids," *IEEE Trans. Smart Grid*, 2016, to be published.

[17] V. C. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, and G. P. Hancke, "Smart grid technologies: Communication technologies and standards," *IEEE Trans. Ind. Informat.*, vol. 7, no. 4, pp. 529–539, Nov 2011.

[18] H. Meng, Y. L. Guan, and S. Chen, "Modeling and analysis of noise effects on broadband power-line communications," *IEEE Trans. Power Del.*, vol. 20, no. 2, pp. 630–637, April 2005.

[19] J. G. Proakis, *Digital Communications*. New York: McGraw-Hill, 1995.

[20] D. Apostolopoulou, A. D. Domnguez-Garca, and P. W. Sauer, "An assessment of the impact of uncertainty on automatic generation control systems," *IEEE Trans. Power Syst.*, vol. 31, no. 4, pp. 2657–2665, July 2016.

[21] A. Shapoury, V. Venkataramanan, A. Mallikeswaran, A. Mehrizi-Sani, and M. Lopez, "Study of stability of an islanded microgrid in the presence of communication delays," in *Proc. 40th Annu. Conf. of the IEEE Ind. Electron. Soc.*, Dallas, TX, USA, Oct 2014, pp. 5666–5671.

[22] L. Xiao, S. Boyd, and S.-J. Kim, "Distributed average consensus with least-mean-square deviation," *J. Parallel Distrib. Comput.*, vol. 67, no. 1, pp. 33 – 46, Jan 2007.

[23] V. Nasirian, Q. Shafiee, J. M. Guerrero, F. L. Lewis, and A. Davoudi, "Droop-free distributed control for ac microgrids," *IEEE Trans. Power Electron.*, vol. 31, no. 2, pp. 1600–1617, Feb 2016.

[24] D. P. Bertsekas and J. N. Tsitsiklis, *Parallel and Distributed Computation: Numerical Methods*. Prentice-Hall, Inc., 1989.

[25] R. Olfati-Saber and R. Murray, "Consensus problems in networks of agents with switching topology and time-delays," *IEEE Trans. Autom. Control*, vol. 49, no. 9, pp. 1520–1533, Sept 2004.

[26] N. Pogaku, M. Prodanovic, and T. Green, "Modeling, analysis and testing of autonomous operation of an inverter-based microgrid," *IEEE Trans. Power Electron.*, vol. 22, no. 2, pp. 613–625, March 2007.

[27] J. L. Stensby, *Phase-locked loops: Theory and applications*. CRC Press, 1997.

[28] R. E. Best, *Phase locked loops. Design, Simulation, and Applications*, 6th ed. McGraw-Hill, 2007.

[29] J. C. Vasquez, J. M. Guerrero, M. Savaghebi, J. Eloy-Garcia, and R. Teodorescu, "Modeling, analysis, and design of stationary-reference-frame droop-controlled parallel three-phase voltage source inverters," *IEEE Transactions on Ind. Electron.*, vol. 60, no. 4, pp. 1271–1280, April 2013.

[30] G. Mateos, I. D. Schizas, and G. B. Giannakis, "Performance analysis of the consensus-based distributed LMS algorithm," *EURASIP J. Adv Signal Process.*, vol. 2009, no. 68, pp. 1–19, 2009.

[31] N. Mwakabuta and A. Sekar, "Comparative study of the IEEE 34 node test feeder under practical simplifications," in *Proc. 39th North Amer. Power Symp.*, Las Cruces, NM, USA, 2007, pp. 484–491.

CHAPTER 4

SYNCHRONY IN NETWORKED MICROGRIDS UNDER ATTACKS[1]

Authors: S. Abhinav, H. Modares, F. Lewis, F. Ferrese, and A. Davoudi.

Reprinted, with permission from all the co-authors.

Journal: IEEE Transactions on Smart Grid (in press),

DOI: 10.1109/TSG.2017.2721382

[1]Used with permission of the publisher, 2017. In reference to IEEE copyrighted material which is used with permission in this thesis, the IEEE does not endorse any of the University of Texas at Arlington's (UTA) products or services. Internal or personal use of this material is permitted. If interested in reprinting/republishing IEEE copyrighted material for advertising or promotional purposes or for creating new collective works for resale or redistribution, please go to $http$: $//www.ieee.org/publications_standards/publications/rights/rights_link.html$ to learn how to obtain a License from RightsLink.

Synchrony in Networked Microgrids under Attacks

Shankar Abhinav, *Graduate Student Member, IEEE,*

Hamidreza Modares, *Member, IEEE* Frank L. Lewis, *Life Fellow, IEEE,*

Frank Ferrese, *Senior Member, IEEE,*

and Ali Davoudi, *Senior Member, IEEE*

Abstract

This paper proposes attack-resilient distributed control for synchronization of islanded, networked, inverter-based microgrids. Existing cooperative control techniques are susceptible to attacks and cannot guarantee synchronization. The effect of attacks on sensor/actuator, communication links, and hijacking controllers is studied. A resilient synchronization protocol is presented to address sensors/actuators attacks. Attacks on communication links and adverse effects of hijacking controllers are also mitigated by designing a trust-based control protocol. The efficacy of the proposed solutions is evaluated for a modified IEEE 34-bus feeder system under different types of attack.

Index Terms

AC microgrids, cooperative control, distributed control, attack, secondary control.

This material is based upon research supported in part by the U.S. Office of Naval Research under award numbers N00014-14-1-0718 and N00014-17-1-2239, and by the National Science Foundation under Grant ECCS-1405173.

S. Abhinav, F. Lewis, and A. Davoudi are with Electrical Engineering Department, the University of Texas at Arlington, TX 76019 USA (e-mail: {shankar.abhinav, lewis, davoudi}@uta.edu).

H. Modares is with the Department of Electrical and Computer Engineering, Missouri University of Science and Technology, Missouri, MO 19112 USA (e-mail: modaresh@mst.edu).

F. Ferrese is with the Naval Surface Warfare Center, Philadelphia, PA 19112 USA (e-mail: frank.ferrese@navy.mil).

I. Introduction

Distributed cooperative control of islanded AC microgrids, that uses a sparse communication network to exchange information among inverters as seen in Fig. 1, has recently emerged as a superior alternative to central control structures in microgrids [1]–[5]. Central controllers have a fully-connected, bidirectional, one-to-all communication network where the central control entity collect information from all agents, process the information centrally, and broadcast the control commands to all agents. Therefore, it features global situational awareness. This feature is missing in distributed control settings, where a sparse communication network limits node-to-node information propagation. Distributed controllers consists of local controllers with access to local data and partial neighbor data, which makes them vulnerable to malicious attacks. A malicious entity might corrupt the data exchanged by attacking the node, communication link, or hijacking the entire node. On the other hand, central controllers expose a single point-of-failure, which is a reliability bottleneck. Central controllers also require a complex and fully-connected communication network, while distributed control systems are more reliable, scalable, and flexible. The drawback of distributed control paradigms, vulnerability to cyber-attacks, is addressed in this paper.

The high-volume integration of power electronic devices in microgrids, that leverage advanced software-intensive controllers and communication networks, makes them vulnerable to future cyber attacks. Massive adaptation of computation, communication, and control will make power electronics-intensive microgrids analogous to robotic, autonomous vehicle, and other cyber-physical systems that are currently subject to cyber attacks. As predecessors to microgrids, legacy power grids with advanced communication and control have already been a subject of security vulnerability. Maroochy malicious breach of supervisory control and data acquisition [6], SQL slammer worm attack on the Davis Besse nuclear plant, and StuxNET computer worm attack on a

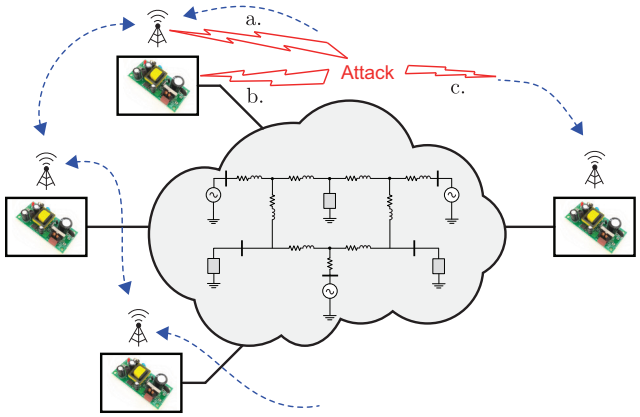

Fig. 1. A networked AC microgrid under attack: a) Controller compromised; b) Attack on sensors; c) Attack on communication links.

nuclear enrichment facility [7], exemplifying the vulnerability of cyber-physical systems.

Corrupt data can disrupt inverters' synchrony and lead to a network-wide instability. The bulk of existing research has been focused on attack detection in power systems [8]–[13]. Synergistically, mitigation techniques shall prevent the attacker from propagating its adverse effects throughout the microgrid. In a false-data injection attack, disturbances are injected to the sensors and/or actuators of agents to disrupt their transmitted data. While one could identify and remove misbehaving agents, [8], [9], this would require knowledge of the communication network, and such solutions can be difficult to scale. Computationally-efficient techniques [14] detect deception attacks on the sensors, but do not mitigate their adverse effects. Robust game-theoretic solutions [15], [16] lead to conservative results against sophisticated attacks. [17] designs an output-feedback law despite attacks on sensors, given the full knowledge of network topology. The cooperative economic dispatch in [18] uses an additional communication network to observe the original network's behavior.

An attack can be modeled similar to noise/disturbance, whose *intent* could be to destabilize the system. There exist noise filtration techniques [19] and disturbance attenuation methods [20] for multi-agent systems. Noise filtration techniques [21] usually assume certain statistical properties, e.g., they mostly assume a white Gaussian noise

signal with zero mean and finite variance. This is not valid for the case of an attack that can be deliberately designed. Disturbance attenuation techniques aim to minimize the effect of the disturbance on the local neighborhood tracking error. However, in the presence of a stealthy attack, which is considered as a constant signal in this paper, the attacker can deceive the agents by assuring that their local neighborhood tracking error is zero even in the presence of the attack. Such attacks cannot be detected or mitigated using existing disturbance attenuation or noise filtering techniques.

In this paper, resilient distributed protocols for secondary cooperative control of islanded AC microgrids under attacks are studied. The vulnerability of existing distributed controllers, in the presence of attacks on sensor/actuator, controllers, and communication links, is evaluated. To address sensor/actuator attacks, a distributed observer-based framework is presented. To mitigate attacks on communication links and hijacking of controllers, a trust/confidence-based control protocol is designed. Each inverter monitors the information it receives from its neighbors, updates its local confidence factor, and sends to its neighbors. Each inverter also updates trust factors for all its neighboring inverters (assigned to each incoming communication link). Data received at each inverter from neighbors is plugged in the distributed observer-based frequency update law, weighted by its trust factor for each neighbor and the neighbors' confidence factor. The inverters in close proximity to the attack source will have smaller confidence factor and, therefore, slow down the rate at which the corrupted data from compromised inverter spreads. This allows neighbors of the compromised inverter to assign smaller trust factors for their compromised neighbors and, therefore, eventually discards the information received, once the trust value drops below a threshold. Connectivity conditions required to ensure inverters' synchrony are explored.

This paper is organized as follows: Section II provides preliminaries of graph theory. Conventional distributed cooperative control is presented in Section III. In Section IV,

attack modeling and vulnerability of the conventional cooperative control are discussed. Section V presents the attack-resilient distributed cooperative control. Case studies, using a 34-bus IEEE feeder network with six inverters, are presented in Section VI. The conclusion is drawn in Section VII.

II. Preliminary of Graph Theory

The communication network among inverters is represented by a graph $Gr = (O, E)$, as shown in Fig. 1(b). $O = \{o_1, o_2, ..., o_n\}$ is a set of n nodes or vertices corresponding to each inverter. E is a set of edges or arcs, where each edge from o_i to o_j is denoted by (o_i, o_j), and indicates the information flow between inverters i and j. N_i is the set of inverters providing information to inverter i, also referred to as its neighbors. The graph can be represented by an adjacency matrix $\mathbf{A} = [a_{ij}]$, with weights $a_{ij} > 0$ if $(o_i, o_j) \epsilon E$, otherwise $a_{ij} = 0$. The diagonal in-degree matrix is defined as $\mathbf{D} = \mathrm{diag}\{N_i\}$.

The graph Laplacian matrix, $\mathbf{L} = \mathbf{D} - \mathbf{A}$, includes distributed system dynamics, e.g., the convergence rate. A path from node i to node j is a sequence of edges $(o_i, o_k), (o_k, o_l), ..., (o_m, o_j)$. A graph is said to have a spanning tree, if there is a root node with a path from that node to every other node in the graph. In that case, the Laplacian matrix eigenvalue $\lambda_1 = 0$ is a simple eigenvalue [22]. The solution to $\mathrm{L}\boldsymbol{\omega} = \mathbf{0}$ can be written as $\boldsymbol{\omega} = c\underline{\mathbf{1}}$, where c is a constant. Thus, synchronization is guaranteed as long as the communication graph has a spanning tree.

A leader node can be connected to some nodes (at least to one root node) by unidirectional edges. The nodes connected to the leader node and the corresponding connecting edges are called pinned nodes and pinning edges, respectively. A gain is assigned to each pinning edge, e.g., g_i is the pinning gain from the leader to the node i. The pinning gain is zero for an unpinned node. The pinning gain matrix is $\mathbf{G} = \mathrm{diag}\{g_i\}$.

III. COOPERATIVE CONTROL OF AC MICROGRIDS

A. Dynamics of the Physical Microgrid

The inverter model consists of a DC power source, inverter bridge, power sharing controller, output filter, and voltage and current controllers. Dynamics of each inverter are formulated in its own direct-quadrature (d-q) reference frame. The reference frame of one inverter is considered as the common reference frame. The power controller dynamics are

$$\begin{cases} \dfrac{\mathrm{d}P_i}{\mathrm{d}t} = -\omega_{ci}P_i + \omega_{ci}(v_{odi}i_{odi} + v_{oqi}i_{oqi}) \\ \dfrac{\mathrm{d}Q_i}{\mathrm{d}t} = -\omega_{ci}Q_i + \omega_{ci}(v_{oqi}i_{odi} - v_{odi}i_{oqi}) \end{cases}, \tag{1}$$

where v_{odi} and v_{oqi} are the direct and quadrature components of the output voltage of inverter i, while i_{odi} and i_{odi} are the corresponding current terms. P_i and Q_i are the active and reactive powers measured at inverter i. ω_{ci} is the cut-off frequency of the low-pass filter used to measure power.

The large-signal dynamical model of an inverter, with internal control loops, is adopted from [23]

$$\begin{cases} \dfrac{\mathrm{d}\mathbf{x}_i}{\mathrm{d}t} = f_i(x_i) + g(x_i)u_i \\ \mathbf{y}_i = h_i(x_i) \end{cases}, \tag{2}$$

where the state vector is

$$\mathbf{x}_i = \left[\delta_i, P_i, Q_i, \phi_{di}, \phi_{qi}, \gamma_{di}, \gamma_{qi}, i_{ldi}, i_{lqi}, v_{odi}, v_{oqi}, i_{odi}, i_{oqi}\right]. \tag{3}$$

The inductive load dynamics are modeled as

$$\begin{cases} \frac{\mathrm{d}i_{load,d}}{\mathrm{d}t} = -\frac{R_{load}}{L_{load}}i_{load,d} + \omega i_{load,q} + \frac{1}{L_{load}}v_{bd} \\ \frac{\mathrm{d}i_{load,q}}{\mathrm{d}t} = -\frac{R_{load}}{L_{load}}i_{load,q} - \omega i_{load,d} + \frac{1}{L_{load}}v_{bq} \end{cases}. \tag{4}$$

Detailed expressions for (2)-(4), and inverter parameters, can be found in [23].

Assuming inductive lines, the active and reactive power injections at bus i of the power distribution network, due to inverter i, is given by

$$\begin{cases} P_i = \frac{v_{\mathrm{mag},i} v_{\mathrm{bus},i} sin(\theta_i - \beta_i)}{Z_i} \\ Q_i = \frac{v_{\mathrm{mag},i} v_{\mathrm{bus},i} cos(\theta_i - \beta_i)}{Z_i} - \frac{v_{\mathrm{bus},i}^2}{Z_i} \end{cases} . \tag{5}$$

Z_i is the combined impedance of the output filter and the connector. $v_{\mathrm{mag},i} \angle \theta_i$ is the inverter i output voltage, and $v_{\mathrm{bus},i} \angle \beta_i$ is the voltage at bus i. Simplifying (5) leads to linear droop relationships for (P_i, ω_i) and (Q_i, v_i).

B. Primary Droop Controller

Decentralized droop techniques are conventionally adopted for the primary control of AC microgrids by linearizing the relationships for (P_i, ω_i) and (Q_i, v_i) in (5),

$$\begin{cases} \omega_i = \omega_{ni} - m_{pi} P_i \\ v_{\mathrm{mag},i} = V_{ni} - n_{qi} Q_i \end{cases} . \tag{6}$$

$v_{\mathrm{mag},i}$ and ω_i are the reference voltage and frequency, respectively, provided for the internal control loops. P_i and Q_i are the inverters active and reactive powers. m_{pi} and n_{qi} are the droop coefficients evaluated based on the inverter's ratings. ω_{ni} and V_{ni} are the set points for the primary control in (6), and are set by the secondary controller.

C. Cooperative Secondary Controller

Droop control techniques lead to a deviation of voltage and frequency from their reference set points. The secondary control provides ω_{ni} and V_{ni} in (6) to synchronize the inverters' voltages and frequencies to their reference values. This can be achieved by each inverter exchanging data only with its neighbors on the communication graph. Differentiating (6) gives the dynamics to obtain the control input ω_{ni},

$$\dot{\omega}_i = \dot{\omega}_{ni} - m_{pi}\dot{P}_i. \tag{7}$$

The auxiliary control input, u_i, is then set as

$$\dot{\omega}_i = u_i. \tag{8}$$

The cooperative frequency control law, based on the frequency information of neighbor inverters and the leader node, is

$$e_{\omega_i}(t) = \sum_{j \in N_i} a_{ij} \left(\omega_i(t) - \omega_j(t)\right) + g_i \left(\omega_i(t) - \omega_{\text{ref}}\right). \tag{9}$$

ω_i and ω_j are the frequencies of inverters i and j. N_i is the set of inverters neighboring inverter i on the communication graph. The pining gain, g_i, is non-zero for the inverters connected to the reference frequency, ω_{ref}.

The auxiliary control u_i is given by

$$u_i(t) = -c_\omega e_{\omega_i}(t). \tag{10}$$

where $c_\omega \in \mathbb{R}$ is a coupling gain. The secondary control set point, ω_{ni}, is then given by

$$\omega_{ni} = \int \left(u_i + m_{pi}\dot{P}_i\right) \mathrm{d}t. \tag{11}$$

where $\dot{P}_i$ is given by (1). A similar procedure by the authors has led to a cooperative secondary voltage control [24]. Moreover, [25]–[28] have studied the effect of communication delay on distributed secondary control of AC microgrids.

IV. Attack Modeling and Control Vulnerability

A. Attack Models

The two types of attacks, in general, include attacks on controller and attacks on communication links [8], [9], [29]. [30], [31] proved that an attacker only needs to obtain local information to launch a stealth attack. Bad data detection techniques can check the validity of the received data, but they are usually applied in a centralized manner. Distributed control of islanded AC microgrids makes them more prone to attacks that can inherently become stealth given the limited communication among inverters.

Assumption 1. Attack signal is considered to be constant. Moreover, the attacker does not send on/off commands to the actuators.

We consider a sophisticated form of attack when the attacker has knowledge of the system and can hijack controllers/corrupt communication links. The attack signal can be an arbitrary signal (not constant) or a constant one. For attack signals that are arbitrary in nature, the local neighborhood tracking error will not go to zero, and the signal can be treated as corrupted with noise. Noise filtration techniques [19] can address such an attack; e.g., the authors have previously addressed noise-resilient synchrony of AC microgrids [21]. The attack of a constant corrupted signal is more complicated, and is considered here. Controller attacks either inject a disturbance into actuators/sensors or hijack the entire controller. However, in this paper it is assumed that attacker does not any send on/off command to the actuators. If an actuator is fully turned off, there would be no control-theoretic solution, as there is no instrument to implement the control command. The attack on actuators, that drive the control input, can be modeled [8], [9] by

$$u_i^c = u_i + \mu_i u_i^a. \tag{12}$$

u_i^a is the disturbance injected into the actuator i and u_i^c is the corrupted control input.

u_i is the control input in (10). $\mu = 1$ represents the presence of attack (in which case $u_i^c = u_i + u_i^a$) and $\mu = 0$ represents absence of attack (in which case $u_i^c = u_i$).

If the entire controller is hijacked, then the attacker can corrupt the inverter's frequency. This is modeled by

$$\omega_i^c = \omega_i + \eta_i \omega_i^a. \tag{13}$$

ω_i^a is the disturbance signal injected into the controller i and ω_i^c is the corrupted inverter frequency. $\eta_i = 1$ indicates the presence of an attack.

If the communication link between two inverters is compromised (e.g., with false-data injection), the controller receives corrupted frequency information. For example, false data injection [30], [31] can corrupt the frequency information. The deception attack on communication links can be modeled by

$$\omega_i^j = \omega_i + \eta_i \omega_i^a. \tag{14}$$

where ω_i^a is the disturbance signal injected into the controller i, and ω_i^j is the frequency of inverter i communicated to inverter j. $\eta_i = 1$ indicates the presence of an attack.

B. Vulnerability of the Cooperative Control to Attacks

Theorem 1: Consider the standard synchronization protocol (9) under attack. The synchronization error is nonzero for an intact inverter, if it is *reachable* from a disrupted inverter.

Proof: Define $\omega^a = [(\omega_1^a)^{\mathrm{T}}, (\omega_2^a)^{\mathrm{T}} ... (\omega_N^a)^{\mathrm{T}}]^{\mathrm{T}}$ and $\mathbf{u}^a = [(u_1^a)^{\mathrm{T}}, (u_2^a)^{\mathrm{T}} ... (u_N^a)^{\mathrm{T}}]^{\mathrm{T}}$ as the vectors injected to sensors and actuators, respectively. Using the control protocol (8), (10), and disturbances (12)-(14), the global synchronization error dynamics, under attack, become

$$\dot{\mathbf{e}}_\omega = -c_\omega (\mathbf{L} + \mathbf{G}) \mathbf{e}_\omega. \tag{15}$$

Define $\iota = \eta(\mathbf{L}+\mathbf{G})\mathbf{e}_\omega^a + \mu\mathbf{u}$, where $\eta = \mathrm{diag}(\eta_i)$, and $\mu = \mathrm{diag}(\mu_i)$. $\eta_i = 1$ and $\mu_i = 1$ indicate the presence of attack in inverter frequency and control input respectively. The solution to (15) is

$$\mathbf{e}_\omega(t) = \mathrm{e}^{-c_\omega(\mathbf{L}+\mathbf{G})t}\mathbf{e}_\omega(0) + \int_0^t \mathrm{e}^{-c_\omega(\mathbf{L}+\mathbf{G})(t-\tau)}\iota\,\mathrm{d}\tau. \tag{16}$$

Since $(\mathbf{L}+\mathbf{G})$ is positive-definite, and c_ω is a positive constant, the first term goes to zero. Then, using $\mathrm{e}^{At} = \sum_{m=1}^{\infty}(At)^m$, one has

$$\mathbf{e}_\omega(t) \to \sum_{m=1}^{\infty}\int_0^t (-c_\omega(\mathbf{L}+\mathbf{G})(t-\tau))^m\iota\,\mathrm{d}\tau. \tag{17}$$

If $m > 0$ is the first integer, such that $l_{ij}^m = [(\mathbf{L}+\mathbf{G})^m]_{ij}$ is nonzero, then the node i is reachable from the node j, and m is the length of the shortest directed path from j to i. Therefore, if the inverter i is reachable from the disrupted inverter j, then $l_{ij}^m \neq 0$ for some $0 < m < N-1$ making the synchronization error for inverter i non-zero. This completes the proof. ■

V. Attack-resilient Cooperative Control

A. *Observer-based Cooperative Control*

Conventional cooperative control is vulnerable to attacks due to the absence of a central controller to monitor global activities. An attack on a single inverter can propagate across the network, and affect the fidelity of information used in the cooperative control law. Instead of using neighbors' information, one can use a distributed observer to track the reference frequency set point, and the attack effect can be restricted to the inverter under attack. The secondary frequency control can then be achieved by using the inverter's local frequency and its local estimation of the reference set point, using

a distributed observer that tracks the leader node's information. The control input (10) is modified into

$$u_i(t) = -c_{\hat{\omega}} \left(\omega_i(t) - \hat{\omega}_i(t) \right). \tag{18}$$

$c_{\hat{\omega}} \in \mathbb{R}$ is a coupling gain. $\hat{\omega}_i$ is the frequency observed at inverter i given by

$$\dot{\hat{\omega}}_i(t) = \sum_{j \in N_i} a_{ij} \left(\hat{\omega}_i(t) - \hat{\omega}_j(t) \right) + g_i \left(\hat{\omega}_i(t) - \omega_{\text{ref}} \right). \tag{19}$$

where $\hat{\omega}_j$ is the observed frequency at inverter j.

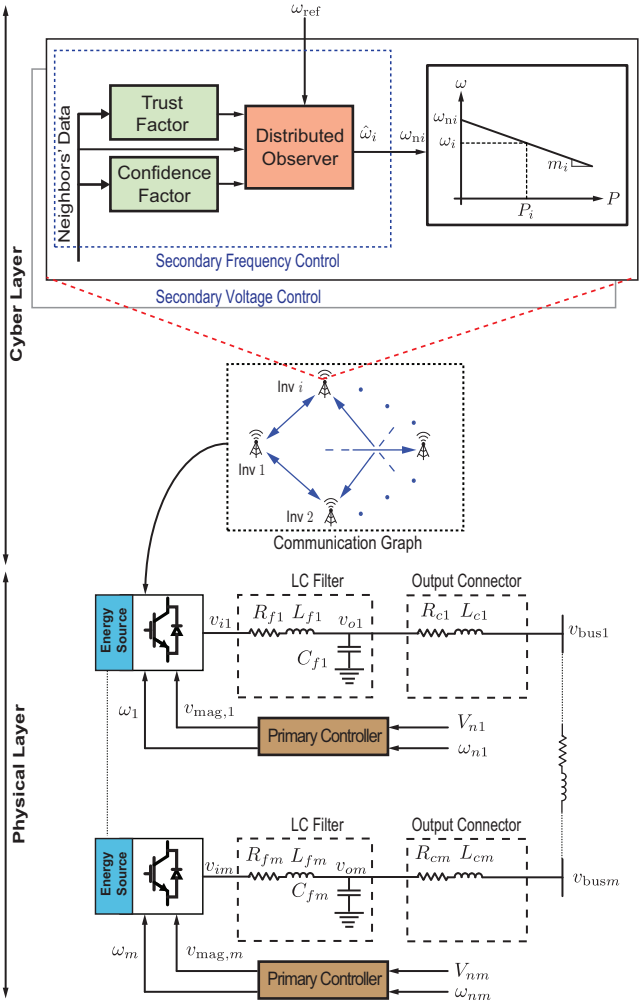

Fig. 2. Observer-based controller with trust and confidence factors.

The secondary control set point, ω_{ni}, is given by (11). From (18) and (19), it can be seen that attack on actuator/sensor modeled by (12) only effects the local frequency. Due to the separation between the communication network and the inverter local frequency, the attack is limited to the inflicted inverter and does not spread across the communication network in contrast to the conventional cooperative control.

The network of inverters has only one legitimate leader. However, if the controller of inverter i is hijacked, this inverter can be considered as an illegitimate leader that might access a subset of inverters, depending on the communication graph topology and the inverter position in graph. Since the only information exchanged is the observer's output, the compromised inverter acts as an illegitimate leader with its own observer, regardless of neighbors, to disrupt the synchronization process. The compromised inverter adds a constant to the original observer output. Consider the proposed observer (19), and define

$$e_{\hat{\omega}_i}(t) = \sum_{j \in N_i} a_{ij} \left(\hat{\omega}_i(t) - \hat{\omega}_j(t) \right) + g_i \left(\hat{\omega}_i(t) - \omega_{\text{ref}} \right). \tag{20}$$

as the local neighborhood tracking error for inverter i.

Theorem 2: Let the controllers of a subset of inverters be entirely compromised. Then, the inverters' observer output is a constant, and a convex combination of the legitimate and illegitimate leaders' state. Moreover, the local neighborhood tracking error (20) goes to zero for an intact inverter.

Proof: A leader-follower network with a single leader under attack with constant frequency output signal can be considered as a network of inverters with one legitimate leader and some illegitimate ones (compromised inverters). It is shown in the containment problem in [32] that the agents' outputs synchronize to a convex combination of the outputs of all leaders. To prove that the local neighborhood in (20) converges to zero, let $\mathbf{L}$ be the Laplacian matrix associated with the entire communication graph including the leaders. Let N and M specify the number of inverters and all leaders

(including the one legitimate leader and $M-1$ illegitimate ones). The leaders have no neighbor and, therefore, can be partitioned as

$$\mathbf{L} = \begin{bmatrix} \mathbf{L}_1 & \mathbf{L}_2 \\ 0_{M\times(N-M)} & 0_{M\times M} \end{bmatrix}. \tag{21}$$

Then, for the observer (20), one has

$$\dot{\boldsymbol{\omega}}_{\text{norm}} = (-c_{\hat{\omega}}\mathbf{L}_1)\boldsymbol{\omega}_{\text{norm}} - c_{\hat{\omega}}(\mathbf{L}_2)\boldsymbol{\omega}_{\text{l}}. \tag{22}$$

where $\boldsymbol{\omega}_{\text{norm}}$ and $\boldsymbol{\omega}_{\text{l}}$ are the stacked states of the intact inverters and the leaders, respectively. On the other hand, the local neighborhood tracking error, (19), can be written as

$$\mathbf{e}_{\hat{\omega}} = -\mathbf{L}_1\boldsymbol{\omega}_{\text{norm}} - \mathbf{L}_2\boldsymbol{\omega}_{\text{l}}. \tag{23}$$

Taking the derivative of $\mathbf{e}_{\hat{\omega}}$, and using (22) and (23), one has

$$\dot{\mathbf{e}}_{\hat{\omega}} = -c_{\hat{\omega}}\mathbf{e}_{\hat{\omega}}. \tag{24}$$

Therefore, $\mathbf{e}_{\hat{\omega}}$ goes to zero. This completes the proof. ■

If the communication link from the inverter i to the inverter j is under a deception attack, then one can assume a virtual illegitimate leader connected to the inverter j. Therefore, the local neighborhood tracking error, for inverters not under attack but afflicted by compromised links, cannot go to zero. Attacks on communication links are the same as scenarios where an inverter is compromised, except that only the neighbor reached by the affected communication link receives corrupted transmission.

B. Observer-based Control with Confidence Factors

A confidence factor is a measure of how much confidence each inverter has about its own observed frequency set point depending on whether it is in the path of an attack,

and its proximity to the attack source. The microgrid can be made more resilient if the immediate neighbors of the infected inverter detect the attack, and stop it from propagating through the network. The synchronization of intact inverters are shown under some connectivity conditions. Define

$$\varepsilon_i = ||e_{\hat{\omega}_i}|| \tag{25}$$

as the norm of the local neighborhood observer tracking error for inverter i , with $e_{\hat{\omega}_i}$ defined in (20). Based on Theorem 2, $e_{\hat{\omega}_i}$ and, consequently, ε_i converge to zero, regardless of the attack status. For the inverter i, define

$$\sigma_i = \sum_{j \in N_i} a_{ij} ||\hat{\omega}_i(t) - \hat{\omega}_j(t)|| + g_i ||\hat{\omega}_i(t) - \omega_{\text{ref}}||. \tag{26}$$

For an inverter reached from an illegitimate leader, σ_i does not converge to zero but to a steady-state value. Therefore, even though ε_i converges to zero, σ_i will reach a nonzero steady-value. In the absence of an attack, all inverters synchronize to the legitimate leader and, therefore, both ε_i and σ_i go to zero asymptotically. Using (20), one has

$$\zeta = (\mathbf{L} + \mathbf{G})\, \mathbf{e}_{\hat{\omega}}. \tag{27}$$

where $\mathbf{e}_{\hat{\omega}} = [e_{\hat{\omega}_1}^{\mathrm{T}}, e_{\hat{\omega}_2}^{\mathrm{T}}, ..., e_{\hat{\omega}_N}^{\mathrm{T}}]^{\mathrm{T}}$, with $e_{\hat{\omega}_i}$ defined in (20). $\zeta = [\zeta_1^{\mathrm{T}}, \zeta_2^{\mathrm{T}}, ..., \zeta_N^{\mathrm{T}}]^{\mathrm{T}}$ with $\zeta_i = \hat{\omega}_i - \omega_{\text{ref}}$. Since $(\mathbf{L} + \mathbf{G})$ is positive-definite, if $\mathbf{e}_{\hat{\omega}}$ converges to zero asymptotically fast, the global tracking error ζ also converges to zero asymptotically fast. On the other hand, assuming that $\mathbf{e}_{\hat{\omega}}$ is the global state vector, $(\mathbf{L} + \mathbf{G})$ is a similarity transformation matrix which gives ζ as the new state vector. Since the similarity transformation does not change system eigenvalues, in the absence of an attack, $\mathbf{e}_{\hat{\omega}}$ and ζ and, consequently, ε_i and σ_i have the same behavior. Thus, comparing ε_i and σ_i can detect whether the corresponding inverter is reachable from an illegitimate leader or not.

The confidence value for an intact inverter i is

$$\dot{C}_i(t) = \alpha d_i(t) - \alpha C_i(t). \tag{28}$$

where $0 \leqslant C_i \leqslant 1$ with

$$d_i(t) = \frac{\Delta_i}{\Delta_i + ||\sigma_i(t) - \varepsilon_i(t)||}. \tag{29}$$

$\alpha > 0$ is used to weigh the current data against the past data, Δ_i is a threshold value to consider other factors rather than attacks. If inverter i is not in the path of any attack, then $||\sigma_i - \varepsilon_i|| = 0$ in steady state and, consequently, $C_i = 1$. If inverter i is effected by an attack, then $||\sigma_i - \varepsilon_i|| >> \Delta_i$, and $C_i < 1$ depending on the proximity of inverter i to the attacked node. Taking into account the confidence level received from neighbors, the observer dynamics in (20) become

$$\begin{aligned}\dot{\hat{\omega}}_i(t) = &\sum_{j \in N_i} a_{ij} C_j(t) \left(\hat{\omega}_i(t) - \hat{\omega}_j(t)\right) \\ &+ g_i \left(\hat{\omega}_i(t) - \omega_{\text{ref}}\right).\end{aligned} \tag{30}$$

C. Observer-based Cooperative Control with Trust Factors

In the trust-incorporated observer-based cooperative control, each inverter calculates a trust value for each neighbor. If it drops below a threshold, the intact inverter discards the neighbor's information. Consider the worst-case scenario in which a compromised inverter always sends the confidence value of 1 to its neighbors to deceive them. To calculate the trust level of inverter j for inverter i, the difference between the observer output of inverter j, and the average of the observer outputs for all neighbors of inverter i, is calculated as

$$\dot{b}_{ij}(t) = \xi s_{ij}(t) - \xi b_{ij}(t). \tag{31}$$

where

$$s_{ij} = \frac{\Theta_i}{\left(\Theta_i + ||\hat{\omega}_j(t) - \frac{1}{|N_i|}\sum_{k\in N_i}\hat{\omega}_k(t)||\right)}. \tag{32}$$

$|N_i|$ is the number of neighbors of inverter i. $\xi > 0$ weighs the current data against the past data. Θ_i is a threshold value to consider other factors rather than attacks. The trust value of inverter j for inverter i is defined as

$$T_{ij} = \max\left(C_i(t), b_{ij}(t)\right). \tag{33}$$

where $0 \leqslant T_{ij} \leqslant 1$.

In the absence of an attack, $||\hat{\omega}_j - h_{N_i}|| = 0$ when the network is synchronized in steady state, where $h_{N_i} = \frac{1}{|N_i|}\sum_{k\in N_i}\hat{\omega}_k$ and, consequently, $T_{ij} \approx 1\ \forall j$. When inverter i receives different observer outputs form its neighbors, i.e., $||\hat{\omega}_j - h_{N_i}||$ is nonzero, $T_{ij} \approx 1\ \forall j$ as C_i is close to one, since the difference is caused by a change in the leader state. If inverter i is attacked, then C_i is small, and the trust of inverter j for inverter i depends on $||\hat{\omega}_j - h_{N_i}||$. The greater the difference between $\hat{\omega}_j$ and h_{N_i}, the more likely inverter j is the attack source, or in close proximity to the attack, and the less credible is its transmitted information. We assume that the immediate neighbors of the leader always trust the leader.

If the trust value for a neighboring inverter j drops below a threshold $T_{ij} < \Gamma_i$, then it is identified as a compromised inverter, and its transmitted information are discarded. This can happen if inverter j is the attack source or in its close proximity. The selection of the trust factor is done empirically, as it would depend on several factors like network connectivity, speed of convergence of the consensus algorithm and, in turn, other gains in the consensus algorithm. [18], [33]–[35] have used similar thresholds in trust factors. The purpose of threshold selection is to improve the algorithm performance by disregarding potentially corrupt data when the trust factor is low. Taking

into account the confidence level received from neighbors, and the trust values calculated for neighbors, the observer dynamics in (20) become

$$\dot{\hat{\omega}}_i(t) = \sum_{j \in N_i} a_{ij} C_j(t) T_{ij}(t) \left(\hat{\omega}_i(t) - \hat{\omega}_j(t)\right) + g_i \left(\hat{\omega}_i(t) - \omega_{\text{ref}}\right). \tag{34}$$

The overall observer-based cooperative controller, with trust factors, is presented in Fig. 2, and detailed in Algorithm 1. A similar control algorithm can be used for inverter voltages.

Algorithm 1 Secondary control of frequency using observer-based cooperative control with trust factors at inverter i

$T_{ij} = 1$ and initialize C_i.
for $t = 0, 1...$ **do**
  If $T_{ij} < \Gamma_i$, discard $\hat{\omega}_j$, and set $T_{ij} = 0$
  Update $\hat{\omega}_i$ using (34),
  Update u_i using (18),
  Update ω_{ni} using (11),
  Update C_i using (28),
  Update T_{ij} using (33),
  Transmits $\hat{\omega}_i(t)$ and $C_i(t)$ to neighbors N_i.
end for

Conditions for which the observer outputs for intact inverters synchronize to the leader are discussed.

Assumption 2. (z-local connectivity). The network connectivity is at least $(2z + 1)$, i.e., at least half of the neighbors, for each inverter, are intact [9], [33], where z is the number of neighbors under attack.

Theorem 3. Let Assumption 2 be satisfied. The distributed observer (34) for intact inverters will synchronize to the leader state, even with z compromised inverters.

Proof. If z neighbors of the inverter i are attacked, and they collude to send the same information to the inverter i, there still exists $z + 1$ intact neighbors that have different

values from the compromised ones. The compromised inverters can detect the attack and recover from it as long as Assumption 2 is satisfied. There still exists a spanning tree associated with intact inverters, as the compromised inverters are not disconnected from the communication graph. It is shown in [33] that if $T_{ij} \geqslant \Gamma_i > 0$, and there exists a spanning tree, then synchronization of intact agents is guaranteed.

If Assumption 2 is violated for the compromised inverter j, it deceptively trusts most neighbors. However, its immediate intact neighbors will have small confidence values as they receive different values from their intact neighbors and the compromised neighbor j. Therefore, the inverter j will be isolated by its neighbors to avoid spreading the attack.

VI. Case Studies

System Setup: The proposed controller is evaluated for an islanded microgrid. Figure 3 illustrates a single-line diagram of a modified IEEE 34-bus balanced test feeder [36] by averaging the line parameters provided in [36], augmented with six inverters. The specifications of the inverters connected to the test feeder are given in the Table I. The load impedances are load $1 : 1.5 + j1\ \Omega$, load $2 : 0.5 + j0.5\ \Omega$, load $3 : 1 + j1\ \Omega$, and load $4 : 0.8 + j0.8\ \Omega$ modeled using (4). The test feeder is islanded from the main grid at bus 800 at $t = 0$ s. The inverter specifications are given in the Table I and modeled using (2) and (3). The nominal frequency and line-to-line voltage are 60 Hz and 24.9 kV, respectively. The inverters are connected to the feeder through Y-Y 480V/24.9 kV, 400 kVA transformers with a series impedance of $0.03 + j0.12$ p.u. Each inverter communicates its observer frequency, observer voltage, confidence factors, and trust factors with its neighbors through the communication graph (Fig. 3(b)). Inverter 1 is pinned (receive reference signal) with pinning gain $g_1 = 1$. We consider three cases to evaluate the controller performance. Conventional secondary control is achieved by implementing (9) and (10) for frequency and equivalent voltage control, as in [24].

Case A: The attack on sensor/actuator of inverter 2 is modeled using (12) to produce an output frequency of $f_2 = 60.2$ Hz at $t = 1$ s. Figures 4(a) and 4(b) show the performance of the conventional cooperative controller, clearly leading to a loss of synchrony. Distributed observer-based secondary control of frequency is achieved by implementing (18) and (19) for frequency control. Figures 4(c) and 4(d) show the controller performance with distributed observers. Frequency at all inverters, except inverter 2 (under attack), remains synchronized at $f = 60$ Hz, and voltages of the intact inverters are much closer (but not synchronized). From Fig. 5(a), it can be seen that even if the frequency remain synchronized, the voltage exhibits an oscillatory behavior. This is expected as inverter 2 is operating at a different frequency of $f_2 = 60.2$Hz. Although the controller mitigates the attack, the physical interconnection forces the voltages to vary and exhibit the behavior seen. Nevertheless, the proposed algorithm provides the only viable solution from the distributed control perspective. It can provide time for remedial actions from operator/higher control level, e.g., disconnecting the inverter under attack (inverter 2). The voltage performance until $t = 10$sec is shown in 5(a) with no mitigating action, and in 5(b) when inverter 2 is disconnected at $t = 5$sec. It can be seen that the system performs as desired once inverter 2 is disconnected. The proposed algorithm, in this case, does not completely mitigate the attack as it is a physical attack and not cyber, but still performs adequately.

Case B: The communication link between inverters 2 and 3 is corrupted by the false-data injection modeled using (13) at $t = 1$ s. Figures 6(a) and 6(b) show the observer-based distributed controller performance, where inverters lose synchrony. This is expected since the distributed observer is using the compromised communication network. Distributed observer-based control, with confidence factors in (28), is achieved by implementing (18) and (30) for frequency control. Figures 6(c) and 6(d) show the same controller performance with confidence factors. Here, intact inverters almost reach

synchrony. Inverter 3, which receives false information, has a large deviation from 60 Hz. Distributed observer-based control is achieved by implementing (18) and (34), where confidence and trust factors are calculated using (28) and (33), respectively. The implementation of distributed observer-based secondary control of frequency with trust factors is detailed in Algorithm 1. Figures 6(e) and 6(f) show the performance of the observer-based distributed control with trust factors. The lower threshold on trust is set at $T_{ij} > 0.4$; once the trust level of a link drops below this level, it is disconnected from the graph topology. As seen, all frequency and voltage terms achieve synchrony.

Case C: The controller at inverter 2 is hijacked modeled using (14) to generate $f_2 = 60.2$ Hz during $t \in [1, 2.5]$ s. Figures 7(a) and 7(b) show the observer-based distributed controller performance where inverters lose synchrony. Figures 7(c) and 7(d) show the performance of the controller with confidence factors; inverter 2 operates at a different frequency than the set point. This shows that confidence-incorporated observer-based distributed controller is susceptible to controller hijacking. Figure 8 shows the evolution of confidence factors. The confidence factor of inverter 3, which is the immediate neighbor of compromised inverter 2 decreases significantly, which assigns less weight to data from inverter 3 decreasing the effect of the attack on other

TABLE I
INVERTER SPECIFICATIONS

	Inverters 1,2,4,5		**Inverters 3,6**	
Droop Gains	m_p	5.64×10^{-5}	m_p	7.5×10^{-5}
	n_q	5.2×10^{-4}	n_q	6×10^{-4}
Output Connector	R_c	0.03Ω	R_c	0.03Ω
	L_c	$0.35mH$	L_c	0.35mH
LC Filter	R_f	0.1Ω	R_f	0.1Ω
	L_f	1.35mH	L_f	1.35mH
	C_f	50μF	C_f	50μF

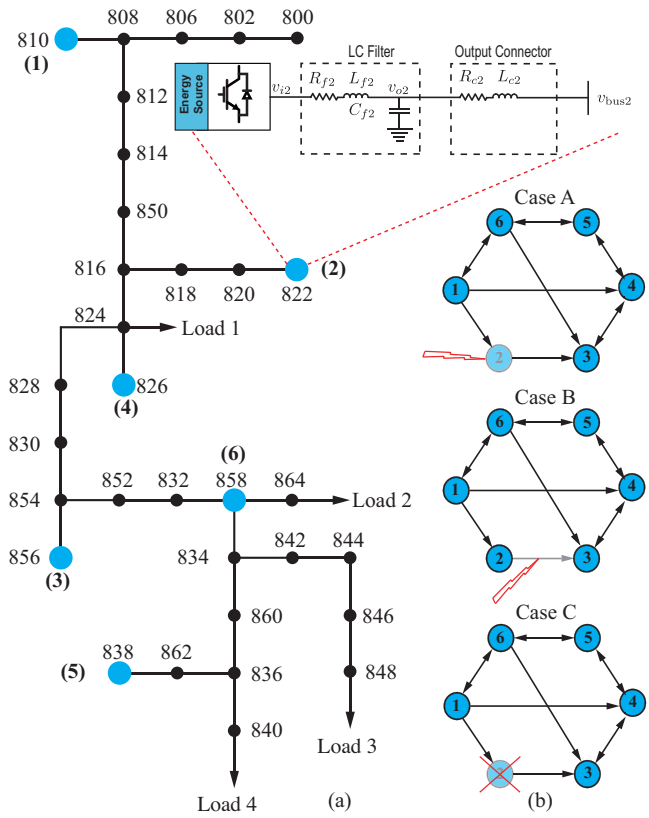

Fig. 3. (a) IEEE standard 34-bus feeder system augmented with six inverters; (b) Topology of the communication network among inverters and attacks in different cases: *Case A*-attack on an actuator/sensor, *Case B*-attack on communication links, and *Case C*-controller compromised.

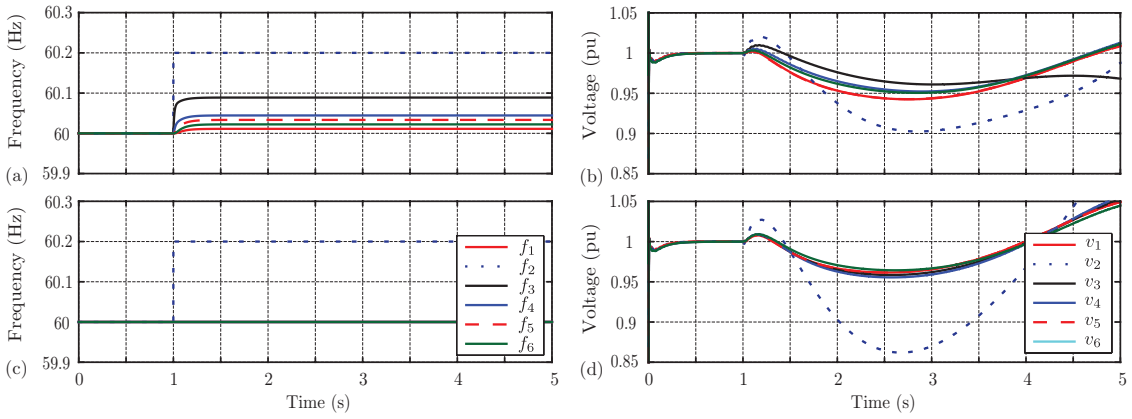

Fig. 4. Inverter 2 sensor/actuator attacked with $f_2 = 60.2$ Hz: (a),(b) Conventional cooperative control; (c),(d) Distributed observer-based cooperative control.

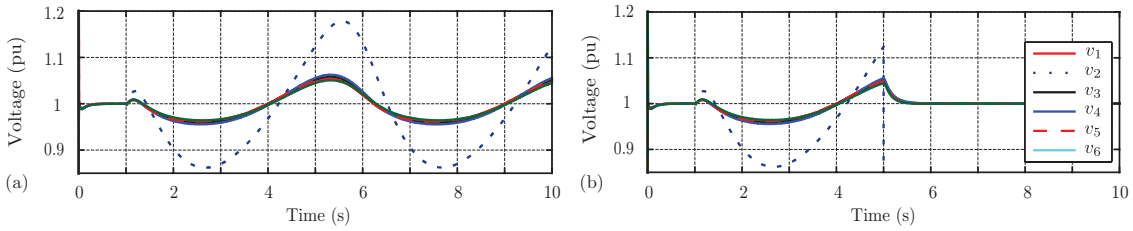

Fig. 5. Inverter 2 sensor/actuator attacked with $f_2 = 60.2$ Hz: (a) Distributed observer-based cooperative control; (b) Distributed observer-based cooperative control with inverter 2 taken offline at $t = 5$ s.

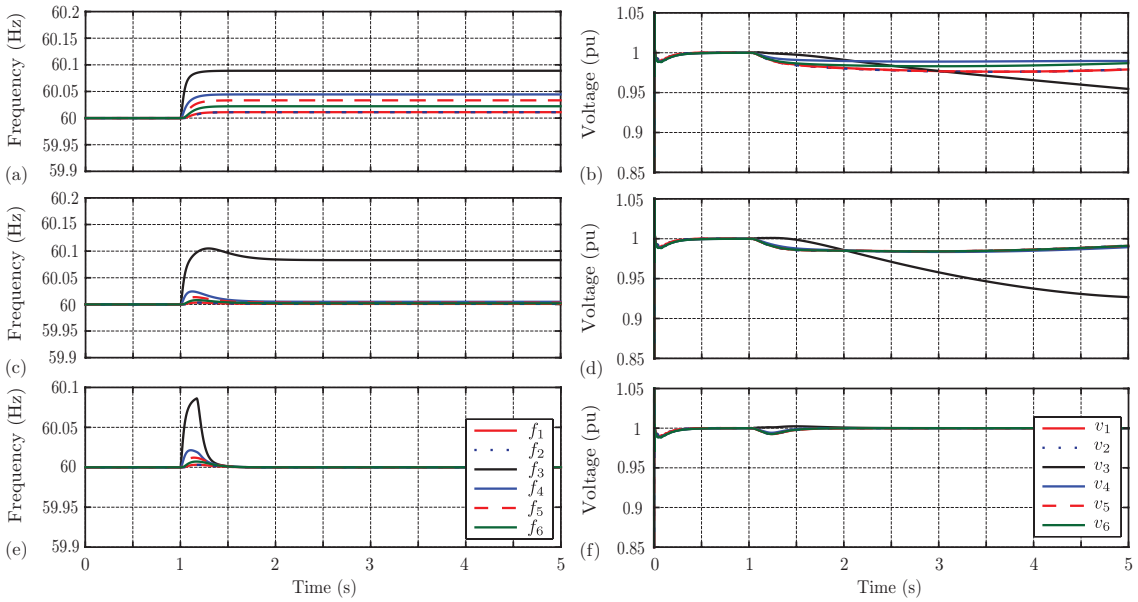

Fig. 6. The outgoing communication link from inverter 2 is attacked with $f_2 = 60.2$ Hz: (a),(b) Distributed observer-based cooperative control; (c),(d) Distributed observer-based cooperative control with confidence factors; (e),(f) Distributed observer-based cooperative control with trust factor.

inverters. Figures 7(e) and 7(f) show the performance of the controller with trust factors. The frequency of all inverters, except the hijacked one, achieve synchrony, and voltages of intact inverters are closer. Figure 9 shows the evolution of trust factors over time. Trust factor of the link from inverter 2 to inverter 3 decreases significantly, and less weight is assigned to the corrupted data from inverter 2. Communication link from inverter 2 to inverter 3 is disabled when trust factor $T_{32} < 0.4$. T_{32} in Fig. 9 goes back to 1 once the communication link is disabled.

Case D: The test feeder is islanded from the main grid at bus 800 at $t = 0$ s,

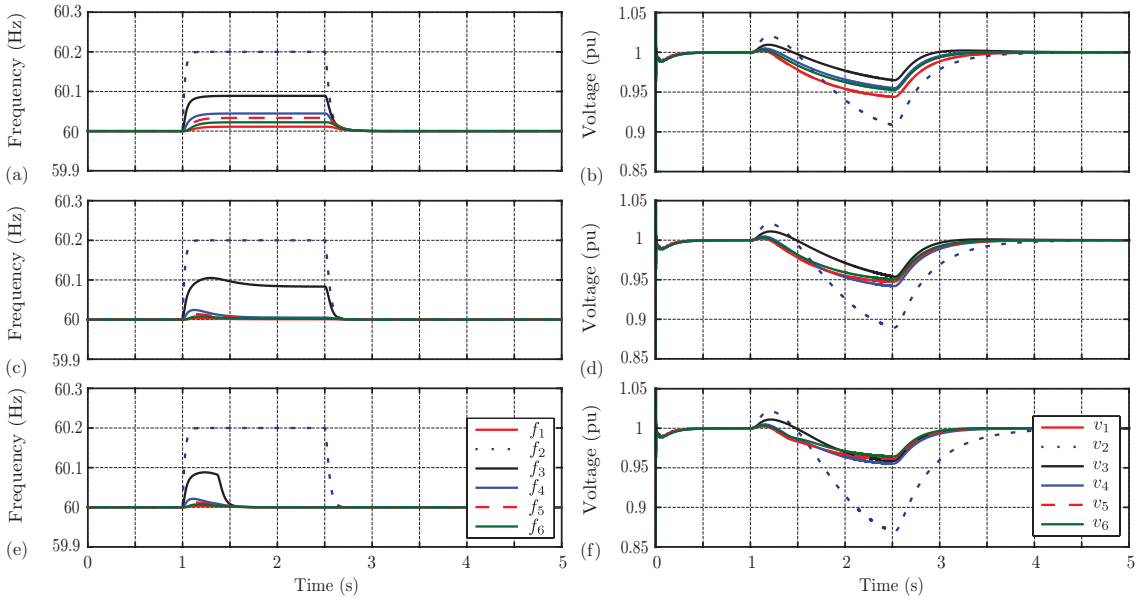

Fig. 7. Inverter 2 controller is compromised between $t = 1$ s and $t = 2.5$ s with $f_2 = 60.2$ Hz: (a),(b) Distributed observer-based cooperative control; (c),(d) Distributed observer-based cooperative control with confidence factors; (e),(f) Distributed observer-based cooperative control with trust factor.

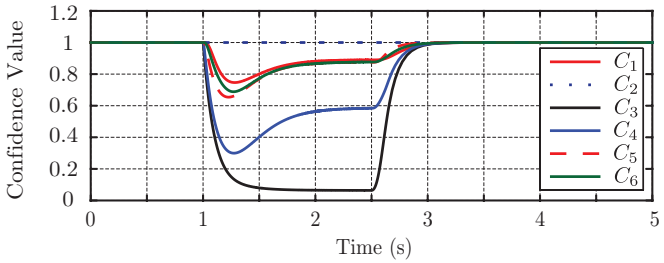

Fig. 8. Confidence levels, C_i, when the inverter 2 controller is compromised between $t = 1$ s and $t = 2.5$ s, with $f_2 = 60.2$ Hz.

and secondary control is applied at $t = 1.4$ s. The outgoing communication links from inverter 2 and 5 are corrupted by the false-data injected at $t = 1$ s as shown in Fig.10(a). The lower threshold on trust is set at $T_{ij} > 0.4$; Once the trust level of a link drops below this level, it is disconnected from the graph topology. Figures 11(a) and 11(b) show the performance of the observer-based distributed control with trust factors. The inverters lose synchrony; This is expected as Assumption 2 is not satisfied. Assumption 2 states that the communication network connectivity is at least $(2z+1)$, where z is the number

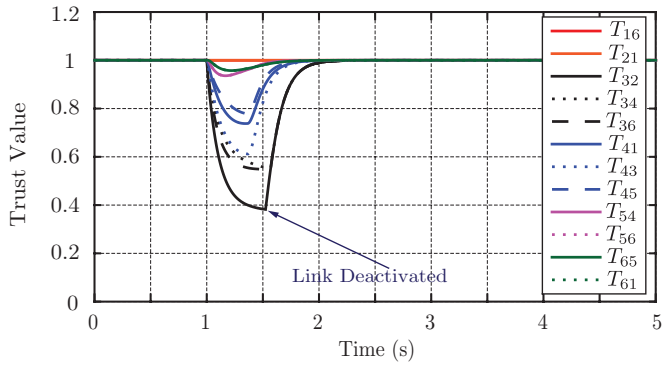

Fig. 9. Trust levels when the inverter 2 is compromised between $t = 1$ s and $t = 2.5$ s, with $f_2 = 60.2$Hz, using a distributed observer with trust factors. T_{ij} is the trust level associated to the link from inverter j to i.

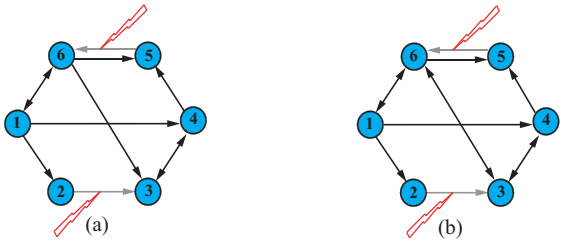

Fig. 10. Topology of the communication network among inverters during multiple attacks on communication links: (a) Network with assumption 2 $(2z+1)$ not satisfied at inverter 6; (b) Network with assumption 2 $(2z+1)$ satisfied (Communication link between inverter 3 and inverter 6 is made bidirectional).

of neighbors under attack. If this Assumption is violated for the compromised inverter j, it deceptively trusts its neighbors and microgrid cannot recover. Figure 12(a) shows the evolution of trust factors over time. In the current network represented by Fig. 10(a), inverter 6 is only receiving information from inverters 5 and 1, that does not satisfy the assumption. Figures 11(c) and 11(d) show the same controller performance with trust factors when a modified communication network shown in Fig.10(b), that satisfies Assumption 2, is used. As seen, all frequency and voltage terms achieve synchrony, that ascertains the importance of network connectivity conditions. Figure 12(b) shows the evolution of trust factors over time. Trust factors of links from inverter 2 to inverter 3, and from inverter 5 to inverter 6, decreases, as less weight is assigned to the corrupted data from inverters 2 and 5.

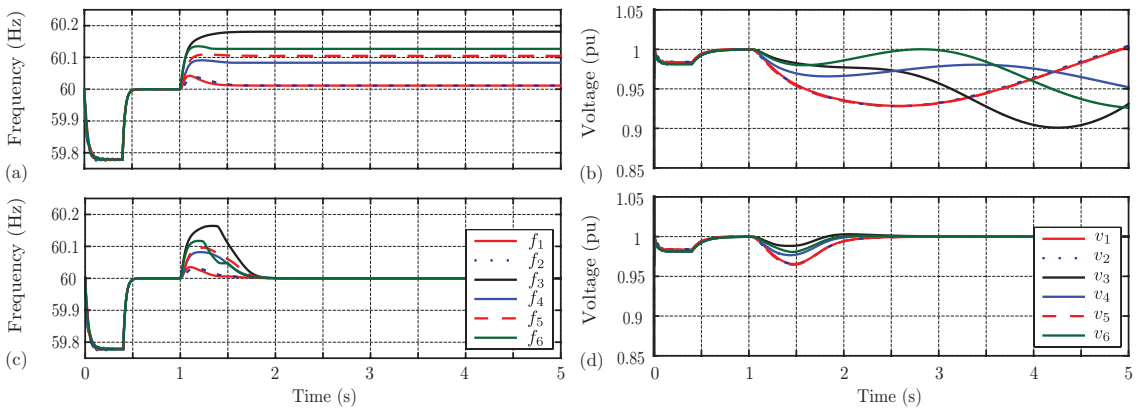

Fig. 11. The outgoing communication links from inverter 2 and 5 are attacked with $f_2 = 60.2$ Hz: (a),(b) Distributed observer-based cooperative control with trust factors using communication topology in Fig. 10(a); (c),(d) Distributed observer-based cooperative control with trust factor using communication topology in Fig. 10(b).

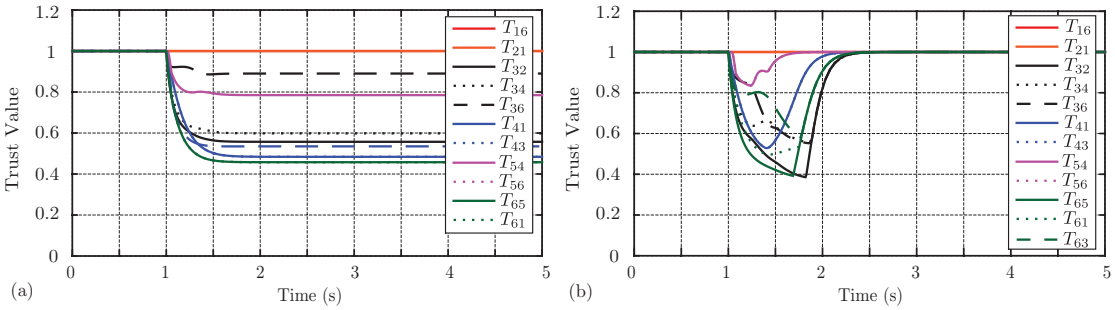

Fig. 12. Trust levels when the outgoing communication links from inverter 2 and 5 are attacked with $f_2 = 60.2$ Hz, using distributed observers with trust factors: (a) Using communication topology in Fig. 10(a); (b) Using communication topology in Fig. 10(b).

VII. Conclusion

Attack-resilient distributed synchronization of inverter-based networked AC microgrids is addressed. The vulnerability of the standard cooperative control to attacks on sensor/actuator and communication links, and controller hijacking, is shown. A distributed observer-based cooperative controller is presented to address sensors/actuators attacks. It is then augmented with confidence and trust factors to make the microgrid more resilient to attacks on communication links and hijacking controllers. The resilience of the proposed control techniques is evaluated for a modified 34-bus IEEE

feeder system for different types of attacks.

REFERENCES

[1] A. Bidram, A. Davoudi, F. Lewis, and J. Guerrero, "Distributed cooperative secondary control of microgrids using feedback linearization," *IEEE Trans. Power Syst.*, vol. 28, no. 3, pp. 3462–3470, Aug 2013.

[2] J. Simpson-Porco, Q. Shafiee, F. Dorfler, J. Vasquez, J. Guerrero, and F. Bullo, "Secondary frequency and voltage control of islanded microgrids via distributed averaging," *IEEE Trans. Ind. Electron.*, vol. 62, no. 11, pp. 7025–7038, Nov 2015.

[3] J. Schiffer, T. Seel, J. Raisch, and T. Sezi, "Voltage stability and reactive power sharing in inverter-based microgrids with consensus-based distributed voltage control," *IEEE Trans. Control Syst. Technol.*, vol. 24, no. 1, pp. 96–109, Jan 2016.

[4] F. Guo, C. Wen, J. Mao, J. Chen, and Y.-D. Song, "Distributed cooperative secondary control for voltage unbalance compensation in an islanded microgrid," *IEEE Trans. Ind. Informat.*, vol. 11, no. 5, pp. 1078–1088, Oct 2015.

[5] M. Tahir and S. Mazumder, "Self-triggered communication enabled control of distributed generation in microgrids," *IEEE Trans. Ind. Informat.*, vol. 11, no. 2, pp. 441–449, April 2015.

[6] J. Slay and M. Miller, *Lessons Learned from the Maroochy Water Breach*. Boston, MA: Springer US, 2008, pp. 73–82.

[7] J. P. Farwell and R. Rohozinski, "Stuxnet and the future of cyber war," *Survival*, vol. 53, no. 1, pp. 23–40, 2011.

[8] F. Pasqualetti, A. Bicchi, and F. Bullo, "Consensus computation in unreliable networks: A system theoretic approach," *IEEE Trans. Autom. Control*, vol. 57, no. 1, pp. 90–104, Jan 2012.

[9] 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.

[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] Y. Huang, J. Tang, Y. Cheng, H. Li, K. A. Campbell, and Z. Han, "Real-time 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.

[12] 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.

[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, no. 2, pp. 612–621, March 2014.

[14] 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.

[15] T. Alpcan and T. Basar, "A game theoretic approach to decision and analysis in network intrusion detection," in *Proc. 42nd IEEE Conference on Decision and Control*, vol. 3, Dec 2003, pp. 2595–2600.

[16] P. Srikantha and D. Kundur, "A der attack-mitigation differential game for smart grid security analysis," *IEEE Trans. Smart Grid*, vol. 7, no. 3, pp. 1476–1485, May 2016.

[17] H. Fawzi, P. Tabuada, and S. Diggavi, "Secure estimation and control for cyber-physical systems under adversarial attacks," *IEEE Trans. Autom. Control*, vol. 59, no. 6, pp. 1454–1467, June 2014.

[18] Y. Liu, H. Xin, Z. Qu, and D. Gan, "An attack-resilient cooperative control strategy of multiple distributed generators in distribution networks," *IEEE Trans. on Smart Grid*, vol. 7, no. 6, pp. 2923–2932, Nov 2016.

[19] M. Basseville, I. V. Nikiforov *et al.*, *Detection of abrupt changes: theory and application*. Prentice Hall Englewood Cliffs, 1993, vol. 104.

[20] Q. Jiao, H. Modares, F. L. Lewis, S. Xu, and L. Xie, "Distributed l_2-gain output-feedback control of homogeneous and heterogeneous systems," *Automatica*, vol. 71, pp. 361 – 368, 2016.

[21] S. Abhinav, I. Schizas, F. Lewis, and A. Davoudi, "Distributed noise-resilient networked synchrony of active distribution systems," *IEEE Trans. Smart Grid*, 2016, to be published.

[22] R. Olfati-Saber and R. Murray, "Consensus problems in networks of agents with switching topology and time-delays," *IEEE Trans. Autom. Control*, vol. 49, no. 9, pp. 1520–1533, Sept 2004.

[23] A. Bidram, F. Lewis, and A. Davoudi, "Distributed control systems for small-scale power networks: Using multiagent cooperative control theory," *IEEE Control Syst.*, vol. 34, no. 6, pp. 56–77, Dec 2014.

[24] A. Bidram, A. Davoudi, F. Lewis, and Z. Qu, "Secondary control of microgrids based on distributed cooperative control of multi-agent systems," *IET Gener. Transmiss. Distrib.*, vol. 7, no. 8, pp. 822–831, Aug 2013.

[25] V. Nasirian, Q. Shafiee, J. M. Guerrero, F. L. Lewis, and A. Davoudi, "Droop-free distributed control for ac microgrids," *IEEE Trans. Power Electron.*, vol. 31, no. 2, pp. 1600–1617, Feb 2016.

[26] Q. Shafiee, V. Nasirian, J. C. Vasquez, J. M. Guerrero, and A. Davoudi, "A multi-functional fully distributed control framework for ac microgrids," *IEEE Trans. Smart Grid*, 2016, to be published.

[27] Q. Shafiee, C. Stefanovic, T. Dragicevic, P. Popovski, J. C. Vasquez, and J. M. Guerrero, "Robust networked control scheme for distributed secondary control of islanded microgrids," *IEEE Trans. Ind. Electron.*, vol. 61, no. 10, pp. 5363–5374, Oct 2014.

[28] Q. Shafiee, J. M. Guerrero, and J. C. Vasquez, "Distributed secondary control for islanded microgrids: A novel approach," *IEEE Trans. Power Electron.*, vol. 29, no. 2, pp. 1018–1031, Feb 2014.

[29] S. Amin, G. A. Schwartz, and S. S. Sastry, "Security of interdependent and identical networked control systems," *Automatica*, vol. 49, no. 1, pp. 186 – 192, 2013.

[30] X. Liu and Z. Li, "Local load redistribution attacks in power systems with incomplete network information," *IEEE Trans. Smart Grid*, vol. 5, no. 4, pp. 1665–1676, July 2014.

[31] ——, "False data attacks against ac state estimation with incomplete network information," *IEEE Trans. Smart Grid*, 2016, to be published.

[32] 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," *International Journal of Robust and Nonlinear Control*, vol. 23, no. 5, pp. 534–547, 2013.

[33] H. J. LeBlanc, H. Zhang, X. Koutsoukos, and S. Sundaram, "Resilient asymptotic consensus in robust networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 4, pp. 766–781, April 2013.

[34] J. Duan, W. Zeng, and M. Y. Chow, "Resilient distributed dc optimal power flow against data integrity attack," *IEEE Trans. Smart Grid*, 2016, to be published.

[35] 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.

[36] N. Mwakabuta and A. Sekar, "Comparative study of the IEEE 34 node test feeder under practical simplifications," in *Proc. 39th North Amer. Power Symp.*, Las Cruces, NM, USA, 2007, pp. 484–491.

CHAPTER 5

RESILIENT COOPERATIVE CONTROL OF DC MICROGRIDS

Authors: S. Abhinav, H. Modares, and A. Davoudi.

Reprinted, with permission from all the co-authors.

Resilient Cooperative Control of DC Microgrids

Shankar Abhinav*, Hamidreza Modares†, Ali Davoudi*

*Electrical Engineering Department, University of Texas at Arlington, TX 76019 USA

Email: shankar.abhinav@mavs.uta.edu

†Department of Electrical and Computer Engineering,

Missouri University of Science and Technology, Missouri, MO 19112 USA

Abstract

The existing cooperative secondary control for DC microgrids are vulnerable to cyber attacks. A trust-based cooperative current sharing controller is proposed, that can mitigate adverse effects of attacks on communication links and controller hijacking. The trust-based cooperative controller only requires local and neighbor information to detect an attack. The proposed controller is able to distinguish between attacks and change in loading conditions occurring naturally. The proposed solution is evaluated using a Hardware in the Loop setup under different types of attack.

I. Introduction

DC microgrids are the natural evolution of reliable power systems, which is moving towards renewable energy sources, storage units, and electronic loads [1], [2]. Distributed cooperative control of DC microgrids has garnered much attention in literature recently. Distributed control [3]–[5] increases reliability by not having a single point of failure, unlike in centralized control [6]. However, the lack of a central controller makes it challenging to identify and mitigate attacks. Cyber attacks [7]–[9] as seen in Fig. 1

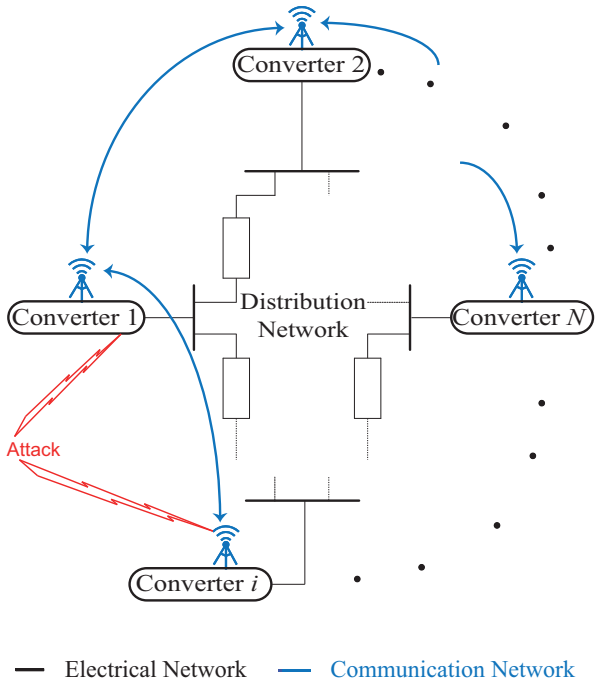

Fig. 1. A networked DC microgrid under attack.

are of particular importance in future DC microgrids, since they will be controlled by advanced processors leveraging communication.

Trust-based cooperative distributed paradigm used to mitigate cyber attacks for secondary cooperative control of current sharing for DC microgrids is studied in this paper. Every converter calculates a trust factor for all its neighboring converters (in the communication graph). Information received from each converter is used in the cooperative distributed current sharing paradigm, weighted by its trust value for that converter. The trust value has a temporal factor to accommodate natural changes in the system , such as load change that disrupts the system for a short period of time. The converter closest to converter under attack will develop a smaller trust value of the converter under attack and, therefore, slow down the rate at which the corrupted data from converter under attack spreads. Eventually once the trust value becomes less than a threshold value, information from the compromised converter is removed from the control paradigm, mitigating the attack.

This paper is organized as follows. Preliminary of graph theory is presented in Section II. Section III provides the standard distributed cooperative control. In Section IV, attack modeling is discussed. Section V presents the trust-based cooperative control of current sharing for DC microgrids. Case studies, using a Hardware in the Loop setup with sixteen converters, are presented in Section VI. The conclusion is drawn in Section VII.

II. Preliminary of Graph Theory

The communication network among converters can be represented by a graph Gr, as shown in Fig. 1. Each converter can be represented by a node on the communication graph, where $O = \{o_1, o_2, ..., o_n\}$ is the set of nodes mapped to each converter. Each converter receives information from its neighbors N_i. The graph dynamics are represented by the adjacency matrix $\mathbf{A} = [a_{ij}]$. $a_{ij} = 0$ if communication link is absent, otherwise $a_{ij} > 0$. If there is atleast one root node with a path from that node to every other node in the graph, then the graph has a spanning tree.

III. Secondary Cooperative Control

Figure 2 represents a DC microgrid comprising of different energy sources connected to converters, physical interconnections, and the cyber layer comprising of communication and control. The secondary control in a DC microgrid has two objectives: voltage regulation and proportional load sharing across the different sources. In this paper we assume that the converters are voltage controlled locally, i.e., the local controller is PI controller $J(S)$ that receives a voltage set point from the secondary controller.

The voltage set point for the local controller for converter i is calculated by using both current sharing and voltage regulation error terms, expressed as follows [3], [5]:

$$v_i^* = v_i^{\text{ref}} - r_i i_i + \delta v_i^i + \delta v_i^v \tag{1}$$

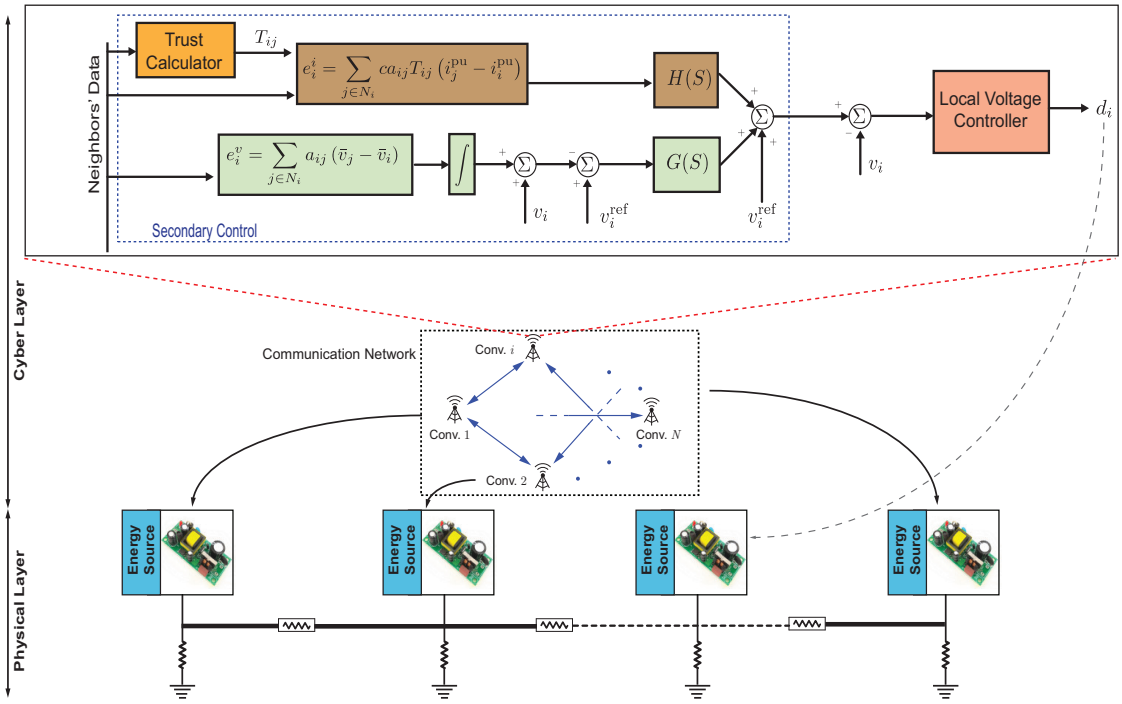

Fig. 2. Trust based Distributed cooperative controller

where v_i^{ref} and r_i are the reference voltage and the virtual impedance (droop coefficient). δv_i^v and δv_i^i are the voltage and current sharing correction terms for converter i.

The voltage regulator consists of a voltage estimator and a PI controller $G(S)$. The voltage estimator estimates the average voltage across the microgrid by utilizing dynamic consensus as follows [3], [5]:

$$\bar{v}_i(t) = v_i(t) + \int_0^t \sum_{j\in N_i} a_{ij}(\bar{v}_j(\tau) - \bar{v}_i(\tau))\,\mathrm{d}\tau \tag{2}$$

where $\bar{v}_i$ and $\bar{v}_j$ are the average microgrid voltage estimate at converter i and converter j respectively.

The average voltage estimated using (2) is then compared with reference voltage and fed to the PI controller $G(S)$ to generate the voltage correction term [3], [5].

To ensure proportional load sharing a current sharing correction term is calculated by exchanging the per unit current of individual converters. The per unit current is current

supplied by the converter divided by its current rating, i.e., $i_i^{\mathrm{pu}} = i_i / I_i^{\mathrm{rated}}$, where i_i and I_i^{rated} are the output current and rated current of converter i. The current sharing regulator calculates the local current sharing mismatch e_i^i detailed in section III and passes it through a PI controller $H(S)$ to generate the current sharing correction term δv_i^i.

IV. Attack Modeling

In general there are two types of attack: attack on communication network and controller hijacking [7]–[9]. Attacks on communication network comprises of false data injection into the communication link, in order to destabilize the system. A communication link attack on the current sharing information exchanged from converter j to converter i can be modeled as

$$i_j^{\mathrm{pu},i} = i_j^{\mathrm{pu}} + \mu_i \omega. \tag{3}$$

where ω is the corrupt data added into the communication link, and $i_j^{\mathrm{pu},i}$ is per unit current of converter j received by i. $\mu_i = 1$ when the attack is active.

For controller hijacking, controller at a converter changes its control to destabilize the system. A controller hijacking attack on the current sharing control for converter i can be modeled as

$$i^{\mathrm{pu,c},i} = (1 - \mu_i) i^{\mathrm{pu},i} + \mu_i \chi. \tag{4}$$

where χ is the corrupted data to which the per unit current at converter i is set by the attacker, and $i^{\mathrm{pu},i}$ is normal per unit current of converter i. $\mu_i = 1$ when the attack is active.

V. Trust-based Current Sharing Cooperative Control

A trust based current sharing cooperative controller is depicted in Fig. 2. It uses a trust value to weigh neighbors information. Norm of the current sharing mismatch at

converter i is defined as

$$\delta_i^i = || \sum_{j \in N_i} ca_{ij} \left(i_j^{\mathrm{pu}}(t) - i_i^{\mathrm{pu}}(t) \right) || \tag{5}$$

where c is the coupling gain. i_i^{pu} and i_j^{pu} are the per unit current for converter i and j respectively. For the converter i, another error norm is defined as

$$\sigma_i^i = \sum_{j \in N_i} ca_{ij} || i_j^{\mathrm{pu}}(t) - i_i^{\mathrm{pu}}(t) ||. \tag{6}$$

If converter i is under attack σ_i^i does not asymptotically reach zero, whereas δ_i^i will converge to zero. When the converter is not under attack both σ_i^i and δ_i^i asymptotically reach zero, indicating convergence of all the per unit currents. Therefore, this disparity between the σ_i^i and δ_i^i can be exploited to detect attack locally for converter i.

The local confidence value for converter i can be defined as

$$\dot{C}_i(t) = \alpha d_i(t) - \alpha C_i(t). \tag{7}$$

where

$$d_i(t) = \frac{\Delta_i}{\Delta_i + ||\sigma_i^i(t) - \delta_i^i(t)||}. \tag{8}$$

$\alpha > 0$ allows to add a temporal factor, in order to account for natural changes in the system such as load change. Δ_i is a threshold value to normalize the magnitude of attack. For converter i when the system is not under attack, asymptotically $||\sigma_i^i - \delta_i^i|| \to 0$ resulting in $C_i \approx 1$. For converter i during attack, then $||\sigma_i^i - \delta_i^i|| \neq 0$ making $C_i < 1$. Local confidence value is lower for converters that are closer to the attack location.

$$\dot{b}_{ij}(t) = \xi s_{ij}(t) - \xi b_{ij}(t). \tag{9}$$

where

$$s_{ij} = \frac{\Theta_i}{\left(\Theta_i + ||i_j^{\mathrm{pu}}(t) - \frac{1}{N_i}\sum_{k\in N_i} i_k^{\mathrm{pu}}(t)||\right)}. \tag{10}$$

N_i is the converters sending information on communication graph to converter i. $\xi > 0$ allows to add a temporal factor, in order to account for natural changes in system such as load change. Θ_i is a threshold value to normalize the magnitude of attack. Trust value of converter j calculated by converter i is given by

$$T_{ij} = \max\left(C_i(t), b_{ij}(t)\right). \tag{11}$$

During normal operation, asymptotically $||i_j^{\mathrm{pu}} - (\sum_{k\in N_i} i_k^{\mathrm{pu}}/N_i)|| \rightarrow 0$, resulting in $T_{ij} \approx 1\ \forall j$. During an attack, converter i receives different current sharing information from its neighbors, i.e., $||i_j^{\mathrm{pu}} - (\sum_{k\in N_i} i_k^{\mathrm{pu}}/N_i)|| \neq 0$ then C_i decreases, and the trust value of converter j calculated by converter i is directly related to $||i_j^{\mathrm{pu}} - h_{N_i}||$. Larger the difference between the neighbor current sharing information, lower the value of T_{ij}. To ensure attack resilient operation, it is important that at least one more than half of the neighbors, for each converter, are not compromised [10], [11]. Only then can the compromised converters be identified and isolated.

If the trust value for any converter becomes less than a minimum value $T_{ij} < \Gamma_i$, then information received from converter j is removed from the control structure of converter i. The current sharing dynamics becomes

$$e_i^i(t) = \sum_{j\in N_i} ca_{ij} T_{ij}(t)\left(i_j^{\mathrm{pu}}(t) - i_i^{\mathrm{pu}}(t)\right). \tag{12}$$

During attack the trust value associated to the neighbor supplying corrupted data goes down, the weight associated to the neighbor decreases and thus the propagation of attack across the network is restricted. The average per unit current obtained using (12) fed to the PI controller $H(S)$ to generate the current correction term [3]–[5]. The trust-based

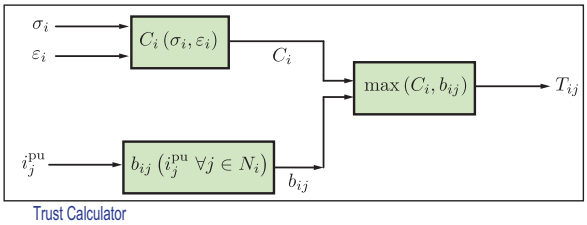

Fig. 3. Trust Calculator block diagram

cooperative controller is presented in Fig. 2, and detailed in Fig. 3. A similar trust based control can be derived for converter voltage correction term.

VI. Hardware in the loop Verification

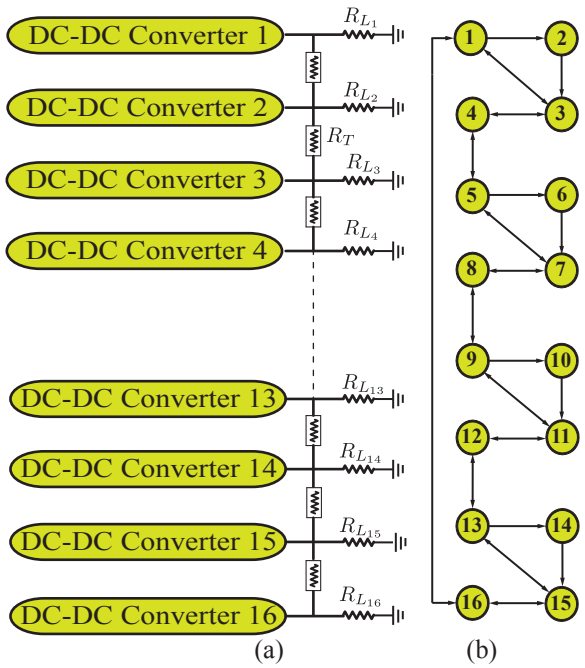

Fig. 4. a) Block diagram of a 16 converter system; (b) Topology of the communication network among converters

A 48 V islanded DC microgrid comprising of sixteen converters is considered as shown in Fig. 4(a). Each converter communicates its reference voltage estimate, per unit current to its neighbors using the communication graph shown in Fig. 4(b). Each converter has a local load as detailed in Table I, and the current rating of each converter is detailed in Table II. The physical microgrid shown in Fig. 4(a) is emulated by 4

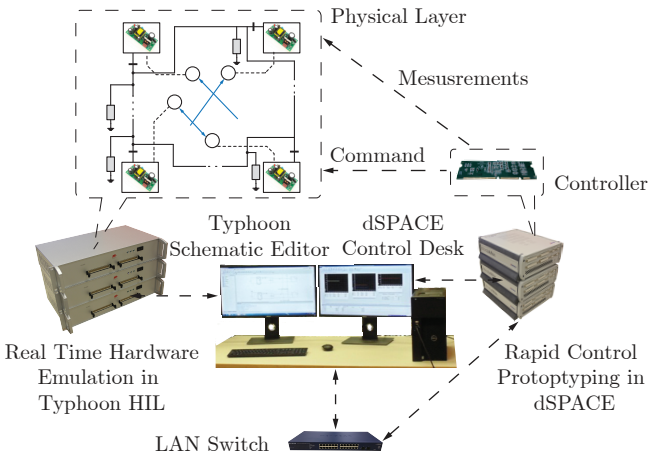

Fig. 5. Hardware in the Loop setup: Comprising of Typhoon 603 HILs, dSPACE ds1202 MicroLabBox, and a computer to monitor and program.

Typhoon HIL 603 (connected in a ring fashion using a Gigabit per second serial link). Each Typhoon HIL 603 emulates the physical characteristics of four converters.

The control is modeled in SIMULINK then deployed on 4 dSPACE ds1202 MicroLabBoxs'. Each MicroLabBox is paired with a Typhoon HIL 603. MicroLabBox receives the physical measurements from the Typhoon HIL 603, and sends out the four switching signals for the four converters emulated in the Typhoon HIL 603. The MicroLabBoxs' are connected to a monitoring computer using Ethernet connection via a LAN switch. Another LAN switch is used to facilitate transfer of information between the MicroLabBoxs' using TCP/IP. For the trust-based cooperative current control the threshold for trust value is set at 0.35. If the trust value of a converter drops below this value, it is disconnected from the communication graph of the converter that calculates trust shown in Fig. 4(b) till the trust value recovers.

Case A: Single Attack The incoming communication link at converter 2 from 3 is attacked with constant false data ($\omega = 0.4$, as modeled in (3)) at $t = 0.5$ s. Figures 6(a) and 7(a) show current and voltage outputs of converters $1-4$ and $7-8$, while using the conventional current sharing cooperative controller. It can been seen from

TABLE I
LOAD SPECIFICATIONS

Converter	Load Resistance (Ω)
5,9,13	30
1-4,6-8,10-12,14-16	20

TABLE II
CURRENT RATING

Converter	Current Rating (A)
1,4,5,8,9,12,13,16	6
2,3,6,7,10,11,14,15	3

Fig. 6(a) that current sharing is lost due to the compromised communication network. Figures 6(b) and 7(b) show the performance when using a trust-based current sharing cooperative controller. As seen, current sharing is maintained, trust value for incoming communication link at converter 2 from 3, T_{32}, is set to zero when the trust value drops below 0.35. Once the attack is removed at $t = 9.8$ s, the trust for the incoming communication link at converter 2 from 3 , T_{32}, goes above the threshold; it is included in the communication graph topology as shown in Fig.10(a) and quickly reaches T_{32} 1.

Case B: Multiple Attack The incoming communication link at converter 2 from 3, link at converter 7 from 6, and link at converter 11 from 10 is attacked with constant false data ($\omega = 0.4$, as modeled in (3)) at $t = 0.5$ s. Figure 6(c) shows current outputs of converters $1 - 4$ and $7 - 8$, while using the conventional current sharing cooperative controller. It can been seen from Fig. 6(c) that current sharing is lost due to the compromised communication network. Figure 6(d) shows the performance when using a trust-based current sharing cooperative controller. As seen, current sharing is maintained, trust value T_{32}, T_{76}, is set to zero when the trust value drops below 0.35 as shown in Fig.10(b).

Case C: Time-Varying Attack The incoming communication link at converter 2 from 3 is attacked with sinusoidal varying false data ($0.4sin(t)$, as modeled in (3)) at $t = 0.5$ s.

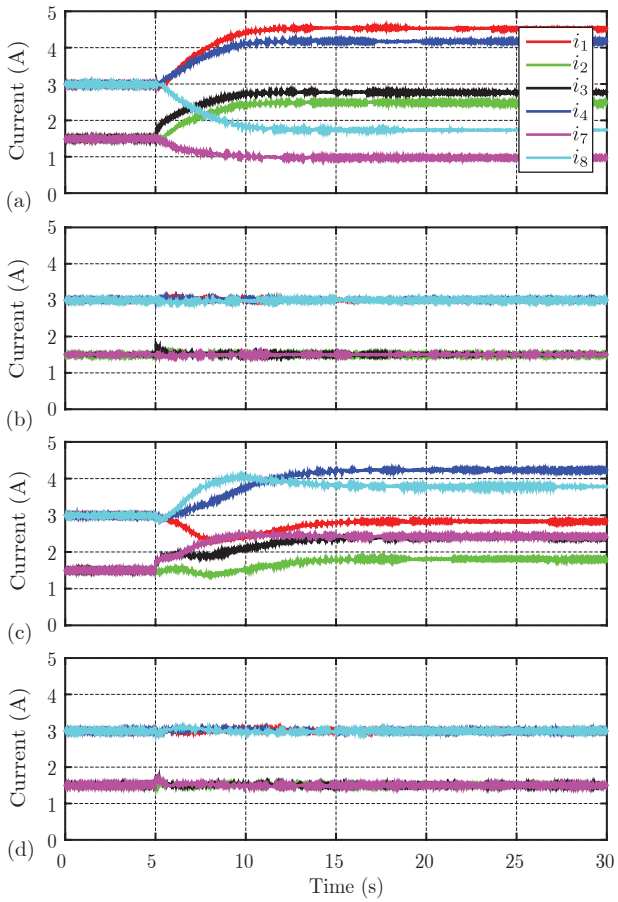

Fig. 6. Current of converters: a) Without trust when communication link at converter 3 from converter 2 is attacked with a constant false data; b) With trust when communication link at converter 3 from converter 2 is attacked with a constant false data; c) Without trust when communication link at converter 3 from converter 2, communication link at converter 7 from converter 6 and communication link at converter 11 from converter 10 is attacked with constant false data; d) With trust when communication link at converter 3 from converter 2, communication link at converter 7 from converter 6 and communication link at converter 11 from converter 10 is attacked with constant false data

Figure 8(a) shows current of converters $1-4$ and $7-8$, while using the conventional current sharing cooperative controller. It can been seen from Fig. 8(a) that current sharing is lost due to the compromised communication network. Figure 8(b) shows the performance when using a trust-based current sharing cooperative controller. As seen, current sharing is maintained.

Case D: Controller Hijacking Attack The controller at converter 2 is hijacked to produce a constant current output ($\chi = 0.2$, as modeled in (4)) irrespective of the

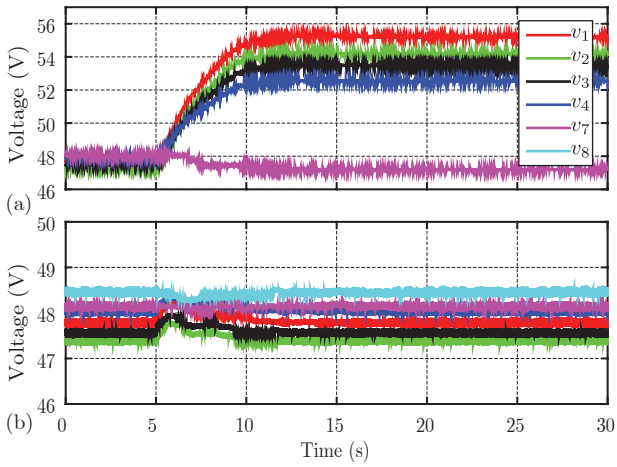

Fig. 7. Voltage of converters: a) Without trust when communication link at converter 3 from converter 2 is attacked with a constant false data; b) With trust when communication link at converter 3 from converter 2 is attacked with a constant false data

cooperative controller at $t = 0.5$ s. Figure 8(c) shows current outputs of converters $1-4$ and $7-8$, while using the conventional current sharing cooperative controller. It can been seen from Fig. 8(a) that current sharing is lost due to the compromised communication network. Figure 8(b) shows the performance when using a trust-based current sharing cooperative controller. As seen, current sharing is maintained except in the hijacked one.

Case E: Load Change The local load at converter 7 is changed from 20 Ω to 30 Ω at $t = 0.5$ s. Figure 9(a) shows current of converters $1-4$ and $7-8$, while using the conventional current sharing cooperative controller. It can been seen from Fig. 9(a) that current sharing is maintained. Figure 9(b) shows the performance when using a trust-based current sharing cooperative controller. As seen, current sharing is maintained and similar performance as the conventional cooperative controller is observed.

VII. Conclusion

Attack-resilient distributed control of DC microgrids is addressed. Two types of attacks are studied: attack on communication channels and controller hijacking. A

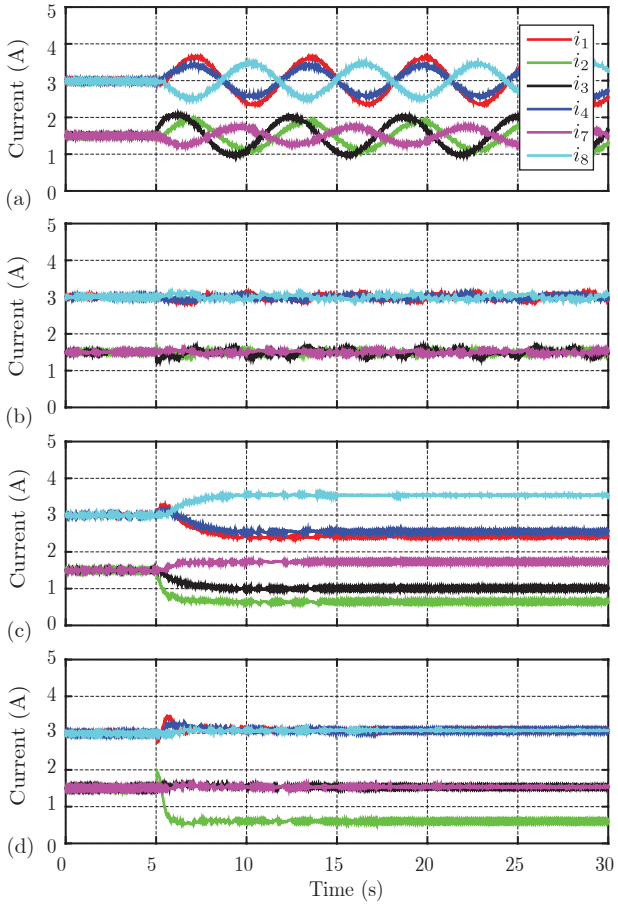

Fig. 8. Current of converters: a) Without trust when the incoming communication link at converter 3 from converter 2 is attacked with a time-varying false data; b) With trust when the incoming communication link at converter 3 from converter 2 is attacked with time-varying false data; c) Without trust when controller at converter 2 is hacked; d) With trust when controller at converter 2 is hacked;

trust-based cooperative current controller is proposed to maintain current sharing. The proposed method is evaluated using a Hardware in the loop setup for a sixteen converter system under different attack scenarios.

ACKNOWLEDGMENT

This material is based upon research supported in part by the U.S. Office of Naval Research under award number N00014-17-1-2239, Defense University Research Instrumentation Program award number N0014-16-1-3180, and by the National Science Foundation under Grant ECCS-1405173.

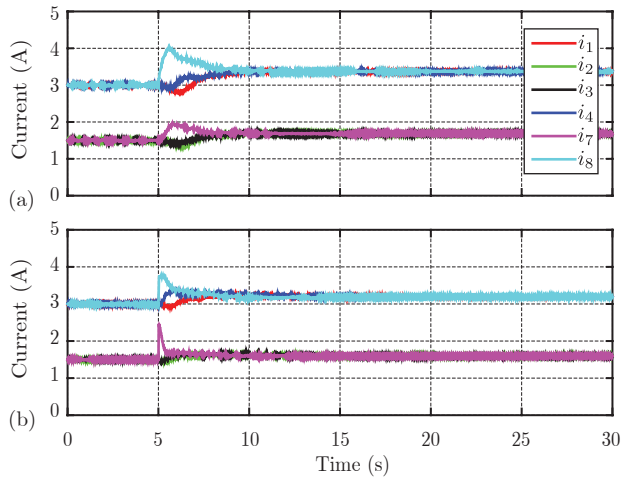

Fig. 9. Current of converters: a) Without trust when load is changed at converter 7 from 20 Ω to 30 Ω; b) With trust when load is changed at converter 7 from 20 Ω to 30 Ω

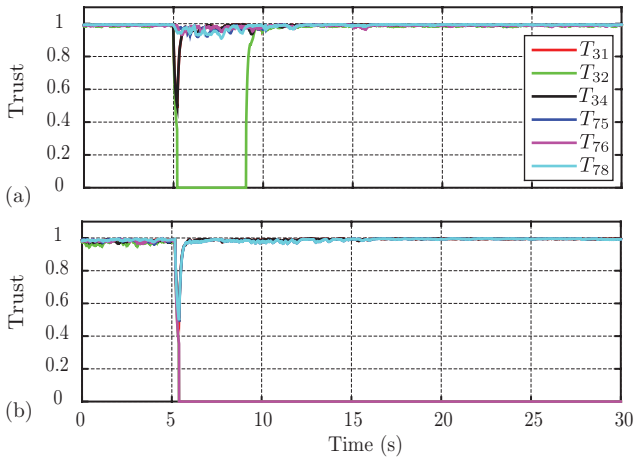

Fig. 10. Trust value: a) When the incoming communication link at converter 3 from converter 2 is attacked with a constant false data; b) When the incoming communication link at converter 3 from converter 2, incoming communication link at converter 7 from converter 6 and incoming communication link at converter 11 from converter 10 is attacked constant false data

REFERENCES

[1] Y. K. Chen, Y. C. Wu, C. C. Song, and Y. S. Chen, "Design and implementation of energy management system with fuzzy control for dc microgrid systems," *IEEE Trans. Power Electron.*, vol. 28, no. 4, pp. 1563–1570, Dec. 2013.

[2] D. Salomonsson, L. Soder, and A. Sannino, "An adaptive control system for a dc microgrid for data centers," *IEEE Trans. Ind. Appl.*, vol. 44, no. 6, pp. 1910–1917, Nov./Dec. 2008.

[3] V. Nasirian, S. Moayedi, A. Davoudi, and F. Lewis, "Distributed cooperative control of dc microgrids," *IEEE Trans. Power Electron.*, vol. 30, no. 4, pp. 2288–2303, Apr. 2015.

[4] S. Moayedi, V. Nasirian, F. Lewis, and A. Davoudi, "Team-oriented load sharing in parallel dc-dc converters," pp. 479–490, Jan./Feb. 2015.

[5] V. Nasirian, A. Davoudi, F. L. Lewis, and J. M. Guerrero, "Distributed adaptive droop control for dc distribution systems," *IEEE Trans. Energy Convers.*, vol. 29, no. 4, pp. 944–956, Dec. 2014.

[6] T. Zhou and B. Francois, "Energy management and power control of a hybrid active wind generator for distributed power generation and grid integration," *IEEE Trans. Ind. Electron.*, vol. 58, no. 1, pp. 95–104, Jan 2011.

[7] S. Amin, G. A. Schwartz, and S. S. Sastry, "Security of interdependent and identical networked control systems," *Automatica*, vol. 49, no. 1, pp. 186 – 192, 2013.

[8] F. Pasqualetti, A. Bicchi, and F. Bullo, "Consensus computation in unreliable networks: A system theoretic approach," *IEEE Trans. Autom. Control*, vol. 57, no. 1, pp. 90–104, Jan 2012.

[9] 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.

[10] H. J. LeBlanc, H. Zhang, X. Koutsoukos, and S. Sundaram, "Resilient asymptotic consensus in robust networks," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 4, pp. 766–781, April 2013.

[11] 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.

CHAPTER 6

CONTAINMENT-BASED DISTRIBUTED CONTROL OF DC MICROGRIDS

Authors: S. Abhinav and A. Davoudi.

Reprinted, with permission from all the co-authors.

Containment-based Distributed Control of DC Microgrids

Shankar Abhinav, Ali Davoudi
Electrical Engineering Department, University of Texas at Arlington, TX 76019 USA
Email: shankar.abhinav@mavs.uta.edu

Abstract

The secondary control objectives of current sharing and voltage regulation in DC microgrids are complimentary in nature. Optimal load sharing and voltage regulation is not feasible. In this paper, a containment based voltage controller that provides an upper and lower voltage bound is proposed for voltage regulation. A cooperative algorithm is used to compare the per-unit current of each converter with its neighbors to achieve proportional load sharing. A sparse communication network is used for exchange of information between the converter. There is a trade off between the two objectives of load sharing and voltage regulation. The voltage of the system is regulated within the voltage bound while maintaining best proportional load sharing. The efficacy of the proposed solution is evaluated using a Hardware in the Loop setup for different load conditions.

I. Introduction

DC microgrid is the solution for a reliable power distribution system in future, which will consist of renewable energy sources and storage devices [1], [2]. The hierarchical control structure in a microgrid consists of primary, secondary, and tertiary control levels [3], [4]. The primary controller sets the output voltage level and balance generations among sources. The secondary controller addresses the voltage drift caused

by the primary level while maintaining the load sharing across the sources. The tertiary addresses controller market related challenges such as economic dispatch.

In practice, centralized secondary control is used to maintain voltage regulation and decentralized droop control is used for load sharing [5], [6]. The droop control introduces a virtual resistance at each converter to enforce load sharing in inverse proportion to the virtual resistance. DC microgrids are increasing in complexity, with regard to the nature of computation and control. Purely centralized or decentralized control lacks the flexibility to address such complexities. Distributed cooperative control of DC microgrids as seen in Fig. 1 has garnered much attention in literature recently. Distributed control [7]–[9] increases reliability by not having a single point of failure, unlike in centralized control [10]. These distributed control methods [7]–[9] still use droop controller and achieve optimal load sharing at the expense of voltage regulation. In these methods though the average microgrid voltage is regulated, the individual converter voltage is not regulated.

Load sharing consists of dividing the total load on the microgrid among converters in proportion to their rated power. This is achieved by ensuring the per-unit current supplied by each converter is equal. In this paper, a current regulator at each converter uses cooperative control to correlate the converter per-unit current output with the neighbors per-unit currents to achieve proportional load sharing. A containment based voltage regulator is used to correlate the output voltage of the converter with its neighbor and the voltage bound to enforce voltage regulation within the bound. Containment based consensus control can be effectively used to bound the followers outputs within the convex hull of leaders output [11]–[13]. The containment and cooperative controller used in this paper require only a sparse communication network. The proposed controller does not need an additional droop controller to ensure proportional load sharing.

This paper is organized as follows. Preliminary of graph theory is given in Section

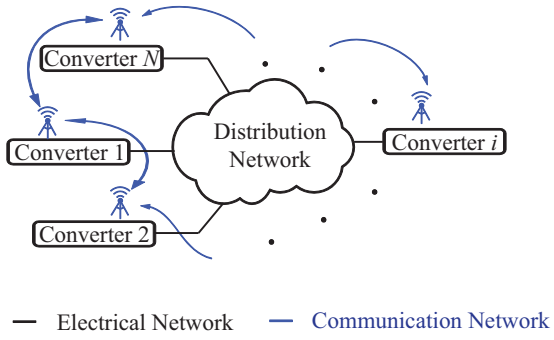

Fig. 1. A networked DC microgrid

II. Section III provides the proposed distributed control. Case studies, using a Hardware in the Loop setup with four converters, are detailed in Section IV. The conclusion is drawn in Section V.

II. Preliminary of Graph Theory

The communication network used by the converters can be represented by a graph Gr, as shown in Fig. 1. Each converter can be represented on the graph by a node, where $O = \{o_1, o_2, ..., o_n\}$ is the set of nodes mapped to each converter. $\mathbf{E} \subset O \times O$ is the set of edges representing communication links, and the associated adjacency matrix is $\mathbf{A} = [a_{ij}] \in \mathbb{R}^{N \times N}$. An edge starting at converter j and ending at converter i is denoted by (o_j, o_i), which indicates a communication link such that information flows from converter j to converter i. a_{ij} is the weight of edge (o_j, o_i), and $a_{ij} > 0$ if $(o_j, o_i) \in \mathbf{E}$, otherwise, $a_{ij} = 0$. Converters providing data to a particular converter are called its neighbors N_i. The diagonal in-degree matrix is defined as $\mathbf{D} = \mathrm{diag}\{N_i\}$. The graph Laplacian matrix, $\mathbf{L} = \mathbf{D} - \mathbf{A}$, whose eigenvalues describes communication network properties, such as the convergence rate. If there is a root node with a path from that node to every other node in the graph, then the graph has a spanning tree.

The set of leaders is denoted by $\mathcal{M} = \{n+1, n+2, ..., m\}$. A leader node k can be connected to a few converters (at least to one root node) by unidirectional edges. The

converters connected to a leader node and the corresponding edges are called pinned converters and pinning edges, respectively. g_i^k is the pinning gain from a leader k to the converter i. The pinning gain is zero for an unpinned converter. The pinning gain matrix for leader k is $\mathbf{G_k} = \mathrm{diag}\{g_i^k\}$.

III. Secondary Control

The secondary control in a DC microgrid has two objectives voltage regulation and proportional load sharing across the individual sources. The primary control for the converter are voltage controllers that are operated locally, and obtain their set points from the secondary controller. The secondary controller tunes the voltage set point such that voltage regulation and proportional load sharing objectives are met across the DC microgrid.

Figure 2 is a schematic of the DC microgrid comprising of different power generators connected to converters, physical interconnections, and the cyber layer comprising of communication and control. A sparse communication network is used. Each source along with its converter is represented as a node on the communication graph. Every converter transmits its per unit current and output voltage to its neighbors. The per unit current is current supplied by converter divided by its current rating, i.e., $i_i^{\mathrm{pu}} = i_i / I_i^{\mathrm{rated}}$, where i_i and I_i^{rated} are the output current and rated current of converter i respectively. Two converter are pinned (receive information from the leader) as shown in Fig. 2. One converter p receives the upper bound of the output voltage permissible ,v_u, and the other converter q receives the lower bound of the output voltage permissible v_l.

Figure 3 is block diagram representation proposed secondary controller for every converter. The voltage set point for the local controller $J(S)$ for converter i is calculated by using both load sharing and voltage regulation error terms, expressed as follows [7], [9], [14]:

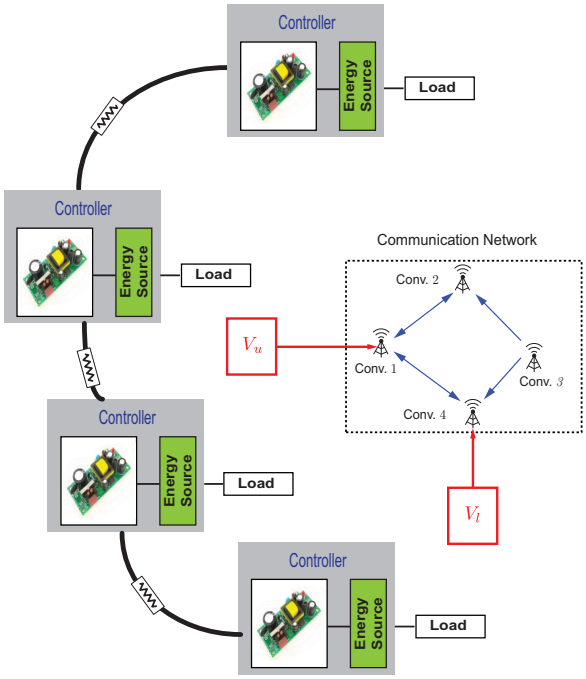

Fig. 2. DC Microgrid along with its communication network receiving voltage bound inputs

$$v_i^* = v^{\text{ref}} + \delta v_i^i + \delta v_i^v \tag{1}$$

where v^{ref} is the reference voltage. δv_i^v and δv_i^i are the voltage and load sharing correction terms for converter i, generated by the voltage and current regulator respectively.

The voltage regulators objective is to regulate the output voltage of each converter within the permissible bound ,(v_l, v_u). This can be realized by using a containment based cooperative control. The containment control objective is to design distributed controller for each converter such that the output voltage converges to the convex hull spanned leaders voltage set points, i.e. $v_l < v_i < v_l$.

The voltage regulator calculates the voltage mismatch term and passes it through a PI controller $G(S)$ to generate the voltage sharing correction term δv_i^v. This correction term is used to modify the local voltage set point of converter i to ensure voltage regulation within the permissible bound. The voltage mismatch is calculated by using

a containment protocol:

$$e_i^v(t) = \sum_{j \in N_i} ba_{ij} \left(v_j(t) - v_i(t)\right) + \sum_{k=n+1}^{m} g_i^k \left(v_k(t) - v_i(t)\right) \tag{2}$$

where v_i and v_j are the output voltage at converter i and converter j respectively.

Since the objective is to regulate the voltage between two voltage levels, it is sufficient to have pinned converters p and q. Converter p receives the upper bound and the voltage mismatch is calculated as follows:

$$e_p^v(t) = \sum_{j \in N_p} ba_{pj} \left(v_j(t) - v_p(t)\right) + g_p^{n+1} \left(v_u(t) - v_p(t)\right) \tag{3}$$

Converter q receives the lower bound and the voltage mismatch is calculated as follows:

$$e_q^v(t) = \sum_{j \in N_q} ba_{qj} \left(v_j(t) - v_q(t)\right) + g_q^{n+2} \left(v_l(t) - v_q(t)\right) \tag{4}$$

As long as there is a spanning tree and communication network Laplacian is balanced, the output voltage of each converter will be contained within the bound (v_l, v_u) [11], [12], [14].

To ensure proportional load sharing a load sharing, correction term is calculated by exchanging the per unit current of the individual converter. The current sharing regulator calculates the local load sharing mismatch e_i^i and passes it through a PI controller $H(S)$ to generate the current sharing correction term δv_i^i. The load sharing mismatch is calculated by using a dynamic consensus based control protocol similar to the one in [7], [9], [14] :

$$e_i^i = \sum_{j \in N_i} ca_{ij} \left(i_j^{\mathrm{pu}}(t) - i_i^{\mathrm{pu}}(t)\right) \tag{5}$$

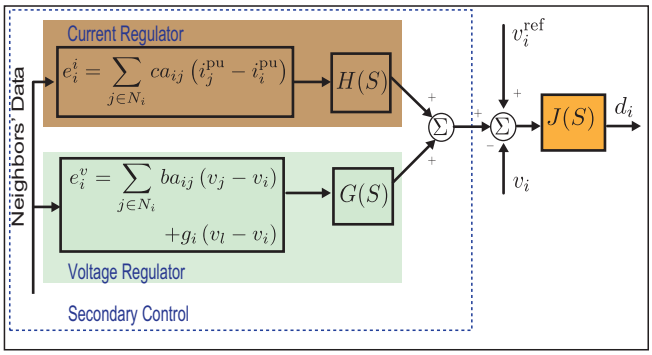

Fig. 3. Distributed secondary controller

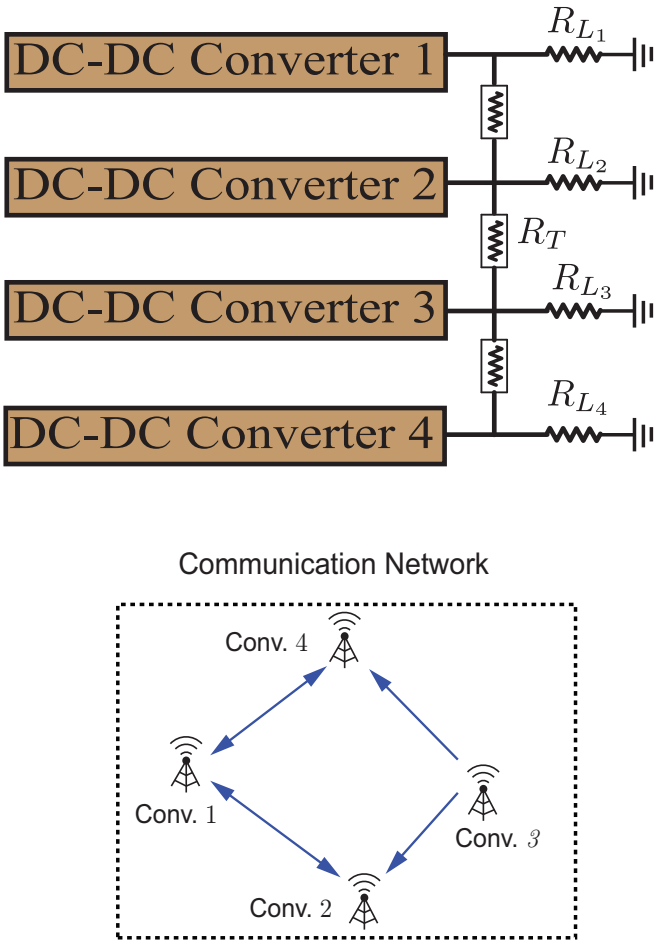

Fig. 4. a) Block diagram of a four converter system; (b) Topology of the communication network among converters

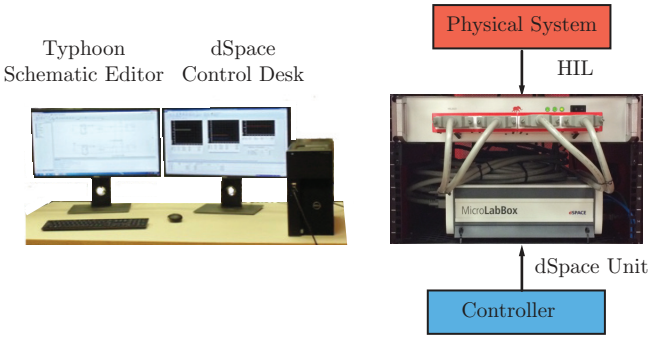

Fig. 5. Hardware in the Loop setup: Comprising of Typhoon 603 HIL, dSPACE ds1202 MicroLabBox, and a computer to monitor and program.

IV. Hardware in the Loop Verification

A 48 V islanded DC microgrid comprising of four converters is considered as shown in Fig. 4(a). A sparse undirected communication graph shown in Fig. 4(b) is used to facillitate exchange of information between each converter. Each converter communicates its voltage, per unit current to its neighbors using the communication graph . Each converter has a local load of $R = 20\ \Omega$, and the current rating of each converter is detailed in Table I. The design parameters of the converter and control are detailed in the Appendix. The physical microgrid shown in Fig. 4(a) is emulated by Typhoon HIL 603.

The control is modeled in SIMULINK then deployed on dSPACE ds1202 MicroLabBox. MicroLabBox is paired with a Typhoon HIL 603. MicroLabBox receives the physical measurements from the Typhoon HIL 603, and sends out the four switching signals for the four converters emulated in the Typhoon HIL 603. The MicroLabBox is connected to a monitoring computer using Ethernet connection via a LAN switch.

The control objective is to maintain proportional load (current) sharing, while ensuring voltage regulation between the bound $v_u = 49.5$ V and $v_l = 47.5$ V. Figures 6(a) and 7(a) study the performance of the distributed controller. For $t < 5$ s, the secondary controller is absent, it can be seen from Figs. 6(a) and 7(a) that voltage across each

TABLE I
CURRENT RATING

Converter	Current Rating (A)
1,4	10
2,3	3

converter is regulated to 48 V, but proportional load sharing is absent. At $t = 5$ s the secondary controller is engaged. It can been seen that after $t = 5$ s load has been proportionality shared between converters. The second and the third converter supply one-third of the load that the first and the fourth converter supply. Voltage of the converter is also regulated between the bound $v_u = 49.5$ V and $v_l = 47.5$ V.

The controller performance for load change is studied. The secondary controller has been engaged at $t < 0$ s. Figures 6(b) and 7(b) show the current and voltage of the converters when the load at the third converter is changed from $R_{L_3} = 20\ \Omega$ to $R_{L_3} = 30\ \Omega$ at $t = 5$ s. It can be seen that proportional load sharing is maintained even though the current requirement has changed. Voltage of the converter is also regulated between the bound $v_u = 49.5$ V and $v_l = 47.5$ V. Figures 6(c) and 7(c) show the current and voltage of the converters when the load at the second converter is changed from $R_{L_2} = 20\ \Omega$ to $R_{L_2} = 25\ \Omega$ at $t = 5$ s. It can be seen that proportional load sharing and voltage regulation is maintained.

Figures 6(d) and 7(d) show the current and voltage of the converters when the load at the third converter is changed from $R_{L_1} = 20\ \Omega$ to $R_{L_1} = 30\ \Omega$ at $t = 5$ s. It can be seen that proportional load sharing is not optimal, current supplied by the first and fourth converter are not equal. The converter voltages are still within the bound. In this particular case, due the presence of the voltage bound, there is a trade off between optimal load sharing and voltage regulation. Even though optimal current sharing is not achieved, converters are still sharing the load proportionally. Second and the third

converter approximately supply one-third the amount of the load, that the first and the fourth converter supply.

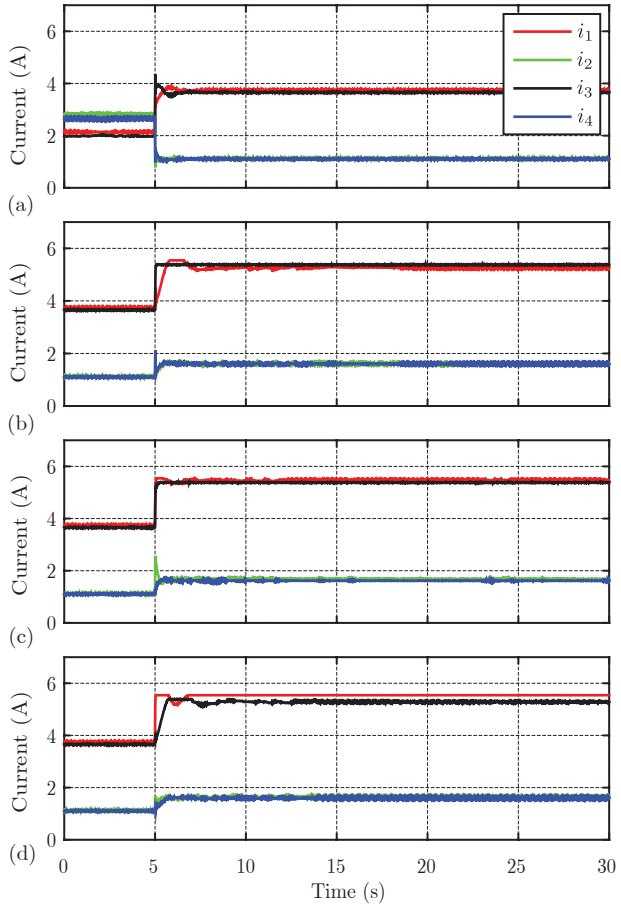

Fig. 6. Current of converters: (a) Secondary controller activated at at $t = 5$ s; (b) $R_{L_3} = 20\ \Omega$ changed to $R_{L_3} = 30\ \Omega$; (c) $R_{L_2} = 20\ \Omega$ changed to $R_{L_3} = 25\ \Omega$; (d) $R_{L_1} = 20\ \Omega$ changed to $R_{L_1} = 30\ \Omega$

V. Conclusion

A distributed containment-based voltage controller and cooperative current sharing control is proposed for DC microgrid. The proposed method is evaluated using a Hardware in the Loop setup under different loading conditions. The proposed controller allows proportional load sharing, while ensuring the output voltage of each converter is bounded.

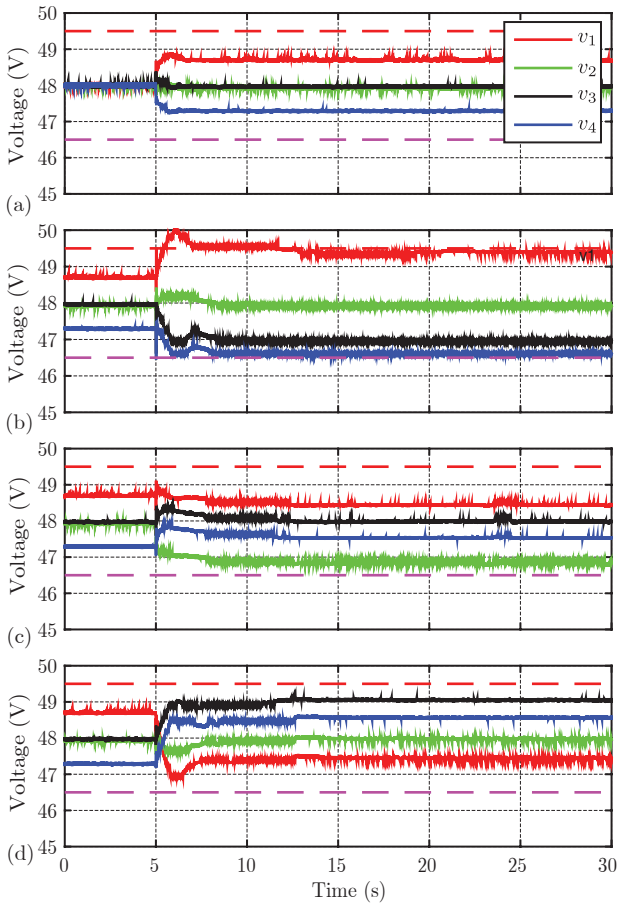

Fig. 7. Voltage of converters: (a) Secondary controller activated at at $t = 5$ s; (b) $R_{L_3} = 20\ \Omega$ changed to $R_{L_3} = 30\ \Omega$; (c) $R_{L_2} = 20\ \Omega$ changed to $R_{L_3} = 25\ \Omega$; (d) $R_{L_1} = 20\ \Omega$ changed to $R_{L_1} = 30\ \Omega$

APPENDIX

Each buck converter has inductance $L = 2640\ \mu$H, capacitance $C = 2.2$ mF and switching frequency $f_s = 60$kHz.

Adjacency matrix is

$$\mathbf{A} = \begin{bmatrix} 0 & 90 & 0 & 110 \\ 90 & 0 & 100 & 0 \\ 0 & 100 & 0 & 120 \\ 110 & 0 & 120 & 0 \end{bmatrix} \tag{6}$$

Control parameters are $b = 0.001$ and $c = 0.1$.

ACKNOWLEDGMENT

This material is based upon research supported in part by the U.S. Office of Naval Research under award number N00014-17-1-2239, Defense University Research Instrumentation Program award number N0014-16-1-3180, and by the National Science Foundation under Grant ECCS-1405173.

REFERENCES

[1] Y. K. Chen, Y. C. Wu, C. C. Song, and Y. S. Chen, "Design and implementation of energy management system with fuzzy control for dc microgrid systems," *IEEE Trans. Power Electron.*, vol. 28, no. 4, pp. 1563–1570, Dec. 2013.

[2] D. Salomonsson, L. Soder, and A. Sannino, "An adaptive control system for a dc microgrid for data centers," *IEEE Trans. Ind. Appl.*, vol. 44, no. 6, pp. 1910–1917, Nov./Dec. 2008.

[3] J. Guerrero, J. Vasquez, J. Matas, L. de Vicua, and M. Castilla, "Hierarchical control of droop-controlled AC and DC microgrids-a general approach toward standardization," *IEEE Trans. Ind. Electron.*, vol. 58, no. 1, pp. 158–172, Jan 2011.

[4] L. Che, M. Shahidehpour, A. Alabdulwahab, and Y. Al-Turki, "Hierarchical coordination of a community microgrid with AC and DC microgrids," *IEEE Trans. Smart Grid*, vol. 6, no. 6, pp. 3042–3051, Nov 2015.

[5] P. Karlsson and J. Svensson, "Dc bus voltage control for a distributed power system," *IEEE Transactions on Power Electronics*, vol. 18, no. 6, pp. 1405–1412, Nov 2003.

[6] J. A. P. Lopes, C. L. Moreira, and A. G. Madureira, "Defining control strategies for microgrids islanded operation," *IEEE Transactions on Power Systems*, vol. 21, no. 2, pp. 916–924, May 2006.

[7] V. Nasirian, S. Moayedi, A. Davoudi, and F. Lewis, "Distributed cooperative control of dc microgrids," *IEEE Trans. Power Electron.*, vol. 30, no. 4, pp. 2288–2303, Apr. 2015.

[8] S. Moayedi, V. Nasirian, F. Lewis, and A. Davoudi, "Team-oriented load sharing in parallel dc-dc converters," pp. 479–490, Jan./Feb. 2015.

[9] V. Nasirian, A. Davoudi, F. L. Lewis, and J. M. Guerrero, "Distributed adaptive droop control for dc distribution systems," *IEEE Trans. Energy Convers.*, vol. 29, no. 4, pp. 944–956, Dec. 2014.

[10] T. Zhou and B. Francois, "Energy management and power control of a hybrid active wind generator for distributed power generation and grid integration," *IEEE Trans. Ind. Electron.*, vol. 58, no. 1, pp. 95–104, Jan 2011.

[11] 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," *International Journal of Robust and Nonlinear Control*, vol. 23, no. 5, pp. 534–547, 2013.

[12] Y. Cao, D. Stuart, W. Ren, and Z. Meng, "Distributed containment control for multiple autonomous vehicles with double-integrator dynamics: Algorithms and experiments," *IEEE Transactions on Control Systems Technology*, vol. 19, no. 4, pp. 929–938, July 2011.

[13] ——, "Distributed containment control for multiple autonomous vehicles with double-integrator dynamics: Algorithms and experiments," *IEEE Transactions on Control Systems Technology*, vol. 19, no. 4, pp. 929–938, July 2011.

[14] V. Nasirian, A. Davoudi, and F. L. Lewis, "Distributed adaptive droop control for dc microgrids," in *IEEE Applied Power Electronics Conference and Exposition (APEC)*, March 2014, pp. 1147–1152.

CHAPTER 7

CONCLUSION

A robust control structure using advanced distributed control algorithms for AC and DC microgrids have been evaluated. A distributed controller with ADMM based estimator was proposed for synchronization of frequency and voltage in AC microgrids using communication network, while considering noise and link failures. Synchronization in AC microgrids was cast as an optimization problem and was solved using Alternating Direction Method of Multipliers, to provide a robust distributed controller. An upper error bound was analytically derived for synchronization under noisy communication channels and verified by simulation results.

An attack resilient controller was also proposed for AC microgrids, which utilizes observer-based consensus to localize attacks and trust-confidence based techniques to detect and mitigate attacks on communication links and controller (hijacking). Trust-based evaluation of neighbors was used to detect and mitigate attacks on communication links and controller (hijacking) in cooperative current sharing of DC microgrids. A containment based voltage regulator and consensus based load sharing regulator were also evaluated, to achieve voltage regulation within a bound and proportional load sharing in a DC microgrid.

Future work may focus on developing learning based controller for adapting to changes in an efficient and reliable manner.

BIOGRAPHICAL STATEMENT

Shankar Abhinav received the B.E. degree in Electrical and Electronics Engineering from Visvesvaraya Technological University, Karnataka, India, in 2011. He is currently working toward the Ph.D. degree at the University of Texas at Arlington, USA. His research interests include modeling and control of power electronics in a microgrid setting. He was awarded the Office of Graduate Studies Dissertation Fellowship for Summer 2017 by UT Arlington.