DISTRIBUTED RESILIENT CONTROL OF MULTI-AGENT SYSTEMS WITH APPLICATIONS TO MICROGRIDS

by

SHAN ZUO

DISSERTATION

Submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy at
The University of Texas at Arlington
August, 2020

Arlington, Texas

Supervising Committee:

Ali Davoudi, Supervising Professor

Frank L. Lewis, Supervising Professor

Yan Wan

Jonathan Bredow

Rasool Kenarangui

ACKNOWLEDGEMENTS

I would like to express my sincere gratitude to my supervising professors, Dr. Ali Davoudi and Dr. Frank L. Lewis, for constantly motivating me, sparing their valuable time, and giving me great guidance during my doctoral research. Dr. Ali Davoudi has always been so supportive and helpful whenever I run into difficulties. Thanks to his high standards and strict requirements, I am able to break through barriers and make progress in my research. I would thank my dissertation committee members, Dr. Yan Wan, Dr. Jonathan Bredow, and Dr. Rasool Kenarangui for showing interest in this work, sparing time, and advising me for completion of this dissertation. I would also like to thank Dr. Omar A. Beg, Tuncay Altun, Dr. Deepak Pullaguram, and Ajay Yadav for their invaluable comments and discussions to improve this work. I thank all my research group members for their help, support, and memorable time during the course of my doctoral studies.

The material presented in this dissertation is based upon work supported, in part, by the University of Texas at Arlington, National Science Foundation (NSF) under grant number ECCS-1405173, and U.S. Office of Naval Research (ONR) under grant number N00014-17-1-2239. The materials presented in this dissertation are approved for public release under DCN # 43-6704-20. The U.S. government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon. Any opinions, findings, and conclusions or recommendations expressed in this dissertation are those of the author and do not necessarily reflect the views of NSF or ONR.

July 30, 2020

To my family

TABLE OF CONTENTS

ABSTRACT

DISTRIBUTED RESILIENT CONTROL OF MULTI-AGENT SYSTEMS WITH APPLICATIONS TO MICROGRIDS

SHAN ZUO, Ph.D.

The University of Texas at Arlington, 2020

Supervising Professors: Ali Davoudi and Frank L. Lewis

Distributed cooperative control of multi-agent systems (MAS) has been an active research area over the last few decades. Distributed cooperative controller is locally designed using the neighborhood relative information. Such a distributed control manner, however, is vulnerable to malicious attacks, due to the absence of a centralized control architecture to effectively monitor and verify the local information flow. Those attacks could undermine cooperative performance and even cause system instability. In this work, a new concept of multi-group system is first proposed, consisting of cooperative leaders and followers, as well as adversaries. A resilient control framework is developed for general linear heterogeneous MAS to counter sensor faults and adversaries' attacks by preserving the uniformly ultimately bounded (UUB) convergence for output containment performance. Then, attack-resilient control methods are developed for the secondary control level of AC and DC microgrids. In particular, fully distributed control protocols using observer-based techniques are proposed for the secondary frequency regulation and voltage containment of AC microgrids to address general unknown unbounded attacks. A fully distributed attack-resilient control framework using adaptive techniques is established for DC microgrids to

mitigate the adverse effect of unbounded attacks on local control input channels. A two-layer hierarchy for networked MAS with two opposing teams is developed, including a control protagonist team with cooperative multi-inverter microgrids and an attack antagonist team with interacting attackers. A distributed control architecture, that is resilient to correlated sensor attacks and unbounded attacks on actuators and communication channels, is proposed. Finally, a distributed control framework using adaptive techniques is proposed for AC microgrids. Compared to the observer-based approach, this method does not need extra cyber layers for information exchange between observers, reducing computational complexity and system vulnerability against attacks. Moreover, the ultimate bound can be reduced by adjusting the tuning parameters. Extensive numerical simulations or hardware-in-the-loop studies validate the effectiveness of the proposed methods.

CHAPTER 1

INTRODUCTION

1.1 Motivation

Distributed cooperative control of MAS has been an active research area over the past decades [1–5], and has been applied to various engineering problems [6–10]. Generally, a distributed cooperative controller is locally designed for each agent, and requires only the local relative information with respect to its neighbors. Such a distributed control framework can achieve better robustness, efficiency, and scalability, compared to the standard centralized control. However, due to the absence of a centralized architecture to effectively monitor and verify the information flow of each agent, the networked MAS is vulnerable to faults and attacks, which can easily prevent network-level control goals and even lead to an overall system instability [11, 12]. Secure and resilient controller design is essential in providing the overall system stability and achieving the desired system performance under faults and even attacks.

Two general approaches have been presented to make the distributed MAS resilient against attacks. In the first approach, compromised agents are first detected and identified, and then overcome or simply isolated [13–15]. Similar techniques are also applied in power grids to address malicious attacks [16–22]. On one hand, attack-correction methods usually have strict restrictions on the number of misbehaving agents. For example, it is shown in [23, 24] that it is impractical to restore the system state if more than half of the sensors have been affected. On the other hand, simply isolating the corrupted agents may potentially compromise the connectivity and performance of the sparse communication network. Furthermore, sufficient and necessary conditions for undetectable or unidentifiable attacks

are well discussed in the literature [25–27]. Since one could not list and remove every potential threat, the concept of attack-resilience is proposed. Hence, the second solution category develops distributed attack-resilient control protocols to enhance the resilience of the MAS against potential noises/faults, without the need to detect, identify and correct/remove misbehaving agents [28–35]. The resilient control protocols are recently proposed in [36–41] and [6] for the secondary control of AC and DC microgrids, respectively. These unintentional noises/faults have been assumed to be bounded signals. Direct adaptation to adversarial attacks is not practical as such attacks could be intentionally designed to maximize their damage and, hence, cannot be assumed bounded. Note that unbounded attack injections not only undermine the network-level cooperative performance, but also jeopardize the system stability and cause catastrophic damage. It is, therefore, important to design control strategies resilient to unknown unbounded attacks to assure reliability and security of MAS and, particularly, microgrids.

1.2 Outline

In this dissertation, a new concept of cooperative and adversarial multi-group system is proposed, which consists of cooperative leaders and followers, as well as adversaries. A distributed resilient control architecture is proposed for heterogeneous MAS to guarantee uniform ultimate boundedness of the closed-loop dynamical system against sensor faults and attacks from adversaries. Attack-resilient control approaches are developed for AC and DC microgrids against unknown unbounded attacks. Observer-based and adaptive control based techniques are used to construct the resilient control framework to mitigate the adverse effect of unbounded attacks and preserve the UUB convergence for regulation terms.

The dissertation is organized as follows:

1.2.1 Chapter 2 - Resilient Output Containment of Heterogeneous Cooperative and Adversarial Multi-Group Systems

1.2.1.1 Description

This chapter presents a journal paper published in the IEEE Transactions on Automatic Control. It introduces a new concept of cooperative and adversarial multi-group system. A novel control framework resilient to both sensor faults and malicious attacks from adversaries is proposed to maintain bounded stability of the overall system and achieve the resilient output containment control objective for heterogeneous MAS. Explicit local sufficient conditions and design procedures are obtained. The effectiveness of the proposed control protocols is verified by the simulated case studies.

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. Lewis supervised the work and was involved from conceptualization to execution, and Dr. Davoudi had a supportive role.

1.2.2 Chapter 3 - Resilient Networked AC Microgrids under Unbounded Cyber Attacks

1.2.2.1 Description

This chapter presents a journal paper accepted for publication in IEEE Transactions on Smart Grid. It considers a cooperative and adversarial AC microgrid system. A fully distributed resilient control framework using observer-based techniques is offered for the secondary frequency regulation and voltage containment to ensure system stability and preserve bounded synchronization. A modified IEEE 34-bus test feeder benchmark system

is emulated in a controller/ hardware-in-the-loop (HIL) environment, where the control objectives are met under different attack scenarios.

1.2.2.2 Individual Contribution

The author was the principal architect of the endeavor. The author identified the problem, theorized the solution, and executed the solution. Dr. Beg helped the author to build the experimental setup and run the experimental analysis. Dr. Davoudi supervised the work and was involved from conceptualization to execution, and Dr. Lewis had a supportive role.

1.2.3 Chapter 4 - Distributed Resilient Secondary Control of DC Microgrids against Unbounded Attacks

1.2.3.1 Description

This chapter presents a journal paper accepted for publication in the IEEE Transactions on Smart Grid. It develops a fully distributed attack-resilient secondary control framework for DC microgrids, in the presence of unknown unbounded attacks on control input channels. Rigorous proofs based on Lyapunov techniques show that the proposed method guarantees the UUB and asymptotic-stability convergences for both global voltage regulation and proportional load sharing objectives under unbounded and bounded attacks, respectively. Experimental results are illustrated in a HIL environment and validate the effectiveness of the proposed approach.

1.2.3.2 Individual Contribution

The author was the principal architect of the endeavor. The author identified the problem, theorized the solution, and executed the solution. Mr. Altun helped with the

experimental setup and running the experimental analysis. Dr. Davoudi supervised the work and was involved from conceptualization to execution, and Dr. Lewis had a supportive role.

1.2.4 Chapter 5 - Resilient AC Microgrids against Correlated Attacks

1.2.4.1 Description

This chapter studies the ramifications of allowing the antagonistic inputs to be unbounded and correlated. A two-layer hierarchy is proposed for a networked MAS with two opposing teams: a control protagonist team with cooperative multi-inverter microgrids and an attack antagonist team with interacting attackers. A fully distributed control framework, that is resilient to external correlated sensor attacks from interacting antagonists, as well as unknown unbounded attacks on actuator commands and communication channels, is developed. The proposed results are validated on a modified IEEE 34-bus test feeder system, which is emulated in a controller/HIL environment.

1.2.4.2 Individual Contribution

The author was the principal architect of the endeavor. The author identified the problem, theorized the solution, and executed the solution. Dr. Pullaguram helped with building the experimental setup and running the experimental analysis. Dr. Davoudi supervised the work and was involved from conceptualization to execution, and Dr. Lewis had a supportive role.

1.2.5 Chapter 6 - Adaptive Resilient Control of AC Microgrids under Unbounded Actuator Attacks

1.2.5.1 Description

This chapter studies unknown unbounded attacks on input signals of both frequency and voltage control loops. A novel fully distributed control framework, using adaptive control techniques, is proposed. Stability analysis using Lyapunov techniques show that the proposed approach is resilient to unknown unbounded actuator attacks for both frequency and voltage control loops by preserving the UUB consensus for frequency regulation and voltage containment, respectively. The proposed result is validated for a modified IEEE 34-bus test feeder benchmark system with four inverters. Compared to the attack-resilient controller using observer-based techniques, the distributed controller developed in this chapter has two merits: (i) Local observers with additional communication information flow are constructed in the observer-based controller to estimate the actual state measurement. This, however, introduces additional computational complexity. Moreover, the additional communication channels, for exchanging observer states, increase the system vulnerability to malicious attacks; (ii) The ultimate bound, using the control protocols proposed in this chapter, can be set to be an arbitrarily small value by increasing the tuning parameters. In other words, the frequency and voltage terms can be tuned to converge to an arbitrarily small neighborhood around reference values.

1.2.5.2 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, and Dr. Lewis has a supportive role.

1.3 References

[1] R. Olfati-Saber and R. M. Murray, "Consensus problems in networks of agents with switching topology and time-delays," *IEEE Control syst. mag.*, vol. 49, no. 9, pp. 1520–1533, Sep. 2004.

[2] W. Ren, R. W. Beard, and E. M. Atkins, "Information consensus in multivehicle cooperative control," *IEEE Control syst. mag.*, vol. 2, no. 27, pp. 71–82, Apr. 2007.

[3] F. L. Lewis, H. Zhang, K. Hengster-Movric, and A. Das, *Cooperative Control of Multi-Agent Systems: Optimal and Adaptive Design Approaches*. London, UK: Springer-Verlag, 2014.

[4] J. Huang, *Nonlinear output regulation: theory and applications*. Philadelphia, PA, USA: SIAM, 2004.

[5] S. Zuo, Y. Song, H. Modares, F. L. Lewis, and A. Davoudi, "A unified approach to output synchronization of heterogeneous multi-agent systems via L_2-gain design," *Control Theory Technol.*, vol. 15, no. 4, pp. 340–353, Nov. 2017.

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

[7] S. Zuo, A. Davoudi, Y. Song, and F. L. Lewis, "Distributed finite-time voltage and frequency restoration in islanded ac microgrids," *IEEE Trans. Ind. Electron.*, vol. 63, no. 10, pp. 5988–5997, Jun. 2016.

[8] W. Ren and N. Sorensen, "Distributed coordination architecture for multi-robot formation control," *Robot. Auton. Syst.*, vol. 56, no. 4, pp. 324–333, Apr. 2008.

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

[10] P. Wang, X. Lu, X. Yang, W. Wang, and D. Xu, "An improved distributed secondary control method for dc microgrids with enhanced dynamic current sharing performance," *IEEE Trans. Power Electron.*, vol. 31, no. 9, pp. 6658–6673, Sep. 2016.

[11] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inf. Syst. Secur.*, vol. 14, no. 1, May 2011.

[12] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 645–658, Dec. 2011.

[13] 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.

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

[15] S. Sundaram and C. N. Hadjicostis, "Distributed function calculation via linear iterative strategies in the presence of malicious agents," *IEEE Trans. Autom. Control*, vol. 56, no. 7, pp. 1495–1508, Jul. 2011.

[16] L. Lu, H. J. Liu, H. Zhu, and C. Chu, "Intrusion detection in distributed frequency control of isolated microgrids," *IEEE Trans. Smart Grid*, vol. 10, no. 6, pp. 6502–6515, Nov. 2019.

[17] A. Mustafa, B. Poudel, A. Bidram, and H. Modares, "Detection and mitigation of data manipulation attacks in ac microgrids," *IEEE Trans. Smart Grid*, vol. 11, no. 3, pp. 2588–2603, May 2020.

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

[19] 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.

[20] O. A. Beg, T. T. Johnson, and A. Davoudi, "Detection of false-data injection attacks in cyber-physical dc microgrids," *IEEE Trans. Ind. Informat.*, vol. 13, no. 5, pp. 2693–2703, Oct. 2017.

[21] O. A. Beg, L. V. Nguyen, T. T. Johnson, and A. Davoudi, "Signal temporal logic-based attack detection in dc microgrids," *IEEE Trans. Smart Grid*, vol. 10, no. 4, pp. 3585–3595, Jul. 2019.

[22] S. Sahoo, S. Mishra, J. C. Peng, and T. Dragičević, "A stealth cyber-attack detection strategy for dc microgrids," *IEEE Trans. Power Electron.*, vol. 34, no. 8, pp. 8162–8174, Aug. 2019.

[23] 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, Jun. 2014.

[24] Z. Tang, M. Kuijper, M. S. Chong, I. Mareels, and C. Leckie, "Linear system security—detection and correction of adversarial sensor attacks in the noise-free case," *Automatica*, vol. 101, pp. 53–59, Mar. 2019.

[25] G. Hug and J. A. Giampapa, "Vulnerability assessment of ac state estimation with respect to false data injection cyber-attacks," *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1362–1370, Sep. 2012.

[26] J. Liang, L. Sankar, and O. Kosut, "Vulnerability analysis and consequences of false data injection attack on power system state estimation," *IEEE Trans. Power Syst.*, vol. 31, no. 5, pp. 3864–3872, Sep. 2016.

[27] K. Pan, A. Teixeira, M. Cvetkovic, and P. Palensky, "Cyber risk analysis of combined data attacks against power system state estimation," *IEEE Trans. Smart Grid*, vol. 10, no. 3, pp. 3044–3056, May 2019.

[28] T. Alpcan and T. Basar, "A game theoretic approach to decision and analysis in network intrusion detection," in *Proc. 42nd IEEE Int. Conf. Decision Control*, Maui, HI, 2003, pp. 2595–2600.

[29] S. M. Dibaji and H. Ishii, "Resilient consensus of double-integrator multi-agent systems," in *2014 American Control Conf.*, Portland, OR, 2014, pp. 5139–5144.

[30] H. J. LeBlanc, H. Zhang, S. Sundaram, and X. Koutsoukos, "Resilient continuous-time consensus in fractional robust networks," in *2013 American Control Conf.*, Washington, DC, 2013, pp. 1237–1242.

[31] E. Arabi, T. Yucelen, and W. M. Haddad, "Mitigating the effects of sensor uncertainties in networked multiagent systems," in *2016 American Control Conf.*, Boston, MA, 2016, pp. 5545–5550.

[32] G. D. L. Torre, T. Yucelen, and J. D. Peterson, "Resilient networked multiagent systems: A distributed adaptive control approachy," in *Proc. 53rd IEEE Int. Conf. Decision Control*, Los Angeles, CA, 2014, pp. 5367–5372.

[33] C.-H. Xie and G.-H. Yang, "Decentralized adaptive fault-tolerant control for large-scale systems with external disturbances and actuator faults," *Automatica*, vol. 85, pp. 83–90, Nov. 2017.

[34] X. Jin, W. M. Haddad, and T. Yucelen, "An adaptive control architecture for mitigating sensor and actuator attacks in cyber-physical systems," *IEEE Trans. Autom. Control*, vol. 62, no. 11, pp. 6058–6064, Nov. 2017.

[35] H. Modares, R. Moghadam, F. L. Lewis, and A. Davoudi, "Static output-feedback synchronisation of multi-agent systems: a secure and unified approach," *IET Control Theory Appl.*, vol. 12, no. 8, pp. 1095–1106, May 2018.

[36] S. Abhinav, I. D. Schizas, F. L. Lewis, and A. Davoudi, "Distributed noise-resilient networked synchrony of active distributed systems," *IEEE Trans. Smart Grid*, vol. 9, no. 2, pp. 836–846, Mar. 2018.

[37] N. M. Dehkordi, H. R. Baghaee, N. Sadati, and J. M. Guerrero, "Distributed noise-resilient secondary voltage and frequency control for islanded microgrids," *IEEE Trans. Smart Grid*, vol. 10, no. 4, pp. 3780–3790, May 2019.

[38] A. Afshari, M. Karrari, H. R. Baghaee, G. B. Gharehpetian, and S. Karrari, "Cooperative fault-tolerant control of microgrids under switching communication topology," *IEEE Trans. Smart Grid*, vol. 11, no. 3, pp. 1866–1879, May 2020.

[39] N. M. Dehkordi, H. R. Baghaee, N. Sadati, and J. M. Guerrero, "Distributed noise-resilient secondary voltage and frequency control for islanded microgrids," *IEEE Trans. Smart Grid*, vol. 10, no. 4, pp. 3780–3790, Jul. 2019.

[40] M. A. Shahab, B. Mozafari, S. Soleymani, N. M. Dehkordi, H. M. Shourkaei, and J. M. Guerrero, "Distributed consensus-based fault tolerant control of islanded microgrids," *IEEE Trans. Smart Grid*, vol. 11, no. 1, pp. 37–47, Jan. 2020.

[41] A. Bidram, B. Poudel, L. Damodaran, R. Fierro, and J. M. Guerrero, "Resilient and cybersecure distributed control of inverter-based islanded microgrids," *IEEE Trans. Ind. Informat.*, vol. 16, no. 6, pp. 3881–3894, Jun. 2020.

CHAPTER 2

RESILIENT OUTPUT CONTAINMENT OF HETEROGENEOUS COOPERATIVE AND ADVERSARIAL MULTI-GROUP SYSTEMS[1]

Authors: Shan Zuo, Frank L. Lewis, and Ali Davoudi.

Reprinted, with permission from all the co-authors.

Journal: IEEE Transactions on Automatic Control,

July 2020, vol 65, no 7, pages 3104-3111

Resilient Output Containment of Heterogeneous Cooperative and Adversarial Multi-Group Systems

Shan Zuo, Frank L. Lewis, *Fellow, IEEE*,

Ali Davoudi, *Senior Member, IEEE*

Abstract

This note introduces a new concept of cooperative and adversarial multi-group system, which consists of cooperative leaders and followers, as well as adversaries. For example, cooperation of multiple vehicles operate in complex dynamic networked environments with hidden malicious attackers. The lack of global situational awareness in distributed settings makes autonomous vehicles prone to cyber-attacks and infiltration. Each agent is unaware of the motives of its neighbors, and may receive information/data from both the teammates and the adversaries. Secure and resilient control protocols are essential for the networked multi-group systems to prevent the adversaries' attacks from propagating across the network, which may influence the system performance and even overall stability. To counter sensor faults and attacks from the adversaries, a distributed resilient control architecture is proposed, which guarantees uniform ultimate boundedness of the closed-loop dynamical system. Numerical simulations illustrate the effectiveness of the proposed results.

This work was supported in part by the NSF grant ECCS-1405173 and in part by the ONR grant N00014-17-1-2239.

Shan Zuo, Frank L. Lewis and Ali Davoudi are with the Electrical Engineering Department, The University of Texas, Arlington, TX 76019, USA (e-mail: shan.zuo@uta.edu; lewis@uta.edu; davoudi@uta.edu).

Index Terms

Adversaries, attacks, heterogeneous multi-group system, resilience, sensor fault.

I. Introduction

Distributed cooperative control of multi-agent systems (MAS) has been an active research area over the past decades [1]–[4], and has been applied to various engineering problems [5]–[9]. Generally, a distributed cooperative controller is locally designed for each agent, and requires only the local relative information with respect to its neighbors. Such a distributed control framework can achieve better robustness, efficiency, and scalability, compared to the standard centralized control. However, due to the absence of a centralized architecture to effectively monitor and verify the information flow of each agent, the networked MAS are vulnerable to faults and cyber-physical data attacks, which can easily prevent system-level control goals and even lead to the overall system instability [10], [11]. Secure and resilient controller design is essential in providing the overall system stability and achieving the desired system performance under faults and cyber-physical attacks.

Two general approaches have been presented to make the distributed MAS resilient against attacks [12]–[24]. In the first approach, compromised agents are first detected and identified, and then removed [12]–[14]. In the second approach, a resilient control framework maintains an acceptable level of performance regardless of the malicious attacks [15]–[19]. However, these methods require full knowledge of the communication graph topology, and/or the number of agents under malicious attacks, which may not be available in a fully distributed manner. Such limitations were removed in [20]–[22] for homogeneous MAS against either sensor or actuator faults. [23] presented an adaptive control architecture to mitigate both sensor and actuator attacks for homogeneous systems. [24] designed secure static output-feedback control protocols for both

homogeneous and heterogeneous MAS under bounded sensor and actuator faults. Local observers with additional observer communication exchange are required to estimate the leader's state, and an ideal state observer is used.

Motivation of this note: This note introduces a heterogeneous networked multi-group system, consisting of leaders, followers, and adversaries. For example, distributed MAS operate in fast-evolving and uncertain complex dynamic networked environments, where unknown hidden enemies can infiltrate information networks and subvert opinions [25]. The lack of global situational awareness in distributed settings makes autonomous teams prone to cyber-attacks and infiltration. An attacker can identify the most vulnerable agents to leverage a single compromise into a network-wide catastrophe. Decision-making agents are unaware of the motives and true intent of both their cooperative colleagues and hidden adversaries seeking to influence public opinions. Individual agents require effective automated decision and control protocols that increase resilience to achieve stability and assure system performance in the presence of sensor faults and malicious attacks from the adversaries.

This note investigates the resilient output containment problem for general linear heterogeneous multi-group systems in the presence of unknown sensor faults and malicious attacks from the adversaries. Our previous paper [9] investigated the output containment problem of heterogeneous MAS when the leaders' dynamics are only known to the neighboring followers. An adaptive observer is locally designed to estimate the leaders' dynamics. Noting that, however, [9] does not consider any sensor faults or adversaries' attacks. The salient contributions of this note are as follows:

• The new concept of cooperative and adversarial multi-group systems is introduced. This heterogeneous networked system consists of cooperative leaders and followers, as well as malicious adversaries. Each agent can have different system dynamics. Each follower is unaware of the motives and true intent of both its teammates and hidden

adversaries, and therefore, is vulnerable to sensor faults and malicious attacks.

• A resilient output containment problem is defined in the presence of sensor faults and adversaries' attacks to guarantee the uniformly ultimately bounded (UUB) convergence of each follower's output to the dynamic convex hull spanned by the outputs of multiple leaders.

• A novel distributed output-feedback control framework guarantees the stability of the overall system and the resilient output containment objective. Local sufficient conditions and design procedures are explicitly presented.

II. Preliminaries and Problem Formulation

A. Preliminaries on Graph Theory and Notations

A heterogeneous multi-group system is considered on a communication digraph $\mathscr{G}$, consisting of leaders, followers, and adversaries. The followers have incoming edges and receive direct information from the neighbors, including the cooperative and adversarial agents. The sets of the leaders, the followers, and the adversaries are denoted by $\mathscr{L}$, $\mathscr{F}$, and $\mathscr{A}$, respectively. The interaction among the followers can be represented by the subgraph $\mathscr{G}_f = (\mathcal{V}, \mathcal{E}, \mathcal{A})$ with a nonempty finite set of nodes $\mathcal{V}$, a set of edges $\mathcal{E} \subset \mathcal{V} \times \mathcal{V}$, and the associated adjacency matrix $\mathcal{A} = [a_{ij}]$. a_{ij} is the weight of edge (v_j, v_i), and $a_{ij} > 0$ if $(v_j, v_i) \in \mathcal{E}$, otherwise $a_{ij} = 0$. Node j is called a neighbor of node i if $(v_j, v_i) \in \mathcal{E}$. Define the in-degree matrix as $\mathcal{D} = \mathrm{diag}(d_i) \in \mathbb{R}^{N\times N}$ with $d_i = \sum_{j\in\mathscr{F}} a_{ij}$ and the Laplacian matrix as $\mathcal{L} = \mathcal{D} - \mathcal{A}$. A sequence of successive edges in the form $\{(v_i, v_k), (v_k, v_l), \ldots, (v_m, v_j)\}$ is a directed path from node i to node j. g_{ik} (respectively, h_{il}) is the pinning gain from the kth leader (respectively, lth adversary) to the ith follower. $g_{ik} > 0$ (respectively, $h_{il} > 0$) if there is a link between the kth leader (respectively, the lth adversary) and the ith follower, otherwise $g_{ik} = 0$ (respectively, $h_{il} = 0$). $\mathcal{G}_k = \mathrm{diag}\left(g_{ik}\right), i \in \mathscr{F}$. For convenience, we assume there are n followers and m leaders.

We use the following notations throughout this note: $\sigma_{\min}(X)$, $\sigma_{\max}(X)$, $\sigma(X)$, and $\rho(X)$ are the minimum and maximum singular values, the spectrum, and the spectral radius of matrix X. $I_n \in \mathbb{R}^{n\times n}$ is the identity matrix. $\mathbf{1}_n \in \mathbb{R}^n$ is a vector with all entries of one. Kronecker product is denoted by $\otimes$. The operator $\mathrm{diag}\{\cdot\}$ builds a block diagonal matrix from its argument. $\|\cdot\|$ denotes the Euclidean norm. The distance from $x \in \mathbb{R}^n$ to the set $\mathfrak{C} \subseteq \mathbb{R}^n$ in the sense of Euclidean norm is denoted by $\mathrm{dist}(x, \mathfrak{C})$, that is, dist $(x, \mathfrak{C}) = \inf_{y\in\mathfrak{C}} \|x - y\|_2$.

B. Problem Formulation

We consider a new type of heterogeneous multi-group system, consisting of cooperative leaders and followers, as well as malicious adversaries. The dynamics of the kth leader and the ith follower are given by

$$\begin{cases} \dot{x}_k = Sx_k \\ y_k = Rx_k \end{cases} k \in \mathscr{L}, \quad \begin{cases} \dot{x}_i = A_i x_i + B_i u_i \\ y_i = C_i x_i \end{cases} i \in \mathscr{F}, \tag{1}$$

respectively, where $x_k \in \mathbb{R}^q$ and $y_k \in \mathbb{R}^p$ are the state and output of the kth leader, respectively, $x_i \in \mathbb{R}^{n_i}$, $u_i \in \mathbb{R}^{m_i}$, and $y_i \in \mathbb{R}^p$ are the state, input, and output of the ith follower, respectively. The dynamics of the lth adversary are given by

$$\begin{cases} \dot{x}_l = f_l(x_l) \\ y_l = C_l x_l \end{cases} l \in \mathscr{A}, \tag{2}$$

where $x_l \in \mathbb{R}^{n_l}$ and $y_l \in \mathbb{R}^p$ are the state and output of the lth adversary, respectively. $f_l \in \mathbb{R}^{n_l}$ is the internal dynamics, and is a smooth vector field on a invariant set $W_l \in \mathbb{R}^{n_l}$ with $f_l(0) = 0$. Let

$$M_l = \left.\frac{\partial f_l(x_l)}{\partial x_l}\right|_{x_l=0} \tag{3}$$

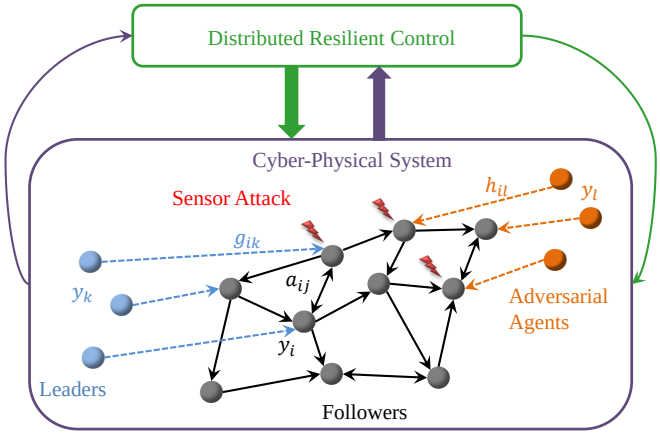

Fig. 1: General layout of a networked cooperative and adversarial multi-group system.

be linear approximation of function f_l. For convenience, we assume adversaries do not have any control input. Note that the system dynamics (f_l, C_l) can be different for each $l \in \mathscr{A}$. The multi-group system is called heterogeneous because their dynamics (S, R), (A_i, B_i, C_i), and (f_l, C_l) are generally not the same.

General layout of a networked cooperative and adversarial multi-group system is illustrated in Fig. 1. For each follower, the state is under an unknown sensor fault, described as

$$\bar{x}_i = x_i + \delta_i, \tag{4}$$

where δ_i denotes the unknown fault from the sensor channel. That is, the actual values of x_i and δ_i are unknown and we can only measure the corrupted state information $\bar{x}_i$. As shown in Fig. 1, each follower receive direct information/data from both the leaders and the adversaries, due to the complex dynamic distributed environment. To this end, take the following corrupted local neighboring relative output information for each follower

$$\bar{e}_{y_i} = \sum_{j \in \mathscr{F}} a_{ij} \left(\bar{y}_j - \bar{y}_i\right) + \sum_{k \in \mathscr{L}} g_{ik} \left(y_k - \bar{y}_i\right) + \sum_{l \in \mathscr{A}} h_{il} \left(y_l - \bar{y}_i\right), \tag{5}$$

where $\bar{y}_i = C_i \bar{x}_i$ is the corrupted output information. Consider the following distributed control protocols

$$u_i = K_i \bar{x}_i + H_i \bar{z}_i - H_i \hat{d}_i \tag{6}$$

$$\dot{\bar{z}}_i = F_i \bar{z}_i + G_i \bar{e}_{y_i}, \tag{7}$$

where K_i, H_i, F_i, and G_i are gain matrices with appropriate dimensions, $\hat{d}_i$ is certain compensational signal to be designed, and $\bar{z}_i$ is the corrupted compensator state.

We make the following assumptions about the participating agents and the communication network.

Assumption 1: There exists at least one leader that has a directed path to each follower $i \in \mathscr{F}$ in the digraph $\mathscr{G}$.

Assumption 2: All eigenvalues of the leaders' dynamics S and the adversaries' dynamics M_l are on the imaginary axis and they are non-repeated.

Assumption 3: (A_i, B_i) is stabilizable and (A_i, C_i) is detectable for each $i \in \mathscr{F}$.

Assumption 4: For all $\lambda \in \sigma(S)$,

$$\operatorname{rank} \begin{bmatrix} A_i - \lambda I_{n_i} & B_i \\ C_i & 0 \end{bmatrix} = n_i + p, \ i \in \mathscr{F}. \tag{8}$$

Assumption 5: The sensor fault δ_i in (4) and its derivative $\dot{\delta}_i$ are bounded.

Remark 1: Assumptions 1, 3, and 4 are standard assumptions for output containment of heterogeneous MAS [8], [26]–[28]. Assumption 2 is made to assure that x_k and x_l are bounded, and also to avoid the trivial case of stable S and M_l. In practice, the adversaries have limited budgets to inject sensor faults to the MAS. In the case when the adversaries launch attacks of infinite magnitude, the cooperative MAS can simply reject such injections by removing excessively large values, which can be easily detected [29]–[31]. We can incorporate a defensive mechanism into (5) for the case of

unbounded attacks. One such example is by letting $a_{ij} = 1$ and/or $h_{il} = 1$, if $\bar{y}_j \in \Theta$ and/or $\bar{y}_l \in \Theta$, otherwise $a_{ij} = 0$ and/or $h_{il} = 0$, where Θ is a compact set describing all feasible values of output variables, which can be chosen based on the operational range of physical variables to be controlled.

Definition 1: A set $\mathfrak{C} \subseteq \mathbb{R}^n$ is convex if $(1-\varepsilon)\, x + \varepsilon y \in \mathfrak{C}$, for any $x, y \in \mathfrak{C}$ and any $\varepsilon \in [0, 1]$ [32]. Let $Y_{\mathscr{L}}$ be the set of the leaders' outputs. The convex hull of $Y_{\mathscr{L}}$ is the minimal convex set containing all points in $Y_{\mathscr{L}}$. That is, $\mathrm{Co}\,(Y_{\mathscr{L}}) = \big\{ \sum_{k\in\mathscr{L}} \alpha_k y_k \big|\, \alpha_k \in \mathbb{R}, \alpha_k \geq 0, \sum_{k\in\mathscr{L}} \alpha_k = 1 \big\}$.

The output containment control objective is to make the output of each follower converge into the dynamic convex hull spanned by the outputs of the leaders, that is

$$\lim_{t\to\infty} \mathrm{dist}(y_i(t), \mathrm{Co}(Y_{\mathscr{L}}(t))) = 0, \quad \forall i \in \mathscr{F} \tag{9}$$

Define the local cooperative neighboring relative output information as

$$e_{y_i} = \sum_{j\in\mathscr{F}} a_{ij}\,(y_j - y_i) + \sum_{k\in\mathscr{L}} g_{ik}\,(y_k - y_i). \tag{10}$$

The global form of (10) can be written as

$$e_y = -\sum_{k\in\mathscr{L}} (\Psi_k \otimes I_p)(y - \underline{y}_k), \tag{11}$$

where $\Psi_k = (\frac{1}{m}\mathcal{L} + \mathcal{G}_k)$, $e_y = [e_{y_1}^T, ..., e_{y_n}^T]^T$, $y = [y_1^T, ..., y_n^T]^T$, and $\underline{y}_k = (\mathbf{1}_n \otimes y_k)$.

Lemma 1 [26]: Given Assumption 1, the matrices Ψ_k and $\sum_{k\in\mathscr{L}} \Psi_k$ are positive-definite and non-singular. Moreover, both $(\Psi_k)^{-1}$ and $(\sum_{k\in\mathscr{L}} \Psi_k)^{-1}$ are non-negative.

Define the global output containment error vector as

$$\eta = y - \left(\sum_{r\in\mathscr{L}} (\Psi_r \otimes I_p) \right)^{-1} \sum_{k\in\mathscr{L}} (\Psi_k \otimes I_p)\, \underline{y}_k, \tag{12}$$

where $\eta = [\eta_1^T, ..., \eta_n^T]^T$ and $e_y = -\sum_{k\in\mathscr{L}} (\Psi_k \otimes I_p)\eta$.

Lemma 2 [27]: Given Assumption 1. The output containment control objective in (9) is achieved if $\lim_{t\to\infty} \eta(t) = 0$.

Definition 2 [33]: The signal $x(t)$ is said to be UUB with ultimate bound b, if there exist positive constants b and c, independent of $t_0 \geq 0$, and for every $a \in (0, c)$, there is $T_1 = T_1(a, b) \geq 0$, independent of t_0, such that

$$\|x(t_0)\| \leq a \quad \Rightarrow \quad \|x(t)\| \leq b, \forall t \geq t_0 + T_1 \tag{13}$$

Now, we introduce the distributed resilient output containment problem for heterogeneous cooperative and adversarial multi-group systems.

Definition 3: Consider the dynamics of the leaders and the followers in (1), and the adversaries' dynamics (2) on a cooperative and adversarial multi-group communication digraph $\mathscr{G}$. The resilient output containment problem is to design distributed control protocols u_i in (1) for each follower such that for all initial conditions, η in (12) is UUB.

III. Distributed Ultimate Boundedness and Stabilization for Resilient Output Containment

In this section, we present a distributed resilient compensational method to solve the resilient output containment problem, in the presence of sensor faults and malicious attacks from adversaries. First, a distributed observer structure is proposed. Then, a local design procedure is given for observer gains. Finally, it is shown the proposed control structure solves the resilient output containment problem.

A. Distributed Observer Structure for Resilient Output Containment

We first introduce the following two measurable error terms

$$\theta_i = \bar{x}_i - \hat{x}_i - \hat{\delta}_i, \tag{14}$$

$$\varpi_i = \bar{z}_i - \hat{z}_i - \hat{d}_i, \tag{15}$$

where $\hat{x}_i$ and $\hat{z}_i$ are estimations of uncorrupted state and compensator state, respectively. $\hat{\delta}_i$ is an estimation term of the sensor fault. It is seen that both θ_i and ϖ_i can be measured. Noting that ϖ_i can be considered as a resilience index to the error propagation across the communication network since $\bar{z}_i$ only uses $\bar{e}_{y_i}$, which includes the propagated attack information from the neighbors. Let $\hat{y}_i = C_i\hat{x}_i$. Define the following local neighboring relative output estimation for each observer

$$\hat{e}_{y_i} = \sum_{j\in\mathscr{F}} a_{ij}\left(\hat{y}_j - \hat{y}_i\right) + \sum_{k\in\mathscr{L}} g_{ik}\left(y_k - \hat{y}_i\right), \tag{16}$$

To cope with the sensor faults and malicious attacks from the adversaries, we present the following distributed observer structure

$$\dot{\hat{x}}_i = A_i\hat{x}_i + B_iK_i\hat{x}_i + B_iH_i\hat{z}_i + B_iH_i\varpi_i, \tag{17}$$

$$\dot{\hat{z}}_i = F_i\hat{z}_i + G_i\hat{e}_{y_i}, \tag{18}$$

$$\dot{\hat{\delta}}_i = -\left(A_i + B_iK_i\right)\theta_i - B_iH_i\varpi_i, \tag{19}$$

$$\dot{\hat{d}}_i = F_i\hat{d}_i - G_iC_i\hat{\delta}_i. \tag{20}$$

This observer structure serves to compute the compensational signal $\hat{d}_i$, which is used in the distributed control protocols (6).

Remark 2: The observer's dynamics in (17) can be adversely affected by the sensor faults and the adversaries' attacks due to the extra term $B_iH_i\varpi_i$. This is more practical compared to the ideal observer structure in [24]. Moreover, [24] requires the initial

condition of each observer's output equals to that of each follower's output, which may not be guaranteed in practice.

B. Local Design of Observer Gains

We first analyze the containment convergence for the observer's output $\hat{y}_i$. Assume the communication digraph of the observers is normalized so that

$$\sum_{j\in\mathscr{F}} a_{ij} + \sum_{k\in\mathscr{L}} g_{ik} = 1,\ \forall i \in \mathscr{F}. \tag{21}$$

Then, $\hat{e}_{y_i}$ in (16) can be rewritten as

$$\hat{e}_{y_i} = -\hat{y}_i + \sum_{j\in\mathscr{F}} a_{ij}\hat{y}_j + \sum_{k\in\mathscr{L}} g_{ik} y_k. \tag{22}$$

Define

$$\vec{A}_i = \begin{bmatrix} A_i + B_i K_i & B_i H_i \\ -G_i C_i & F_i \end{bmatrix}, \tag{23}$$

$\vec{x}_i = [\hat{x}_i^T, \hat{z}_i^T]^T$, $\vec{G}_i = [\ 0 \quad {G_i}^T\ ]^T$, $\vec{C}_i = \begin{bmatrix} C_i & 0 \end{bmatrix}$, and $\vec{H}_i = \begin{bmatrix} B_i H_i \\ 0 \end{bmatrix}$. Then, the augmented dynamics of (17) and (18) has the following closed-loop form

$$\begin{cases} \dot{\vec{x}}_i = \vec{A}_i\vec{x}_i + \vec{G}_i \sum\limits_{j\in\mathscr{F}} a_{ij}\vec{C}_j\vec{x}_j + \\ \qquad\qquad \vec{G}_i \sum\limits_{k\in\mathscr{L}} g_{ik} R x_k + \vec{H}_i\varpi_i, \\ \hat{y}_i = \vec{C}_i\vec{x}_i. \end{cases} \tag{24}$$

Denote $\vec{x} = [\vec{x}_1^T, ..., \vec{x}_n^T]^T$, $\hat{y} = [\hat{y}_1^T, ..., \hat{y}_n^T]^T$, and $\underline{x}_k = \mathbf{1}_n \otimes x_k$. The global form of

(24) can be written as

$$\begin{cases} \dot{\vec{x}} = \mathrm{diag}(\vec{A}_i)\vec{x} + \mathrm{diag}(\vec{G}_i)\left(\mathcal{A} \otimes I_p\right)\mathrm{diag}(\vec{C}_i)\vec{x} + \\ \mathrm{diag}(\vec{G}_i)\sum\limits_{k\in\mathscr{L}}\left(\mathcal{G}_k \otimes I_p\right)\left(I_n \otimes R\right)\underline{x}_k + \mathrm{diag}(\vec{H}_i)\varpi, \\ \hat{y} = \mathrm{diag}(\vec{C}_i)\vec{x}, \end{cases} \tag{25}$$

For the next result, we first introduce the following augmented output regulator equations with solutions X_i

$$\begin{cases} \vec{A}_i X_i + \vec{G}_i R = X_i S, \\ \vec{C}_i X_i = R. \end{cases} \tag{26}$$

Then, we define the following global estimation state-containment error vector

$$\xi = \vec{x} - \mathrm{diag}\left(X_i\right)\left(\sum_{r=n+1}^{n+m}\left(\Psi_r \otimes I_q\right)\right)^{-1}\sum_{k\in\mathscr{L}}\left(\Psi_k \otimes I_q\right)\underline{x}_k, \tag{27}$$

where $\xi = [\xi_1^T, ..., \xi_n^T]^T$. Based on (21), (25), and (26), taking the derivative of (27) with respect to t, and doing the same manipulations as Theorem 1 of [27], we obtain the following global closed-loop estimation output-containment error dynamics

$$\begin{cases} \dot{\xi} = \mathrm{diag}(\vec{A}_i)\xi + \mathrm{diag}(\vec{G}_i)(\mathcal{A} \otimes I_p)\,\mathrm{diag}(\vec{C}_i)\xi + \mathrm{diag}(\vec{H}_i)\varpi, \\ \hat{\eta} = \mathrm{diag}(\vec{C}_i)\xi, \end{cases} \tag{28}$$

where $\hat{\eta} = \hat{y} - \left(\sum_{r=n+1}^{n+m}\left(\Psi_r \otimes I_p\right)\right)^{-1}\sum_{k\in\mathscr{L}}\left(\Psi_k \otimes I_p\right)\underline{y}_k = [\hat{\eta}_1^T, ..., \hat{\eta}_n^T]^T$ is the estimated global output containment error, i.e., estimation of η in (12). The local form of (28) can be written as

$$\begin{cases} \dot{\xi}_i = \vec{A}_i\xi_i + \vec{G}_i\sum\limits_{j\in\mathscr{F}} a_{ij}\vec{C}_j\xi_j + \vec{H}_i\varpi_i, \\ \hat{\eta}_i = \vec{C}_i\xi_i. \end{cases} \tag{29}$$

Next, we give the local sufficient conditions to guarantee the UUB containment

convergence for the estimation observers.

Lemma 3: Suppose that Assumption 1 holds. Let the observer's dynamics consist of (17) and (18), the local observer's output, $\hat{y}_i$, achieves the UUB output containment convergence, if the following two local conditions both hold for each $i \in \mathscr{F}$:

(i) There exists a unique solution X_i to the augmented output regulator equations (26);

(ii) The local closed-loop estimation output containment error system (29) is UUB.

Proof: It is seen that, if condition (i) holds, the output containment convergence can be achieved by stabilizing system (29). This completes the proof. ■

The following result is needed to construct observer gains.

Lemma 4 (Theorem 1.9 of [8]): Given Assumption 4, the following local output regulator equations

$$\begin{cases} A_i\Pi_i + B_i\Gamma_i = \Pi_i S, \\ C_i\Pi_i = R, \end{cases} \tag{30}$$

have a unique solution pair (Π_i, Γ_i).

Now, we give local design procedures to guarantee conditions (i) and (ii) of Lemma 3. The next result gives the detailed procedure to choose observer gains for (17) to (20).

Lemma 5 (Theorem 2 of [4]): Assume that for each $i \in \mathscr{F}$, matrix $\vec{A}_i$ is Hurwitz. Make Assumption 4. Let (Π_i, Γ_i) be the solution to (30). Then, under Assumption 2, there exists a unique solution $X_i = \left[\begin{array}{cc} \Pi_i^T & I_q \end{array} \right]^T$ to (26), if the gain matrices K_i , H_i , F_i, and G_i are designed as

$$\begin{cases} H_i = \Gamma_i - K_i\Pi_i, \\ F_i = S, \end{cases} \tag{31}$$

where K_i is such that $A_i + B_iK_i$ is Hurwitz and G_i is such that (S, G_i) is controllable.

Now, we define $\bar{A}_i = \left[\begin{array}{cc} A_i & B_i\Gamma_i \\ -G_iC_i & S \end{array} \right]$, $\bar{B}_i = \left[\begin{array}{c} B_i \\ 0 \end{array} \right]$, $\bar{u}_i = K_i \left[\begin{array}{cc} I_{n_i} & -\Pi_i \end{array} \right] \xi_i$,

and $\varepsilon_i = \sum_{j\in\mathscr{F}} a_{ij}\vec{C}_j\xi_j$. Then, using (31) to rewrite (29) as

$$\begin{cases} \dot{\xi}_i = \bar{A}_i\xi_i + \bar{B}_i\bar{u}_i + \vec{G}_i\varepsilon_i + \vec{H}_i\varpi_i, \\ \hat{\eta}_i = \vec{C}_i\xi_i, \end{cases} \tag{32}$$

Define measured outputs

$$\bar{w}_i = \begin{bmatrix} I_{n_i} & -\Pi_i \end{bmatrix} \xi_i \equiv \Phi_i\xi_i. \tag{33}$$

Definition 4: Consider the local system (32) with control input $\bar{u}_i(t)$, performance output $\hat{\eta}_i(t)$, and disturbance $\varepsilon_i(t)$. The system $\mathcal{L}_2$-gain is said to be bounded by a prescribed γ_i if

$$\frac{\int_0^\infty (\hat{\eta}_i^T(t)\hat{\eta}_i(t) + \alpha_i\bar{u}_i^T(t)Q_i\bar{u}_i(t))dt}{\int_0^\infty \varepsilon_i^T(t)\varepsilon_i(t)dt} \leq \gamma_i^2, \tag{34}$$

for some weight matrices $Q_i^T = Q_i \succ 0$ and scalars $\alpha_i > 0$.

Based on the small-gain theorem [33], (32) is stable for each $i \in \mathscr{F}$, if the system $\mathcal{L}_2$-gain is bounded by $\gamma_i < 1/\rho(\mathcal{A})$.

Theorem 1: Given Assumptions 1 to 4, select $\gamma_i < 1/\rho(\mathcal{A})$, and use Lemma 5 to design the gain matrices. Then, the local estimation output containment error $\hat{\eta}_i(t)$ in (29) is UUB if

(i) There exist matrices K_i and L_i such that

$$K_i\Phi_i = -(1/\alpha_i)Q_i^{-1}\left(\bar{B}_i^T P_i + L_i\right), \tag{35}$$

where $P_i^T = P_i \succ 0$ is the solution to

$$\begin{aligned} &P_i\bar{A}_i + \bar{A}_i^T P_i + \vec{C}_i^T\vec{C}_i + (1/\gamma_i^2)P_i\vec{G}_i\vec{G}_i^T P_i \\ &-(1/\alpha_i)P_i\bar{B}_iQ_i^{-1}\bar{B}_i^T P_i + (1/\alpha_i)L_i^T R_i^{-1}L_i = 0. \end{aligned} \tag{36}$$

(ii) The measurable error ϖ_i is UUB.

Proof: Use (34) to define the following performance function

$$J(K_i, \varepsilon_i) = \int_0^\infty (\hat{\eta}_i^T \hat{\eta}_i + \alpha_i \bar{u}_i^T Q_i \bar{u}_i - \gamma_i^2 \varepsilon_i^T \varepsilon_i) dt. \tag{37}$$

Define the following quadratic energy function

$$V^*(\xi_i(t)) = \xi_i(t)^T P_i \xi_i(t) \geq 0, \tag{38}$$

where $V^*(\xi_i)$ is the optimal value function. Then, the Hamiltonian function is given by

$$\begin{aligned} \Theta_i(V_i^*, K_i, \varepsilon_i) &= (\frac{\partial V_i^*}{\partial \xi_i})^T (\bar{A}_i \xi_i + \bar{B}_i K_i \Phi_i \xi_i + \vec{G}_i \varepsilon_i \\ &+ \vec{H}_i \varpi_i) + \hat{\eta}_i^T \hat{\eta}_i + \alpha_i \xi_i^T \Phi_i^T K_i^T Q_i K_i \Phi_i \xi_i - \gamma_i^2 \varepsilon_i^T \varepsilon_i. \end{aligned} \tag{39}$$

Note that $(\partial V_i^*/\partial \xi_i)^T = 2\xi_i^T P_i$. Based on the H_∞ control theory [34], applying the stationarity condition $\partial \Theta_i(V_i^*, K_i, \varepsilon_i)/\partial \varepsilon_i = 2\vec{G}_i^T P_i \xi_i - 2\gamma_i^2 \varepsilon_i = 0$ yields the following maximizing disturbance inputs

$$\varepsilon_i^* = (1/\gamma_i^2) \vec{G}_i^T P_i \xi_i. \tag{40}$$

Substituting (40) into (39) yields

$$\begin{aligned} &\Theta_i(V_i^*, K_i, \varepsilon_i^*) = \xi_i^T (P_i \bar{A}_i + \bar{A}_i^T P_i + \vec{C}_i^T \vec{C}_i + \\ &(1/\gamma_i^2) P_i \vec{G}_i \vec{G}_i^T P_i + P_i \bar{B}_i K_i \Phi_i + \Phi_i^T K_i^T \bar{B}_i^T P \\ &+ \alpha_i \Phi_i^T K_i^T Q_i K_i \Phi_i) \xi_i + 2\xi_i^T P_i \vec{H}_i \varpi_i \\ &= \xi_i^T (P_i \bar{A}_i + \bar{A}_i^T P_i + \vec{C}_i^T \vec{C}_i + (1/\gamma_i^2) P_i \vec{G}_i \vec{G}_i^T P_i - \\ &(1/\alpha_i) P_i \bar{B}_i Q_i{}^{-1} \bar{B}_i^T P_i + (\alpha_i K_i \Phi_i + Q_i{}^{-1} \bar{B}_i^T P)^T \times \\ &Q_i (K_i \Phi_i + (1/\alpha_i) Q_i{}^{-1} \bar{B}_i^T P_i)) \xi_i + 2\xi_i^T P_i \vec{H}_i \varpi_i. \end{aligned} \tag{41}$$

Substituting the control gain defined by (35) into (41), and noting that (36) holds,

the following Hamilton-Jacobi-Isaac (HJI) equation can be obtained

$$\begin{aligned}&\Theta_i(V_i^*, K_i^*, \varepsilon_i^*) = \xi_i^T(P_i\bar{A}_i + \bar{A}_i^T P_i + \vec{C}_i^T\vec{C}_i + \\ &(1/\gamma_i^2)P_i\vec{G}_i\vec{G}_i^T P_i - (1/\alpha_i)P_i\bar{B}_i{Q_i}^{-1}\bar{B}_i^T P_i + \\ &(1/\alpha_i)L_i^T{Q_i}^{-1}L_i)\xi_i + 2\xi_i^T P_i\vec{H}_i\varpi_i = 2\xi_i^T P_i\vec{H}_i\varpi_i.\end{aligned} \tag{42}$$

Expressing the Hamiltonian function for any K_i and ε_i in terms of the Hamiltonian function for K_i^* and ε_i^* [35] yields

$$\begin{aligned}&\Theta_i(V_i^*, K_i, \varepsilon_i) = \Theta_i(V_i^*, K_i^*, \varepsilon_i^*) + \xi_i^T\times \\ &(L_i + Q_i(K_i - K_i^*)\Phi_i)^T Q_i^{-1}(L_i + Q_i(K_i - K_i^*)\Phi_i) \\ &\times\xi_i - \xi_i^T(L_i^T{Q_i}^{-1}L_i)\xi_i - \gamma_i^2\|\varepsilon_i - \varepsilon_i^*\|^2.\end{aligned} \tag{43}$$

Combining (39) and (43), and using (42), we obtain

$$\begin{aligned}&\dot{V}_i^* + \hat{\eta}_i^T\hat{\eta}_i + \alpha_i\bar{u}_i^T Q_i\bar{u}_i - \gamma_i^2\varepsilon_i^T\varepsilon_i \\ &= \xi_i^T(L_i + Q_i(K_i - K_i^*)\Phi_i)^T Q_i^{-1}\times \\ &\quad (L_i + Q_i(K_i - K_i^*)\Phi_i)\xi_i - \xi_i^T(L_i^T Q_i^{-1}L_i)\xi_i \\ &\quad -\gamma_i^2\|\varepsilon_i - \varepsilon_i^*\|^2 + 2\xi_i^T P_i\vec{H}_i\varpi_i.\end{aligned} \tag{44}$$

Substituting the optimal gain $K_i = K_i^*$ in (44) yields

$$\dot{V}_i^* + \hat{\eta}_i^T\hat{\eta}_i + \alpha_i\bar{u}_i^{*T} Q_i\bar{u}_i^* - \gamma_i^2\varepsilon_i^T\varepsilon_i = -\gamma_i^2\|\varepsilon_i - \varepsilon_i^*\|^2 + 2\xi_i^T P_i\vec{H}_i\varpi_i. \tag{45}$$

From [34], a sufficient condition to achieve the bounded $\mathcal{L}_2$-gain in (34) is

$$-\gamma_i^2\|\varepsilon_i - \varepsilon_i^*\|^2 + 2\xi_i^T P_i\vec{H}_i\varpi_i \leq 0. \tag{46}$$

Using (40) to obtain the following sufficient condition to guarantee (46)

$$2\left\|\xi_i^T P_i\vec{H}_i\varpi_i\right\| \leq \gamma_i^2\left\|\varepsilon_i - (1/\gamma_i^2)\vec{G}_i^T P_i\xi_i\right\|^2. \tag{47}$$

Then, with some manipulations of standard properties of matrix and vector norms, we obtain the following sufficient condition to achieve the bounded $\mathcal{L}_2$-gain in (34)

$$\|\xi_i\| \geq \frac{2\gamma_i^2}{\sigma_{\min}(P_i\vec{G}_i\vec{G}_i^T P_i)} \left(\gamma_i^2 \left\|P_i\vec{H}_i\right\| \|\varpi_i\| + \left\|\vec{G}_i^T P_i\right\| \|\varepsilon_i\|\right). \tag{48}$$

It is seen that, if ϖ_i is UUB, then the local estimation output containment error, $\hat{\eta}_i$, is UUB. This completes the proof. ■

Remark 3: By using the small-gain theorem to decouple the local controller design and the graph spectrum property, the stabilization problem is cast into a $\mathcal{L}_2$-gain static output-feedback problem, which can be solved by a modified yet more general algebraic Riccati equation (36) for some L_i. Noting that the disturbance rejection can also be assured by lumping the disturbance matrix and $\vec{G}_i$ together.

Remark 4: If $1/\rho(\mathcal{A})$ or its estimated information is unknown to each follower, γ_i can be set as small as possible. Noting that a necessary condition for the existence of a positive-definite solution P_i to (36) is $\gamma_i > \gamma_i^*$, where γ_i^* is the smallest allowable γ_i that guarantees (36) to have a positive-definite solution. This γ_i^* is larger than the standard H_∞ gain using state-feedback approach due to the fact that the static output-feedback is a subset of the state-feedback.

Remark 5: It will be proved in the next section that by designing the gain matrices as in Lemma 5, condition (ii) in Theorem 1 is guaranteed if condition (i) holds.

C. Resilient Output Containment Solution

It was shown in the previous section that despite the sensor faults and the malicious attacks from the adversaries, the proposed observer structure (17) and (18) guarantees the UUB convergence of the observer's output $\hat{y}_i$ to the dynamic convex hull spanned by multiple leaders' outputs under certain conditions. Therefore, to solve the resilient output containment problem introduced in Definition 3, it remains to show the UUB

convergence of each follower's output y_i to the estimation observer's output $\hat{y}_i$. That is, $\tilde{y}_i \equiv y_i - \hat{y}_i = C_i\left(x_i - \hat{x}_i\right)$ is UUB.

Next, we present the main result of the containment convergence analysis of each follower using the proposed approach.

Theorem 2: Given Assumptions 1, 2, 3, 4 and 5, consider the heterogeneous cooperative and adversarial multi-group system composed of (1) and (3). The resilient output containment problem under the sensor faults (4) and the malicious attacks from the adversaries, is solved by the distributed control protocols (6), (7), (17) to (20) if the gain matrices are designed as (31) and (35).

Proof: Theorem 1 proves that the local estimation output-containment error $\hat{\eta}_i$ of each observer is UUB. Hence, to solve the resilient output containment problem, we need to prove that $\tilde{y}_i$ is UUB, and condition (ii) in Theorem 1 holds.

Using (4), (6), (7), and (17) to (19) to differentiate the measurable error θ_i in (14) yields

$$\begin{aligned}\dot{\theta}_i &= \dot{\bar{x}}_i - \dot{\hat{x}}_i - \dot{\hat{\delta}}_i \\ &= A_i x_i + B_i K_i \bar{x}_i - A_i \hat{x}_i - B_i K_i \hat{x}_i + \left(A_i + B_i K_i\right)\theta_i + B_i H_i \varpi_i + \dot{\delta}_i \\ &= 2\left(A_i + B_i K_i\right)\theta_i + B_i H_i \varpi_i - \left(A_i + B_i K_i\right)\tilde{\delta}_i + B_i K_i \delta_i + \dot{\delta}_i.\end{aligned} \tag{49}$$

Using (7), (18) and (20) to differentiate the measurable error ϖ_i in (15) yields

$$\begin{aligned}\dot{\varpi}_i &= \dot{\bar{z}}_i - \dot{\hat{z}}_i - \dot{\hat{d}}_i \\ &= S\bar{z}_i + G_i \bar{e}_{y_i} - S\hat{z}_i - G_i \hat{e}_{y_i} - S\hat{d}_i + G_i C_i \hat{\delta}_i \\ &= S\varpi_i + G_i\left(\bar{e}_{y_i} - \hat{e}_{y_i}\right) + G_i C_i \hat{\delta}_i.\end{aligned} \tag{50}$$

Noting that

$$\begin{aligned}\bar{e}_{y_i} - \hat{e}_{y_i} &= -(\sum_{j\in\mathscr{F}} a_{ij} + \sum_{k\in\mathscr{L}} g_{ik})C_i\left(\bar{x}_i - \hat{x}_i\right) \\ &\quad + \sum_{j\in\mathscr{F}} a_{ij}C_j\left(\bar{x}_j - \hat{x}_j\right) + \sum_{l\in\mathscr{A}} h_{il}\left(y_l - \bar{y}_i\right) \\ &= -C_i(\theta_i + \hat{\delta}_i) + \sum_{j\in\mathscr{F}} a_{ij}C_j(\theta_j + \hat{\delta}_j) + \sum_{l\in\mathscr{A}} h_{il}\left(y_l - \bar{y}_i\right).\end{aligned} \tag{51}$$

Hence, we obtain

$$\dot{\varpi}_i = S\varpi_i - G_iC_i\theta_i + G_i\sum_{j\in\mathscr{F}} a_{ij}C_j(\theta_j - \tilde{\delta}_j) + G_i\sum_{j\in\mathscr{F}} a_{ij}C_j\delta_j + G_i\sum_{l\in\mathscr{A}} h_{il}\left(y_l - \bar{y}_i\right). \tag{52}$$

For convenience, denote $\chi_i = G_i\sum_{j\in\mathscr{F}} a_{ij}C_j\delta_j + G_i\sum_{l\in\mathscr{A}} h_{il}\left(y_l - \bar{y}_i\right)$. It is seen that, given Assumptions 2 and 5, χ_i is bounded. Define the estimation error of the sensor fault to be $\tilde{\delta}_i = \delta_i - \hat{\delta}_i$. Then, using (19) one has

$$\dot{\tilde{\delta}}_i = \dot{\delta}_i - \dot{\hat{\delta}}_i = \left(A_i + B_iK_i\right)\theta_i + B_iH_i\varpi_i + \dot{\delta}_i. \tag{53}$$

Define

$$A_i^a = \begin{bmatrix} 2\left(A_i + B_iK_i\right) & B_iH_i & -\left(A_i + B_iK_i\right) \\ -G_iC_i & S & 0 \\ A_i + B_iK_i & B_iH_i & 0 \end{bmatrix}, \tag{54}$$

$G_i^a = \begin{bmatrix} 0 \\ G_i \\ 0 \end{bmatrix}$, $\psi_i = \begin{bmatrix} \theta_i \\ \varpi_i \\ \tilde{\delta}_i \end{bmatrix}$, $\Delta_i = \begin{bmatrix} B_iK_i\delta_i + \dot{\delta}_i \\ \chi_i \\ \dot{\delta}_i \end{bmatrix}$, and $C_i^a = \begin{bmatrix} C_i & 0 & -C_i \end{bmatrix}$.
Noting that Δ_i is bounded.

Then, the augmented dynamics of (49), (52), and (53) becomes

$$\dot{\psi}_i = A_i^a\psi_i + G_i^a\sum_{j\in\mathscr{F}} a_{ij}C_j^a\psi_j + \Delta_i. \tag{55}$$

Let $T_i = \begin{bmatrix} I_{n_i} & 0 & 0 \\ 0 & I_q & 0 \\ -I_{n_i} & 0 & I_{n_i} \end{bmatrix}$. Define the following coordinate transformation

$$\zeta_i = T_i \psi_i. \tag{56}$$

Then, we obtain

$$\dot{\zeta}_i = T_i A_i^a T_i^{-1} \zeta_i + T_i G_i^a \sum_{j \in \mathscr{F}} a_{ij} C_j^a T_i^{-1} \zeta_j + T_i \Delta_i. \tag{57}$$

Noting that

$$\begin{aligned} \bar{A}_i^a &\equiv T_i A_i^a T_i^{-1} \\ &= \begin{bmatrix} A_i + B_i K_i & B_i H_i & -(A_i + B_i K_i) \\ -G_i C_i & S & 0 \\ 0 & 0 & A_i + B_i K_i \end{bmatrix}. \end{aligned} \tag{58}$$

Reformulating (57) as

$$\dot{\zeta}_i = \bar{A}_i^a \zeta_i + \bar{\Delta}_i, \tag{59}$$

where $\bar{\Delta}_i = T_i G_i^a \sum_{j \in \mathscr{F}} a_{ij} C_j^a T_i^{-1} \zeta_j + T_i \Delta_i$. It is seen that, if $\vec{A}_i = \begin{bmatrix} A_i + B_i K_i & B_i H_i \\ -G_i C_i & S \end{bmatrix}$ and $A_i + B_i K_i$ are Hurwitz, then $\bar{A}_i^a$ is Hurwitz. Next, we prove that, if condition (i) in Theorem 1 holds, then both $\vec{A}_i$ and $A_i + B_i K_i$ are Hurwitz. Use (35) to rewrite (36) as

$$\begin{aligned} &P_i \left(\bar{A}_i + \bar{B}_i K_i \Phi_i \right) + (\bar{A}_i + \bar{B}_i K_i \Phi_i)^T P_i + \vec{C}_i^T \vec{C}_i \\ &+ (1/\gamma_i^2) P_i \vec{G}_i \vec{G}_i^T P_i + \alpha_i \Phi_i^T K_i^T R_i K_i \Phi_i = 0. \end{aligned} \tag{60}$$

Since $\vec{C}_i^T \vec{C}_i + (1/\gamma_i^2) P_i \vec{G}_i \vec{G}_i^T P_i + \alpha_i \Phi_i^T K_i^T R_i K_i \Phi_i \succ 0$ and $P_i \succ 0$, we obtain that $\vec{A}_i = \bar{A}_i + \bar{B}_i K_i \Phi_i$ is Hurwitz. It follows from Lemma 5 that $A_i + B_i K_i$ is also Hurwitz. Hence, $\bar{A}_i^a$ is Hurwitz. Then, given any $Q_i^a \succ 0$, there exists $P_i^a \succ 0$ such that $P_i^a \bar{A}_i^a + \bar{A}_i^{aT} P_i^a = -Q_i^a$. Choosing the Lyapunov function candidate as $V_i^a = \zeta_i^T P_i^a \zeta_i$,

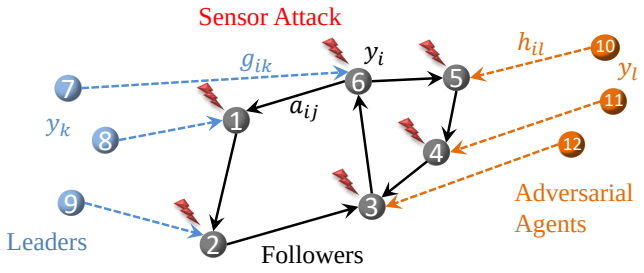

Fig. 2: The communication digraph $\mathscr{G}$ of heterogeneous multi-group systems.

and its time derivative is $\dot{V}_i^a = -\zeta_i^T Q_i^a \zeta_i + 2\zeta_i^T P_i^a \bar{\Delta}_i$. Recalling Sylvester's inequality, we obtain $\dot{V}_i^a \leq -\sigma_{\min}(Q_i^a) \|\zeta_i\|^2 + 2\sigma_{\max}(P_i^a) \|\zeta_i\| \|\bar{\Delta}_i\|$. Based on the LaSalle's invariance principle, ζ_i is bounded by $\frac{2\sigma_{\max}(P_i^a)\|\bar{\Delta}_i\|}{\sigma_{\min}(Q_i^a)}$. Hence, ζ_i and ψ_i are UUB. Since $\psi_i = [\ \theta_i{}^T \quad \varpi_i{}^T \quad \tilde{\delta}_i^T\ ]^T$, we obtain that ϖ_i is UUB. That is, condition (ii) in Theorem 1 holds by designing the gain matrices as (31) and (35). Noting that

$$\tilde{y}_i = C_i(x_i - \hat{x}_i) = C_i(\theta_i - \tilde{\delta}_i) = C_i^a \psi_i, \tag{61}$$

we obtain that $\tilde{y}_i$ is also UUB. This completes the proof. ■

IV. Simulation Results

To show system resilience to sensor faults and malicious attacks, we apply the proposed control protocols to the output containment problem of heterogeneous multi-group systems, consisting of three leaders, six followers, and three adversaries, with the communication digraph $\mathscr{G}$ depicted in Fig. 2. The leaders' dynamics for agents $k = 7, 8, 9$, the followers' dynamics for agents $i = 1, 2, ..., 6$, and the adversaries' dynamics for agents $l = 10, 11, 12$ are described by $S = \begin{bmatrix} 1 & -3 \\ 2 & -1 \end{bmatrix}$, $R = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $A_{1,4} = \begin{bmatrix} 3 & -2 \\ 1 & -2 \end{bmatrix}$, $B_{1,4} = \begin{bmatrix} 1.8 & -1 \\ 2 & 3 \end{bmatrix}$, $C_{1,4} = \begin{bmatrix} -1 & 2 \\ 4 & -3 \end{bmatrix}$, $A_{2,5} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & -2 \end{bmatrix}$,

$B_{2,5} = \begin{bmatrix} 6 & 0 \\ 0 & 1 \\ 1 & 0 \end{bmatrix}$, $C_{2,5} = \begin{bmatrix} 1 & -1 & 1 \\ -1 & -1 & 1 \end{bmatrix}$, $A_{3,6} = \begin{bmatrix} 0 & -1 \\ 1 & -2 \end{bmatrix}$, $B_{3,6} \begin{bmatrix} 1 & -2 \\ 3 & 4 \end{bmatrix}$, $C_{3,6} = \begin{bmatrix} -2 & 1 \\ 3 & -2 \end{bmatrix}$, $M_{7,8,9} = \begin{bmatrix} 1 & -1 \\ 3 & -1 \end{bmatrix}$, $C_{7,8,9} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. The sensor fault δ_i is introduced for each follower by selecting $\delta_1 = \begin{bmatrix} 0.3\sin(t) \\ 0.3\sin(t) \end{bmatrix}$, $\delta_2 = \begin{bmatrix} -0.6\sin(t) \\ -0.6\sin(t) \\ -0.6\sin(t) \end{bmatrix}$, $\delta_3 = \begin{bmatrix} 0.9\sin(t) \\ 0.9\sin(t) \end{bmatrix}$, $\delta_4 = \begin{bmatrix} -0.3\cos(t) \\ -0.3\cos(t) \end{bmatrix}$, $\delta_5 = \begin{bmatrix} 0.6\cos(t) \\ 0.6\cos(t) \\ 0.6\cos(t) \end{bmatrix}$, $\delta_6 = \begin{bmatrix} -0.9\cos(t) \\ -0.9\cos(t) \end{bmatrix}$.

We construct the resilient control protocols for each follower, consisting of (6), (7), and (17) to (20). Based on Lemma 5, we design $F_i = S$ and $G_i = \begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix}$ for each follower. For the communication digraph of the observers, based on (21), pick $\mathcal{A} = [0\ 0\ 0\ 0\ 0\ 0.5; 0.5\ 0\ 0\ 0\ 0\ 0; 0\ 0.5\ 0\ 0.5\ 0\ 0; 0\ 0\ 0\ 0\ 1\ 0; 0\ 0\ 0\ 0\ 0\ 1; 0\ 0\ 0.5\ 0\ 0\ 0]$. Then, we obtain $\rho(\mathcal{A}) = 0.7477$. Select $\gamma_i = 1.2 < 1/\rho(\mathcal{A})$, and $\alpha_i = 0.5$ for each follower. The gain matrices K_i found by solving (35) and (36) are $K_{1,4} = \begin{bmatrix} -2.91 & 2.12 \\ 31.30 & -23.33 \end{bmatrix}$, $K_{2,5} = \begin{bmatrix} -10.36 & -8.32 & -10.73 \\ -2.68 & -15.48 & -2.75 \end{bmatrix}$, and $K_{3,6} = \begin{bmatrix} 1.48 & -5.33 \\ 22.45 & -17.98 \end{bmatrix}$. Then, by using (31), we obtain the gain matrices H_i as $H_{1,4} = \begin{bmatrix} 0.83 & -0.83 \\ 0.10 & -7.67 \end{bmatrix}$, $H_{2,5} = \begin{bmatrix} 1.35 & -9.94 \\ -7.64 & -7.57 \end{bmatrix}$, and $H_{3,6} = \begin{bmatrix} -18.05 & -5.59 \\ -8.04 & -14.21 \end{bmatrix}$.

The output trajectories of all the agents are presented in Fig. 3 for $t \in [0, 15]\ s$, where $y_i = [\ y_i(1)\ \ y_i(2)\ ]^T$. The convex hulls formed by the trajectories of the leaders are shown for four different instants, ($t = 0s$, $t = 5s$, $t = 10s$ and $t = 15s$), which are

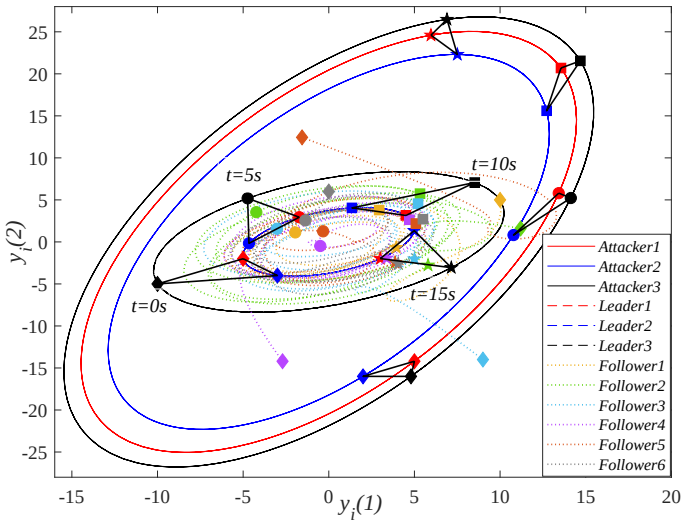

Fig. 3: The output trajectories of all the agents.

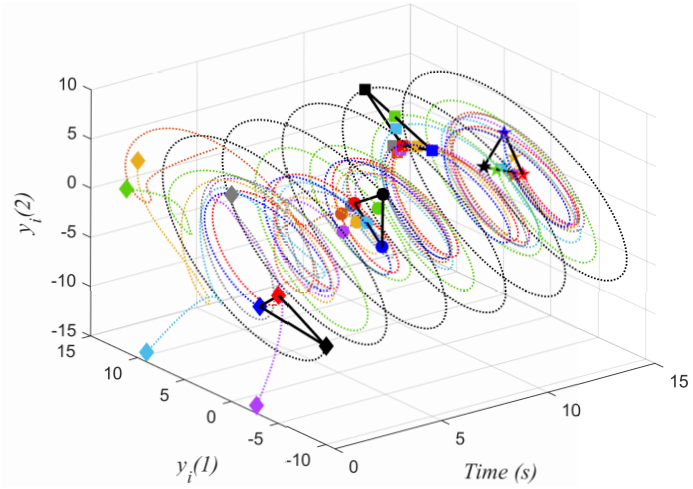

Fig. 4: The output trajectories over time for the followers and the leaders.

denoted by ♢, ◯, □, and ★, respectively. It is seen that, despite the output injections of the adversarial agents moving on the outside circles, the trajectory of each follower stays in a small neighborhood around the dynamic convex hull spanned by the leaders. That is, the UUB output containment is achieved, in the presence of sensor faults and the attacks from the adversaries. Fig. 4 shows the output trajectories over time for the followers and the leaders.

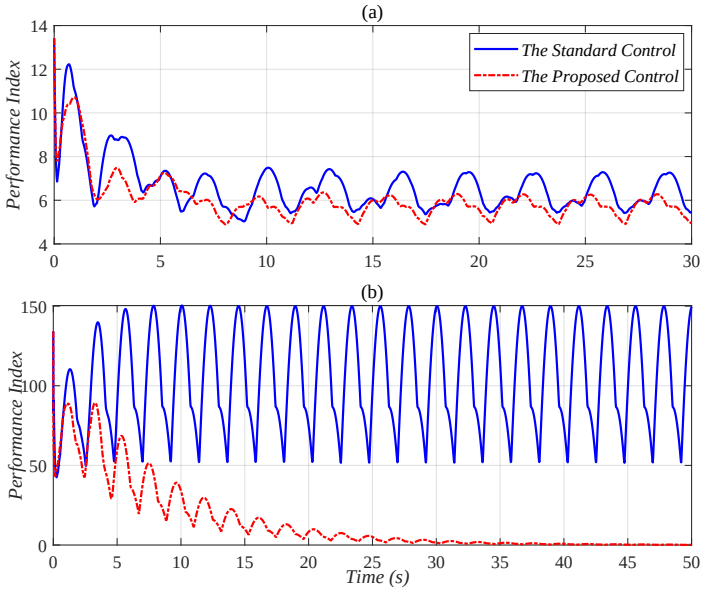

Fig. 5: Performance index comparison between the standard and the proposed approaches for two case scenarios: (a) sensor faults; (b) adversaries' attacks.

In order to show the resilient performance of the proposed approach, we compare our method with the standard approach, i.e., (6) and (7) without the compensational term $\hat{d}_i$. To obtain a clear performance index, we remove the leaders 8 and 9 from $\mathscr{G}$ to construct a output tracking problem. The performance index is set as $\sum_{i=1}^{6} |y_i(1) - y_7(1)| + |y_i(2) - y_7(2)|$, which is the sum of the absolute values of the tracking error entries of each follower. The performance index comparisons between the standard and the proposed resilient approaches are simulated for the cases of sensor faults and adversaries' attacks, respectively, as illustrated in Fig. 5. It is shown that, compared to the standard approach, the proposed control method assures better resilience for both scenarios of sensor faults and adversaries' attacks. Moreover, the tracking error performance index goes to almost zero using the proposed approach under adversaries' attacks. This shows that the proposed approach has strong resilience in the complex distributed settings.

V. Conclusion

In this technical note, we have introduced a new concept of cooperative and adversarial multi-group system. This heterogeneous networked system consists of leaders, followers, and adversaries. To maintain stability of the overall system and achieve the resilient output containment control objective, we have presented a novel control framework resilient to both sensor faults and malicious attacks from the adversaries. Explicit local sufficient conditions and design procedures have been obtained. The effectiveness of the proposed control protocols has been verified by the simulated case studies.

References

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

[2] W. Ren, R. W. Beard, and E. M. Atkins, "Information consensus in multivehicle cooperative control," *IEEE Control syst. mag.*, vol. 2, no. 27, pp. 71–82, 2007.

[3] F. L. Lewis, H. Zhang, K. Hengster-Movric, and A. Das, *Cooperative control of multi-agent systems: optimal and adaptive design approaches*. London, U.K.: Springer-Verlag, 2014.

[4] S. Zuo, Y. Song, H. Modares, F. L. Lewis, and A. Davoudi, "A unified approach to output synchronization of heterogeneous multi-agent systems via $\mathcal{L}_2$-gain design," *Control Theory Technol.*, vol. 15, no. 4, pp. 340–353, Nov. 2017.

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

[6] S. Zuo, A. Davoudi, Y. Song, and F. L. Lewis, "Distributed finite-time voltage and frequency restoration in islanded ac microgrids," *IEEE Trans. Ind. Electron.*, vol. 63, no. 10, pp. 5988–5997, Jun. 2016.

[7] W. Ren and N. Sorensen, "Distributed coordination architecture for multi-robot formation control," *Robot. Auton. Syst.*, vol. 56, no. 4, pp. 324–333, Apr. 2008.

[8] J. Huang, *Nonlinear output regulation: theory and applications*. Philadelphia, PA, USA: SIAM, 2004.

[9] S. Zuo, Y. Song, F. L. Lewis, and A. Davoudi, "Adaptive output containment control of heterogeneous multi-agent systems with unknown leaders," *Automatica*, vol. 92, pp. 235–239, Jun. 2018.

[10] S. Gorman, "Electricity grid in us penetrated by spies," *The Wall Street J.*, vol. 8, Apr. 2009.

[11] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 645–658, Dec. 2011.

[12] 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.

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

[14] S. Sundaram and C. N. Hadjicostis, "Distributed function calculation via linear iterative strategies in the presence of malicious agents," *IEEE Trans. Autom. Control*, vol. 56, no. 7, pp. 1495–1508, Jul. 2011.

[15] M. Zhu and S. Martínez, "On the performance analysis of resilient networked control systems under replay attacks," *IEEE Trans. Autom. Control*, vol. 59, no. 3, pp. 804–808, Mar. 2014.

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

[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, Jun. 2014.

[18] S. M. Dibaji and H. Ishii, "Resilient consensus of double-integrator multi-agent systems," in *American Control Conference*, 2014, pp. 5139–5144.

[19] H. J. LeBlanc, H. Zhang, S. Sundaram, and X. Koutsoukos, "Resilient continuous-time consensus in fractional robust networks," in *American Control Conference*, 2013, pp. 1237–1242.

[20] E. Arabi, T. Yucelen, and W. M. Haddad, "Mitigating the effects of sensor uncertainties in networked multi-agent systems," *J. Dyn. Syst. Meas. Control*, vol. 139, no. 4, p. 041003, Feb. 2017.

[21] G. De La Torre, T. Yucelen, and J. D. Peterson, "Resilient networked multiagent systems: A distributed adaptive control approachy," in *Proc. 53rd IEEE Conf. Decision and Control*, 2014, pp. 5367–5372.

[22] C.-H. Xie and G.-H. Yang, "Decentralized adaptive fault-tolerant control for large-scale systems with external disturbances and actuator faults," *Automatica*, vol. 85, pp. 83–90, Nov. 2017.

[23] X. Jin, W. M. Haddad, and T. Yucelen, "An adaptive control architecture for mitigating sensor and actuator attacks in cyber-physical systems," *IEEE Trans. Autom. Control*, vol. 62, no. 11, pp. 6058–6064, Nov. 2017.

[24] H. Modares, R. Moghadam, F. L. Lewis, and A. Davoudi, "Static output-feedback synchronisation of multi-agent systems: a secure and unified approach," *IET Control Theory Appl.*, vol. 12, no. 8, pp. 1095–1106, May 2018.

[25] E. A. Anderson, C. E. Irvine, and R. R. Schell, "Subversion as a threat in information warfare," *Journal of Information Warfare*, vol. 3, no. 2, pp. 51-64, 2004.

[26] H. Haghshenas, M. A. Badamchizadeh, and M. Baradarannia, "Containment control of heterogeneous linear multi-agent systems," *Automatica*, vol. 54, pp. 210–216, Apr. 2015.

[27] S. Zuo, Y. Song, F. L. Lewis, and A. Davoudi, "Output containment control of linear heterogeneous multi-agent systems using internal model principle," *IEEE Trans. Cybern.*, vol. 47, no. 8, pp. 2099–2109, Aug. 2017.

[28] H. Chu, L. Gao, and W. Zhang, "Distributed adaptive containment control of heterogeneous linear multi-agent

systems: an output regulation approach," *IET Control Theory & Applications*, vol. 10, no. 1, pp. 95–102, Dec. 2016.

[29] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "Distributed fault detection and isolation resilient to network model uncertainties," *IEEE Trans. Cybern.*, vol. 44, no. 11, pp. 2024–2037, Nov. 2014.

[30] Y. L. Wang, P. Shi, C. C. Lim, and Y. Liu, "Event-triggered fault detection filter design for a continuous-time networked control system," *IEEE Trans. Cybern.*, vol. 46, no. 12, pp. 3414-3426, Dec. 2016.

[31] O. A. Beg, T. T. Johnson, and A. Davoudi, "Detection of false-data injection attacks in cyber-physical dc microgrids," *IEEE Trans. Ind. Informatics*, vol. 13, no. 5, pp. 2693-2703, Oct. 2017.

[32] R. T. Rockafellar, *Convex analysis*. Princeton university press, 2015.

[33] H. K. Khalil, *Nonlinear systems*. Upper Saddle River, NJ: Prentice Hall, 3rd edition, 2002.

[34] K. Zhou, J. C. Doyle, K. Glover *et al.*, *Robust and optimal control*. Upper Saddle River, NJ: Prentice Hall, 1996.

[35] J. Gadewadikar, F. L. Lewis, and M. Abu-Khalaf, "Necessary and sufficient conditions for h-infinity static output-feedback control," *J. Guid. Control Dyn.*, vol. 29, no. 4, pp. 915–920, Jul. 2006.

CHAPTER 3

RESILIENT NETWORKED AC MICROGRIDS UNDER UNBOUNDED CYBER ATTACKS[1]

Authors: Shan Zuo, Omar Ali Beg, Frank L. Lewis, and Ali Davoudi.

Reprinted, with permission from all the co-authors.

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

DOI: 10.1109/TSG.2020.2984266

Resilient Networked AC Microgrids Under Unbounded Cyber Attacks

Shan Zuo, Omar Ali Beg, *Member, IEEE*, Frank L. Lewis, *Life Fellow, IEEE*, and Ali Davoudi, *Senior Member, IEEE*

Abstract

This paper considers a cooperative and adversarial AC microgrid system consisting of cooperative leaders and inverters, as well as adversarial attackers. The attackers aim to destabilize the synchronization dynamics of the AC microgrid by first intercepting the communication channels, penetrating the local state feedback, and pretending to be a cooperative neighbor, and then initiating malicious attacks by launching unbounded injections. A fully distributed resilient control framework is offered for the secondary frequency regulation and voltage containment to ensure system stability and preserve bounded synchronization. In particular, a virtual resilient layer with hidden networks is developed to integrate with the original cyber-physical layer. The proposed resilient control framework is fully distributed without requiring any global information. A modified IEEE 34-bus test feeder benchmark system is emulated in a controller/hardware-in-the-loop environment, where the control objectives are met under different attack scenarios.

Index Terms

This work was supported by the ONR grant N00014-17-1-2239. O. A. Beg was supported by the University of Texas at Arlington.

S. Zuo, F. L. Lewis, and A. Davoudi are with the Electrical Engineering Department, The University of Texas, Arlington, TX 76019, USA (e-mail: shan.zuo@uta.edu; lewis@uta.edu; davoudi@uta.edu). O. A. Beg is with the Electrical Engineering Department, the University of Texas Permian Basin, Odessa, TX 79762, USA. He was with the University of Texas at Arlington, Arlington, TX 76019, USA (e-mail: beg_o@utpb.edu).

AC microgrids, containment, inverters, synchronization, resilient control, unbounded attacks.

I. Introduction

Microgrids are evolving into cyber-physical systems with the large-volume adaptation of power electronic devices, sophisticated software-intensive controllers, and communication networks. Analogous to the case of the legacy grid where embedded intelligence made it vulnerable to cyber attacks, the presence of software-based controllers or communication networks in microgrids makes them susceptible to cyber compromises [1]–[7]. The impacts are more pronounced in inverter-based microgrids due to their lack of generational inertia, presence of a weak distribution grid, and often volatile and dynamic source and load profiles. Distributed cooperative control of AC microgrids [8]–[11] have emerged as an alternative to centralized control paradigms since they offer better robustness (by removing the single point-of-failure) and solution scalability. These control techniques map inverters to nodes on a sparse communication digraph, and assure that all nodes reach an agreement on quantities of interests issued by leader nodes (synchronization). In particular, consensus (synchronization with one leader) and containment (synchronization with two leaders) control protocols are used to achieve frequency regulation and voltage containment, respectively, by using the local relative information exchanged among neighboring inverters. However, their distributed nature could potentially make microgrids vulnerable to malicious attacks and infiltration, since each inverter only has access to its local data and neighbors partial data, missing a global perspective.

There are generally two main approaches to address cyber attacks in power grids. The first group of techniques [12]–[19], first detect and identify the compromised agents, and then correct or simply isolate them. Attack-correction methods usually have strict restrictions on the number of misbehaving agents. For example, it is shown in [20],

[21] that it is impractical to restore the system state if more than half of the sensors have been affected. On the other hand, simply isolating the corrupted agents may potentially compromise the connectivity and performance of the sparse communication network. Sufficient and necessary conditions for undetectable or unidentifiable attacks are well discussed in the literature. It is shown in [3], [22]–[24] that the attackers can take advantage of the configuration of the power systems to launch malicious attacks to bypass the existing attack detection methods. The conditions for the existence of undetectable attacks and fundamental limitations of various attack detection and identification monitors are analyzed in [25]. Distributed filters are proposed to detect and identify attacks. However, these filters are computationally expensive and are difficult to implement. Moreover, one could manipulate the good data to be inadvertently removed [26]. Since one could not list and remove every potential threat, the concept of attack-resilience is proposed. Hence, the second solution category develops distributed attack-resilient control protocols to enhance the resilience of the microgrids against potential noises/faults, without the need to detect, identify and correct/remove misbehaving agents [27], [28]. These unintentional noises/faults have been assumed to be bounded signals, and have been collectively addressed in the context of conventional fault-tolerant control [29]. Direct adaptation to adversarial attacks is not practical as such attacks are intentionally designed to maximize their damage and, hence, cannot be assumed bounded [21]. Some approaches assume a certain probabilistic model of an attack [30], which could be limiting since attack nature and form might not be known a priori. To the best of our knowledge, general unbounded cyber attacks on microgrids have neither been systematically studied nor have been addressed using a distributed resilient control framework.

We consider a networked multi-group AC microgrid consisting of cooperative leader nodes and inverters, as well as adversarial attackers as illustrated in Fig. 1. In particular,

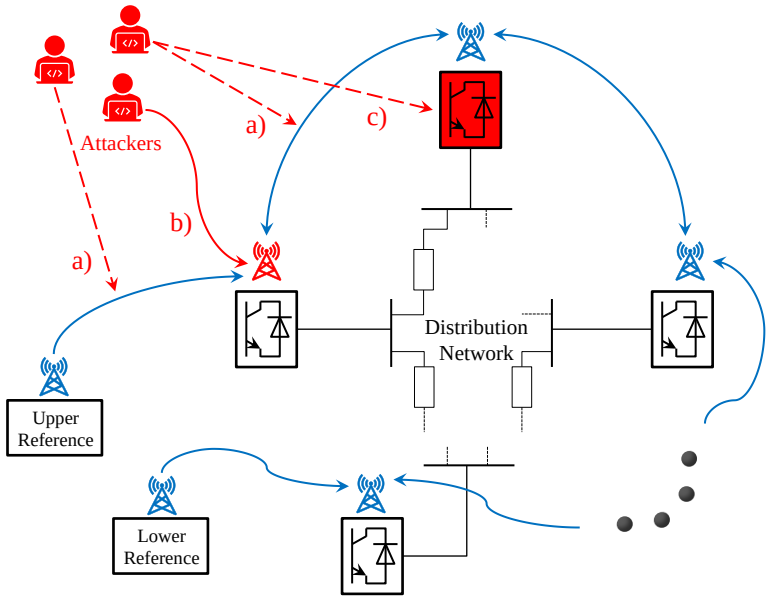

Fig. 1: A networked AC microgrid under different types of cyber attacks: a) polluting the communication channels; b) hijacking neighbor's signals, or pretending to be a cooperative neighbor; c) distorting the local state-feedback of an inverter.

we study three different attack categories. First, the attackers can affect the signals on the communication channels among the leader nodes and the inverters. Second, the attackers can hijack the neighboring inverter or pretend to be a cooperative neighbor and issue relative information/data to local inverter. Third, attackers can launch injections to the local state-feedback of each inverter. These attack injections may be in any form, and even unbounded. These could destabilize the synchronization mechanism, and demand a distributed attack-resilient control framework to assure that the uniformly ultimately bounded (UUB) voltage containment and frequency regulation of each inverter is maintained. In that regard, the salient contributions of this paper are:

• Containment-based control approach is proposed to contain all voltage magnitudes in a prescribed range. In particular, we consider a sparse communication topology among inverters with two leader nodes with their references setting the prescribed voltage boundaries. Identical frequency reference is assigned to both leaders to achieve

regulation on frequency terms. This is in contrast to the existing literature on cooperative control of AC microgrids, which mainly focuses on the voltage tracking strategy [9], [31] or regulating the average value of voltage magnitudes [32]–[34].

• A cooperative and adversarial networked AC microgrid is introduced with cooperative leaders and inverters, as well as adversarial attackers. In particular, we consider different types of unbounded attacks on the communication links among inverters and/or leaders, on the direct relative information exchanged among inverters, and on the local state-feedback of an inverter.

• Resilient containment/consensus-based voltage/frequency synchronization solutions are provided in the presence of unbounded attacks to guarantee the UUB synchronization performance and maintain the the overall system stability, without requiring any global information. In particular, a virtual resilient control layer, with hidden networks, interconnects with the original cyber-physical layer.

The rest of this paper is organized as follows: Section II presents notations and the preliminaries of graph theory. Section III reviews the standard cooperative control of AC microgrids. Section IV incorporates the unbounded cyber attacks and formulates the resilient synchronization problems of AC microgrids. Section V presents the fully distributed attack-resilient control framework for AC microgrids. The proposed method is studied in Section VI in a controller/hardware-in-the-loop (CHIL) environment for the attack scenarios illustrated in Fig. 1. Section VII concludes the paper.

II. Notations and Preliminaries

Notations: $I_N \in \mathbb{R}^{N\times N}$ denotes the identity matrix. $\mathbf{1}_N \in \mathbb{R}^N$ represents a vector where all entries are one. The operator $\mathrm{diag}\{\cdot\}$ establishes a block-diagonal matrix using its elements. $\otimes$ denotes the Kronecker product. $\sigma_{\min}(X)$ and $\sigma_{\max}(X)$ are the minimum and maximum singular values of matrix X.

Preliminaries: A cooperative and adversarial islanded AC microgrid system is mapped on a time-invariant communication digraph $\mathscr{G}$, composed of N inverters, two leader nodes, and some adversarial nodes (attackers). Each inverter receives direct relative information from inverters neighboring it on the communication digraph, including the cooperative inverters and leaders, as well as the adversarial attackers. The two leader nodes issue the upper and lower reference values to the inverters, and are called the upper and lower leaders, respectively. The sets of the inverters and the attackers are shown by $\mathscr{F}$ and $\mathscr{A}$, respectively.

The connections among the local inverters are shown by $\mathscr{G}_f = (\mathcal{W}, \mathcal{E}, \mathcal{A})$, where $\mathcal{W}$ shows the set of nodes, $\mathcal{E} \subset \mathcal{W} \times \mathcal{W}$ shows the set of edges, and $\mathcal{A} = [a_{ij}]$ shows the associated adjacency matrix. $\mathscr{G}_f$ is a subgraph of $\mathscr{G}$. An edge connecting node j to node i is shown by (w_j, w_i), indicating the information flow from inverter j to inverter i. a_{ij} shows the edge weight (w_j, w_i), and $a_{ij} > 0$ if $(w_j, w_i) \in \mathcal{E}$; Otherwise, $a_{ij} = 0$. The in-degree matrix is $\mathcal{D} = \text{diag}(d_i) \in \mathbb{R}^{N \times N}$, with $d_i = \sum_{j=1}^{N} a_{ij}$. The Laplacian matrix is $\mathcal{L} = \mathcal{D} - \mathcal{A}$. $\{(w_i, w_k), (w_k, w_l), \ldots, (w_m, w_j)\}$ denotes a directed path from inverter i to inverter j. g_i^u and g_i^l are pinning gains from the upper and lower leaders to the i^{th} inverter, respectively. $g_i^u > 0$ (respectively, $g_i^l > 0$) if there exists a link from the upper leader (respectively, lower leader) to the i^{th} inverter; Otherwise, $g_i^u = 0$ (respectively, $g_i^l = 0$). $\mathcal{G}_u = \text{diag}\left(g_i^u\right)$ and $\mathcal{G}_l = \text{diag}\left(g_i^l\right), \forall i \in \mathscr{F}$ are diagonal matrices of pinning gains from the upper and lower leaders, respectively. h_{ik} is the pinning gain from the k^{th} attacker to the i^{th} inverter. $h_{ik} > 0$ if there exists a connection between the k^{th} attacker and the i^{th} inverter; Otherwise, one has $h_{ik} = 0$.

III. Standard Cooperative Secondary Control of AC Microgrids

One can adopt the nonlinear large-signal model of an inverter [35] that ignores the switching artifacts and focuses on its average-value model. Assuming inductive

distribution lines, the active and reactive powers delivered by the i^{th} inverter at the i^{th} bus of the distribution network are

$$\begin{cases} P_i = \frac{v_{\mathrm{mag},i} v_{\mathrm{bus},i} \sin(\theta_i - \beta_i)}{Z_i}, \\ Q_i = \frac{v_{\mathrm{mag},i} v_{\mathrm{bus},i} \cos(\theta_i - \beta_i)}{Z_i} - \frac{v_{\mathrm{bus},i}^2}{Z_i}, \end{cases} \tag{1}$$

where Z_i shows the effective collective impedance of the inverter's output filter and the connector between the inverter and the distribution network. P_i and Q_i are the active and reactive output powers of the i^{th} inverter, respectively. $v_{\mathrm{mag},i} \angle \theta_i$ is the output voltage of the i^{th} inverter and $v_{\mathrm{bus},i} \angle \beta_i$ is the i^{th} bus voltage. Relation (1) can be simplified to obtain droop mechanisms for (P_i, ω_i) and (Q_i, v_i) and tune the inverter's frequency and voltage

$$\omega_i = \omega_{n_i} - m_{P_i} P_i, \tag{2}$$

$$v_{\mathrm{mag},i} = V_{n_i} - n_{Q_i} Q_i, \tag{3}$$

where ω_i is the angular frequency of the i^{th} inverter. Tuning $v_{\mathrm{mag},i}$ is effectively the same as tuning the direct term of the output voltage, v_{odi}, after a proper reference frame transformation. ω_{n_i} and V_{n_i} are the set points for the droop mechanism, and are chosen at the secondary level. m_{P_i} and n_{Q_i} are droop coefficients chosen according to the power rating of the corresponding inverter.

To coordinate inverters' terminal frequency and voltage to their respective references, the secondary control provides ω_{ni} and V_{ni} locally by data exchange with its neighbors on a communication digraph. Differentiating (2) and (3) yields

$$\dot{\omega}_{ni} = \dot{\omega}_i + m_{P_i} \dot{P}_i = u_{f_i}, \tag{4}$$

$$\dot{V}_{ni} = \dot{v}_{odi} + n_{Q_i} \dot{Q}_i = u_{v_i}, \tag{5}$$

where u_{f_i} and u_{v_i} are auxiliary control inputs.

The frequency and voltage control of N inverters can then be represented by synchronization problems for the following linear and first-order multi-agent systems (MAS)

$$\begin{cases} \dot{\omega}_1 + m_{P_1}\dot{P}_1 = u_{f_1}, \\ \vdots \\ \dot{\omega}_N + m_{P_N}\dot{P}_N = u_{f_N}, \end{cases} \tag{6}$$

$$\begin{cases} \dot{v}_{od1} + n_{Q_1}\dot{Q}_1 = u_{v_1}, \\ \vdots \\ \dot{v}_{odN} + n_{Q_N}\dot{Q}_N = u_{v_N}. \end{cases} \tag{7}$$

Motivated by [36], with a slight modification of [37], the cooperative frequency and voltage control laws at each inverter, based on the neighbors' information and the information of the leader nodes, are

$$\begin{aligned} u_{f_i} = c_{fi} \Bigg(& \sum_{j=1}^{N} a_{ij} \left(\omega_j - \omega_i\right) + g_i^u \left(\omega_{\text{ref}} - \omega_i\right) \\ & + g_i^l \left(\omega_{\text{ref}} - \omega_i\right) + \sum_{j=1}^{N} a_{ij} \left(m_{P_j} P_j - m_{P_i} P_i\right) \Bigg), \end{aligned} \tag{8}$$

$$\begin{aligned} u_{v_i} = c_{vi} \Bigg(& \sum_{j=1}^{N} a_{ij} \left(v_{odj} - v_{odi}\right) + g_i^u \left(v_{\text{ref}}^u - v_{odi}\right) \\ & + g_i^l \left(v_{\text{ref}}^l - v_{odi}\right) + \sum_{j=1}^{N} a_{ij} \left(n_{Q_j} Q_j - n_{Q_i} Q_i\right) \Bigg), \end{aligned} \tag{9}$$

where $c_{fi}, c_{vi} \in \mathbb{R} > 0$ are the coupling gains, ω_{ref} is the frequency reference, and v_{ref}^u and v_{ref}^l are the bounds on voltage terms, respectively.

It is worth noting that to regulate frequency, its reference values for both the upper and lower leaders are set as ω_{ref}. On the other hand, to bound the voltage magnitudes to a prescribed range, the voltage references for the upper and lower leaders are set as v_{ref}^u

and v^l_{ref}, respectively. That is, we try to achieve consensus-based and containment-based regulations for frequency and voltage terms, respectively.

The droop set points, ω_{ni} and V_{ni}, are then computed from u_{f_i} and u_{v_i} as

$$\omega_{n_i} = \int u_{f_i} \, \mathrm{d}\, t, \tag{10}$$

$$V_{n_i} = \int u_{v_i} \, \mathrm{d}\, t. \tag{11}$$

Based on (2) and (3), we reformulate (8) and (9) as

$$\begin{aligned} u_{f_i} = c_{fi} \Bigg(& \sum_{j \in \mathscr{F}} a_{ij} \left(\left(\omega_j + m_{P_j} P_j \right) - \left(\omega_i + m_{P_i} P_i \right) \right) \\ & + g^u_i \left(\left(\omega_{\text{ref}} + m_{P_i} P_i \right) - \left(\omega_i + m_{P_i} P_i \right) \right) + \\ & g^l_i \left(\left(\omega_{\text{ref}} + m_{P_i} P_i \right) - \left(\omega_i + m_{P_i} P_i \right) \right) \Big) \\ = c_{fi} \Bigg(& \sum_{j=1}^{N} a_{ij} \left(\omega_{n_j} - \omega_{n_i} \right) + g^u_i \left(\omega_{n,\text{ref}} - \omega_{n_i} \right) + g^l_i \left(\omega_{n,\text{ref}} - \omega_{n_i} \right) \Bigg), \end{aligned} \tag{12}$$

$$\begin{aligned} u_{v_i} = c_{vi} \Bigg(& \sum_{j=1}^{N} a_{ij} \left(\left(v_{odj} + n_{Q_j} Q_j \right) - \left(v_{odi} + n_{Q_i} Q_i \right) \right) \\ & + g^u_i \left(\left(v^u_{\text{ref}} + n_{Q_i} Q_i \right) - \left(v_{odi} + n_{Q_i} Q_i \right) \right) + \\ & g^l_i \left(\left(v^l_{\text{ref}} + n_{Q_i} Q_i \right) - \left(v_{odi} + n_{Q_i} Q_i \right) \right) \Big) \\ = c_{vi} \Bigg(& \sum_{j=1}^{N} a_{ij} \left(V_{n_j} - V_{n_i} \right) + g^u_i \left(V^u_{n,\text{ref}} - V_{n_i} \right) + g^l_i \left(V^l_{n,\text{ref}} - V_{n_i} \right) \Bigg), \end{aligned} \tag{13}$$

where $\omega_{n,\text{ref}} = \omega_{\text{ref}} + m_{P_i} P_i$, $V^u_{n,\text{ref}} = v^u_{\text{ref}} + n_{Q_i} Q_i$, and $V^l_{n,\text{ref}} = v^l_{\text{ref}} + n_{Q_i} Q_i$. While power sharing mechanisms are included in the control protocols (12) and (13), [9] shows that the frequency and voltage of each inverter synchronize in the steady state, because of the relationship between the active power of each inverter (respectively, reactive power) and its angular frequency (respectively, voltage magnitude). That is, to synchronize both ω_i and $m_{P_i} P_i$ (respectively, v_{odi} and $n_{Q_i} Q_i$), we can directly synchronize ω_{n_i}

(respectively, V_{n_i}). To this end, combine (4) with (12) and (5) with (13) to obtain

$$\dot{\omega}_{n_i} = c_{fi}\left(\sum_{j=1}^{N} a_{ij}\left(\omega_{n_j} - \omega_{n_i}\right) + g_i^u\left(\omega_{n,\mathrm{ref}} - \omega_{n_i}\right) + g_i^l\left(\omega_{n,\mathrm{ref}} - \omega_{n_i}\right)\right), \tag{14}$$

$$\dot{V}_{n_i} = c_{vi}\left(\sum_{j=1}^{N} a_{ij}\left(V_{n_j} - V_{n_i}\right) + g_i^u\left(V_{n,\mathrm{ref}}^u - V_{n_i}\right) + g_i^l\left(V_{n,\mathrm{ref}}^l - V_{n_i}\right)\right). \tag{15}$$

IV. Attack Modeling and Problem Formulation

We first introduce unbounded cyber attacks, and then formulate the secondary resilient synchronization problems for networked AC microgrids in the presence of unknown unbounded attacks.

A. Modeling of Unbounded Attacks

Herein, we only consider the attack modeling and stability analysis of the secondary voltage control. This procedure can be extended to the secondary frequency control.

The following definition is needed to introduce the unbounded attacks and to evaluate the convergence of the resilient control protocols to be proposed.

***Definition* 1:** The signal $x(t)$ is said to be

(i) bounded if $\exists\ \varepsilon > 0$, such that

$$\|x(t)\| < \varepsilon, \quad \forall t \geq t_0 \geq 0. \tag{16}$$

(ii) unbounded if it is not bounded.

(iii) ([38]) UUB with ultimate bound b if there exist positive constants b and c, independent of $t_0 \geq 0$, and for every $a \in (0, c)$, there is $T = T(a, b) \geq 0$, independent of t_0, such that

$$\|x(t_0)\| \leq a \quad \Rightarrow \quad \|x(t)\| \leq b, \quad \forall t \geq t_0 + T. \tag{17}$$

For convenience, we use V_i to denote V_{n_i}. Then, (15) under attacks becomes

$$\begin{aligned}\dot{V}_i = c_{vi}\Bigg(&\sum_{j=1}^{N} a_{ij}\left(\bar{V}_{i,j} - \bar{V}_{i,i}\right) + g_i^u\left(\bar{V}_{i,\mathrm{ref}}^u - \bar{V}_{i,i}\right)\\ &+ g_i^l\left(\bar{V}_{i,\mathrm{ref}}^l - \bar{V}_{i,i}\right) + \sum_{k\in\mathscr{A}} h_{ik}\left(V_k - \bar{V}_{i,i}\right),\end{aligned} \tag{18}$$

where V_k is the state information of the k^{th} attacker. Note that the attackers can have any linear/nonlinear dynamical systems. $\bar{V}_{i,j}$, $\bar{V}_{i,\mathrm{ref}}^u$, and $\bar{V}_{i,\mathrm{ref}}^l$ denote the corrupted transmitted measurements of V_j, V_{ref}^u, and V_{ref}^l at the i^{th} inverter, respectively. $\bar{V}_{i,i}$ denotes the corrupted feedback measurement of V_i. These potentially corrupted measurements can be expressed as

$$\begin{cases}\bar{V}_{i,j}(t) = V_j(t) + \sigma_{ij}(t),\\ \bar{V}_{i,\mathrm{ref}}^u(t) = V_{\mathrm{ref}}^u(t) + \sigma_{i\,\mathrm{ref}}^u(t),\\ \bar{V}_{i,\mathrm{ref}}^l(t) = V_{\mathrm{ref}}^l(t) + \sigma_{i\,\mathrm{ref}}^l(t),\\ \bar{V}_{i,i}(t) = V_i(t) + \sigma_{ii}(t),\end{cases} \tag{19}$$

where $\sigma_{ij}(t)$, $\sigma_{i\,\mathrm{ref}}^u(t)$, $\sigma_{i\,\mathrm{ref}}^l(t)$, and $\sigma_{ii}(t)$ denote injections launched by the attackers. It is seen that the attackers can pretend to be cooperative neighbors and issue direct relative information to local inverters as shown in $\sum_{k\in\mathscr{A}} h_{ik}\left(V_k - \bar{V}_{i,i}\right)$ in (18), intercept the communication channels among inverters and leaders as shown in $\sigma_{ij}(t)$, $\sigma_{i\,\mathrm{ref}}^u(t)$, and $\sigma_{i\,\mathrm{ref}}^l(t)$ in (19), and distort local feedback of an inverter as shown in $\sigma_{ii}(t)$ in (19).

***Remark* 1:** In practice, AC microgrids may be compromised at the controller level, communication network, and the physical power network. Given the existence of undetectable attacks [3], this paper aims to develop fully distributed resilient control protocols to mitigate the adverse effects caused by the unbounded attack injections described in (18) and (19), without any detection and elimination process.

Without loss of generality, we consider the following assumptions.

***Assumption* 1:** There exists a directed path from at least one voltage leader to each

local inverter.

***Assumption* 2:** $\dot{V}_k$, $\dot{\sigma}_{ij}$, $\dot{\sigma}^u_{i\,\mathrm{ref}}$, $\dot{\sigma}^l_{i\,\mathrm{ref}}$, and $\dot{\sigma}_{ii}$ are bounded.

***Remark* 2:** Assumption 1 is standard for cooperative control of networked MAS to guarantee the network-level synchronization performance. In a practical setting, the attackers may have limited budgets to launch injections to the microgrid. Hence, we suppose Assumption 2 holds. Yet, the attackers' injection values, V_k, σ_{ij}, $\sigma^u_{i\,\mathrm{ref}}$, and $\sigma^l_{i\,\mathrm{ref}}$ can be unbounded. This is in contrast to [27], [28] that consider bounded faults or noises.

B. Resilient Synchronization Problem Formulation

We first analyze the vulnerability of the standard (conventional) cooperative secondary control against unbounded attacks, and then formulate the resilient voltage synchronization problem. Reformulate (18) as

$$\begin{aligned}
\dot{V}_i &= c_{vi}\left(\sum_{j=1}^{N} a_{ij}\left(\bar{V}_{i,j}-\bar{V}_{i,i}\right)+g_i^u\left(\bar{V}^u_{i,\mathrm{ref}}-\bar{V}_{i,i}\right)\right.\\
&\quad\left.+g_i^l\left(\bar{V}^l_{i,\mathrm{ref}}-\bar{V}_{i,i}\right)+\sum_{k\in\mathscr{A}} h_{ik}\left(V_k-\bar{V}_{i,i}\right)\right)\\
&= c_{vi}\left(\left(g_i^u V^u_{\mathrm{ref}}+g_i^l V^l_{\mathrm{ref}}\right)-\left(\left(d_i+g_i^u+g_i^l\right)V_i-\sum_{j=1}^{N} a_{ij}V_j\right)\right.\\
&\quad+\sum_{j=1}^{N} a_{ij}\sigma_{ij}-\left(d_i+g_i^u+g_i^l+\sum_{l\in\mathcal{A}} h_{ik}\right)\sigma_{ii}\\
&\quad\left.+\left(g_i^u\sigma^u_{i\,\mathrm{ref}}+g_i^l\sigma^l_{i\,\mathrm{ref}}\right)+\sum_{k\in\mathscr{A}} h_{ik}\left(V_k-V_i\right)\right).
\end{aligned} \tag{20}$$

Denote the attack vector as $\delta_i = \sum_{j=1}^{N} a_{ij}\sigma_{ij} - \left(d_i+g_i^u+g_i^l+\sum_{l\in\mathscr{A}} h_{ik}\right)\sigma_{ii} + \left(g_i^u\sigma^u_{i\,\mathrm{ref}}+g_i^l\sigma^l_{i\,\mathrm{ref}}\right)+\sum_{k\in\mathscr{A}} h_{ik}\left(V_k-V_i\right)$. Then, (20) becomes

$$\dot{V}_i = c_{vi}\left(\left(g_i^u V^u_{\mathrm{ref}}+g_i^l V^l_{\mathrm{ref}}\right)-\left(\left(d_i+g_i^u+g_i^l\right)V_i-\sum_{j=1}^{N} a_{ij}V_j\right)+\delta_i\right). \tag{21}$$

Since V_k, σ_{ij}, $\sigma^u_{i\,\mathrm{ref}}$, and $\sigma^l_{i\,\mathrm{ref}}$ can be unbounded, δ_i can be unbounded. Therefore, the standard cooperative control (18) not only could not regulate the voltage terms, but also could not guarantee the overall system stability.

Denote $V = [V_1^T, ..., V_N^T]^T$, $c_v = \mathrm{diag}\,(c_{vi})$, and $\delta = [\delta_1^T, ..., \delta_N^T]^T$. Then, (21) has the following global form

$$\dot{V} = c_v \left(\mathcal{G}_u \left(\mathbf{1}_N \otimes V^u_{\mathrm{ref}} \right) + \mathcal{G}_l \left(\mathbf{1}_N \otimes V^l_{\mathrm{ref}} \right) - \left(\mathcal{L} + \mathcal{G}_u + \mathcal{G}_l \right) V + \delta \right). \tag{22}$$

Next, we give some preliminaries on the synchronization of MAS with multiple leaders. The distance from $x \in \mathbb{R}^n$ to the set $\mathfrak{C} \in \mathbb{R}^n$, in terms of the Euclidean norm, is defined by

$$\text{dist } (x, \mathfrak{C}) = \inf_{y \in \mathfrak{C}} \|x - y\|_2. \tag{23}$$

***Definition* 2:** The set $\mathfrak{C} \subseteq \mathbb{R}^n$ is convex when $(1-\varepsilon)\, x + \varepsilon y \in \mathfrak{C}$, for any $x, y \in \mathfrak{C}$ and any $\varepsilon \in [0, 1]$ [39]. Let $V_{\mathscr{L}} = \left\{ V^l_{\mathrm{ref}}, V^u_{\mathrm{ref}} \right\}$ be the bounds on the voltage reference values. The convex hull of $V_{\mathscr{L}}$ is defined as the minimal convex set containing $V_{\mathscr{L}}$ points, i.e., $\mathrm{Co}\,(V_{\mathscr{L}}) = \left\{ (1-\varepsilon)\, V^l_{\mathrm{ref}} + \varepsilon V^u_{\mathrm{ref}} \middle| \, \varepsilon \in [0, 1] \right\}$. Since V^l_{ref} and V^u_{ref} are both constant, $\mathrm{Co}\,(V_{\mathscr{L}}) = \left\{ \left[V^l_{\mathrm{ref}}, V^u_{\mathrm{ref}} \right] \right\}$.

The secondary voltage control aims to converge the voltage of each inverter into the convex hull spanned by the voltage references issued by the two leaders, that is

$$\lim_{t \to \infty} \mathrm{dist}(V_i(t), \mathrm{Co}(V_{\mathscr{L}}(t))) = 0, \quad \forall i \in \mathscr{F}. \tag{24}$$

In the absence of an attack, $\bar{V}_{i,i} = V_i$, $\bar{V}_{i,j} = V_j$, and $h_{ik} = 0$. Hence, $\dot{V}_i = c_{vi} \left(\sum_{j=1}^N a_{ij}(V_j - V_i) + g^u_i(V^u_{\mathrm{ref}} - V_i) + g^l_i(V^l_{\mathrm{ref}} - V_i) \right)$. Then, the synchronization with multiple leaders is guaranteed, i.e., (24) holds for each inverter. Define

$$\Theta_\gamma = \frac{1}{2}\mathcal{L} + \mathcal{G}_\gamma, \ \gamma = u, l. \tag{25}$$

Note that $\mathcal{L}\left(\mathbf{1}_N \otimes V_{\text{ref}}^{\gamma}\right) = \left(\mathcal{D} - \mathcal{A}\right)\left(\mathbf{1}_N \otimes V_{\text{ref}}^{\gamma}\right) = 0, \forall \gamma = u, l$. Then, (22) can be rewritten as

$$\begin{aligned}\dot{V} = c_v \Bigg(& \left(\frac{1}{2}\mathcal{L} + \mathcal{G}_u\right)\left(\mathbf{1}_N \otimes V_{\text{ref}}^{u}\right) + \left(\frac{1}{2}\mathcal{L} + \mathcal{G}_l\right) \times \\ & \left(\mathbf{1}_N \otimes V_{\text{ref}}^{l}\right) - \left(\frac{1}{2}\mathcal{L} + \mathcal{G}_u + \frac{1}{2}\mathcal{L} + \mathcal{G}_l\right) V + \delta \Bigg) \\ = c_v & \left(\sum_{\gamma=u,l} \Theta_\gamma \left(\mathbf{1}_N \otimes V_{\text{ref}}^{\gamma}\right) - \sum_{\gamma=u,l} \Theta_\gamma V + \delta \right).\end{aligned} \tag{26}$$

Define the following global voltage synchronization error

$$\eta_v = V - \left(\sum_{\gamma=u,l} \Theta_\gamma \right)^{-1} \sum_{\gamma=u,l} \Theta_\gamma \left(\mathbf{1}_N \otimes V_{\text{ref}}^{\gamma}\right), \tag{27}$$

where $\eta_v = [\eta_{v1}^T, ..., \eta_{vN}^T]^T$. The following lemmas are required.

***Lemma* 1 ([40]):** Given Assumption 1, $\sum_{\gamma=u,l} \Theta_\gamma$ is non-singular and positive-definite.

***Lemma* 2 ([40]):** Given Assumption 1, the objective in (24) is obtained if $\lim_{t\to\infty} \eta_v\left(t\right) = 0$.

Next, we define the resilient voltage synchronization problem in the presence of unbounded attacks.

***Definition* 3 *(Resilient Voltage Synchronization Problem)*:** Under the unbounded attacks described in (18) and (19), the resilient voltage synchronization problem designs a fully distributed control protocols u_{v_i} in (5) for each inverter using only the local measurement such that, for all initial conditions, η_v in (27) is UUB. That is, the voltage of each inverter converges to a small neighborhood around the convex hull spanned by the voltage references of the two leaders. ■

Note that the resilient frequency synchronization problem can be defined similarly, with a different control objective to make the each inverter's frequency to converge to a small neighborhood around the frequency reference.

V. Fully Distributed Resilient Design

We present a fully distributed voltage containment framework resilient to unbounded attacks, by interconnecting the original cyber-physical layer with a hidden resilient layer with secure communication networks. The security of this hidden virtual layer is guaranteed by using the advanced internet technology, e.g., software-defined networking [41], [42]. This makes it difficult and expensive for attackers to compromise. Moreover, compared to the physical states of the local inverters, the virtual states of the hidden resilient layer have no physical meaning and, hence, are less observable.

The states of the hidden resilient control later will be designed to stabilize the cooperative and adversarial AC microgrids under unknown unbounded attacks. Let's consider the following overall system

$$\begin{aligned}\dot{V}_i = c_{vi}\Bigg(&\sum_{j=1}^{N} a_{ij}\left(\bar{V}_{i,j}-\bar{V}_{i,i}\right)+g_i^u\left(\bar{V}_{i,\mathrm{ref}}^u-\bar{V}_{i,i}\right)\\ &+g_i^l\left(\bar{V}_{i,\mathrm{ref}}^l-\bar{V}_{i,i}\right)+\sum_{k\in\mathscr{A}} h_{ik}\left(V_k-\bar{V}_{i,i}\right)-\hat{\delta}_i\Bigg),\end{aligned} \tag{28}$$

$$\dot{\hat{V}}_i = c_{vi}\left(\sum_{j=1}^{N} a_{ij}\left(\hat{V}_j-\hat{V}_i\right)+g_i^u\left(V_{\mathrm{ref}}^u-\hat{V}_i\right)+g_i^l\left(V_{\mathrm{ref}}^l-\hat{V}_i\right)+\tilde{V}_i\right), \tag{29}$$

$$\dot{\hat{\delta}}_i = -c_{vi}\left(\sum_{j=1}^{N} a_{ij}\left(\tilde{V}_j-\tilde{V}_i\right)-\left(g_i^u+g_i^l\right)\tilde{V}_i\right), \tag{30}$$

where $\hat{V}_i$ is the local state of the hidden resilient layer, $\hat{\delta}_i$ is a compensational signal estimating the attack vector δ_i, and $\tilde{V}_i = V_i - \hat{V}_i$. The virtual layer with secure hidden networks computes the compensational signal $\hat{\delta}_i$ used in (28). By subtracting $\hat{\delta}_i$ from the cyber-physical layer, the adverse effects of the unknown unbounded attacks are compensated.

Figure 2 illustrates the proposed distributed resilient control framework for a networked AC microgrid. Each inverter has a DC source, a bridge, and internal control

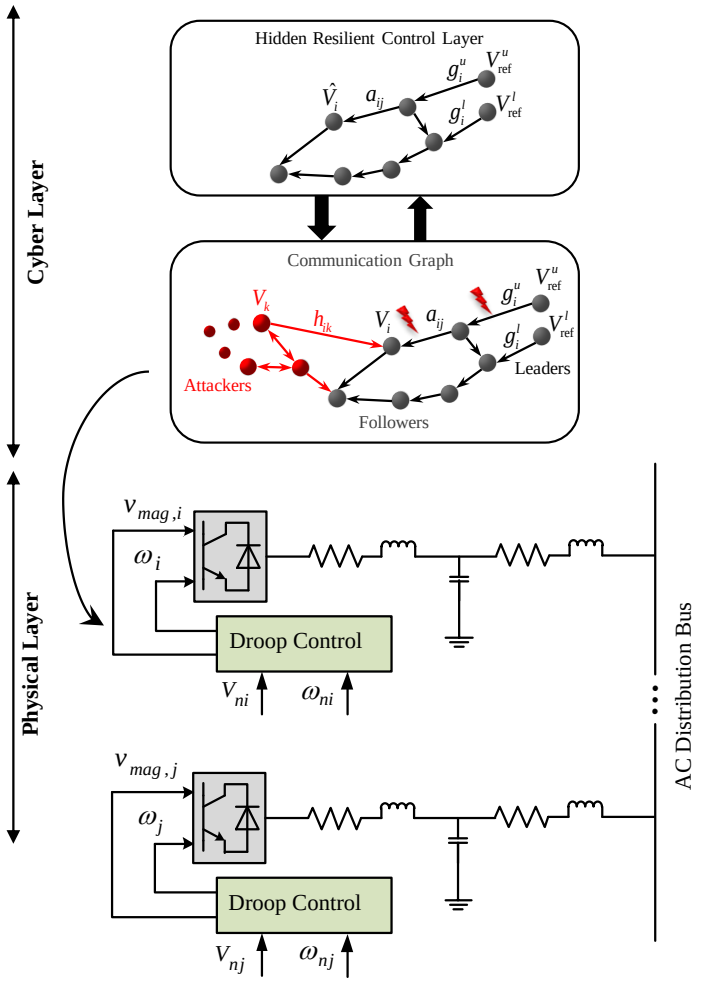

Fig. 2: Distributed resilient control framework in cooperative and adversarial networked AC microgrids.

loops for power, voltage, and current terms. On the secondary control level, a cyber layer is spanned among the inverters to exchange data/information using communication links. It is seen that the information flow on the cooperative and adversarial cyber-physical layer may be attacked. The virtual resilient control layer is shielded from the attackers and has secure communication networks.

Define the estimated global voltage synchronization error as

$$\hat{\eta}_v = \hat{V} - \left(\sum_{\gamma=u,l} \Theta_\gamma\right)^{-1} \sum_{\gamma=u,l} \Theta_\gamma \left(\mathbf{1}_N \otimes V_{\text{ref}}^\gamma\right), \tag{31}$$

where $\hat{\eta}_v = [\hat{\eta}_{v1}^T, ..., \hat{\eta}_{vN}^T]^T$ and $\hat{V} = [\hat{V}_1^T, ..., \hat{V}_N^T]^T$. Next, we analyze the resilience of these protocols against unbounded attacks.

***Theorem* 1:** Consider the unbounded attacks described in (18) and (19). Under Assumptions 1 and 2, and using the cooperative system composed of (28), (29), and (30), the global voltage synchronization error η_v in (27) is UUB. That is, the resilient voltage synchronization problem is solved.

***Proof*:** The global form of (28), (29), and (30) are

$$\dot{V} = c_v(-\sum_{\gamma=u,l} \Theta_\gamma V + \sum_{\gamma=u,l} \Theta_\gamma \left(\mathbf{1}_N \otimes V_{\text{ref}}^\gamma\right) + \delta - \hat{\delta}), \tag{32}$$

$$\dot{\hat{V}} = c_v(-\sum_{\gamma=u,l} \Theta_\gamma \hat{V} + \sum_{\gamma=u,l} \Theta_\gamma \left(\mathbf{1}_N \otimes V_{\text{ref}}^\gamma\right) + \tilde{V}), \tag{33}$$

$$\dot{\hat{\delta}} = c_v \sum_{\gamma=u,l} \Theta_\gamma \tilde{V}, \tag{34}$$

respectively, where $\hat{\delta} = [\hat{\delta}_1^T, ..., \hat{\delta}_N^T]^T$ and $\tilde{V} = [\tilde{V}_1^T, ..., \tilde{V}_N^T]^T$. Define $\tilde{\delta}_i = \delta_i - \hat{\delta}_i$ and the global form $\tilde{\delta} = [\tilde{\delta}_1^T, ..., \tilde{\delta}_N^T]^T$. Combing (32) and (33) yields

$$\dot{\tilde{V}} = -c_v \left(\sum_{\gamma=u,l} \Theta_\gamma + I_N\right) \tilde{V} + c_v \tilde{\delta}. \tag{35}$$

From (34), we have

$$\dot{\tilde{\delta}} = \dot{\delta} - \dot{\hat{\delta}} = -c_v \sum_{\gamma=u,l} \Theta_\gamma \tilde{V} + \dot{\delta}. \tag{36}$$

Put (35) and (36) in the following compact from

$$\begin{bmatrix} \dot{\tilde{V}} \\ \dot{\tilde{\delta}} \end{bmatrix} = \begin{bmatrix} -c_v \left(\sum\limits_{\gamma=u,l} \Theta_\gamma + I_N\right) & c_v \\ -c_v \sum\limits_{\gamma=u,l} \Theta_\gamma & 0_N \end{bmatrix} \begin{bmatrix} \tilde{V} \\ \tilde{\delta} \end{bmatrix} + \begin{bmatrix} 0_N \\ \dot{\delta} \end{bmatrix}. \tag{37}$$

Denote $\chi = [\ \tilde{V}^T \quad \tilde{\delta}^T\ ]^T$ and $\Delta = [\ 0_N \quad \dot{\delta}^T\ ]^T$. Then,

$$\dot{\chi} = \begin{bmatrix} -c_v \left(\sum\limits_{\gamma=u,l} \Theta_\gamma + I_N \right) & c_v \\ -c_v \sum\limits_{\gamma=u,l} \Theta_\gamma & 0_N \end{bmatrix} \chi + \Delta. \tag{38}$$

Introducing $\xi = \mathrm{T}\chi$ with

$$\mathrm{T} = \begin{bmatrix} I_N & 0_N \\ -I_N & I_N \end{bmatrix}. \tag{39}$$

Then, we have

$$\begin{aligned} \dot{\xi} &= \mathrm{T} \begin{bmatrix} -c_v \left(\sum\limits_{\gamma=u,l} \Theta_\gamma + I_N \right) & c_v \\ -c_v \sum\limits_{\gamma=u,l} \Theta_\gamma & 0_N \end{bmatrix} \mathrm{T}^{-1}\xi + \mathrm{T}\Delta \\ &= \begin{bmatrix} -c_v \sum\limits_{\gamma=u,l} \Theta_\gamma & c_v \\ 0_N & -c_v \end{bmatrix} \xi + \Delta \\ &\equiv U\xi + \Delta. \end{aligned} \tag{40}$$

Given Assumption 1 and Lemma 1, $\sum\limits_{\gamma=u,l} \Theta_\gamma$ is positive-definite. Since c_v is also positive-definite, we obtain that $U = \begin{bmatrix} -c_v \sum\limits_{\gamma=u,l} \Theta_\gamma & c_v \\ 0_N & -c_v \end{bmatrix}$ has eigenvalues with negative real parts, and hence is Hurwitz. Then, given any matrix $Q = Q^T \succ 0$, there is a matrix $P = P^T \succ 0$, where

$$PU + U^T P = -Q. \tag{41}$$

Choosing the following Lyapunov function candidate

$$\mathbf{V} = \xi^T P \xi, \tag{42}$$

and its time derivative is

$$\begin{aligned}\dot{\mathbf{V}} &= -\xi^T Q\xi + 2\xi^T P\Delta \\ &\leq -\sigma_{\min}(Q)\|\xi\|^2 + 2\sigma_{\max}(P)\|\xi\|\|\Delta\| \\ &\leq 0, \qquad \forall \|\xi\| \geq \frac{2\sigma_{\max}(P)\|\Delta\|}{\sigma_{\min}(Q)}.\end{aligned} \tag{43}$$

Given Assumption 2, it is straightforward to verify that Δ is bounded. Then, using the LaSalle's invariance principle, we obtain that ξ is UUB with the ultimate bound of $\frac{2\sigma_{\max}(P)\|\Delta\|}{\sigma_{\min}(Q)}$. Hence, χ is also UUB. That is, both $\tilde{V}$ and $\tilde{\delta}$ are UUB.

Next, we prove that the estimated global voltage synchronization error $\hat{\eta}_v$ in (31) is UUB. Using (31) and (33) yields

$$\begin{aligned}\dot{\hat{\eta}}_v &= \dot{\hat{V}} \\ &= c_v\left(-\sum_{\gamma=u,l}\Theta_\gamma\hat{V} + \sum_{\gamma=u,l}\Theta_\gamma\left(\mathbf{1}_N \otimes V_{\text{ref}}^\gamma\right) + \tilde{V}\right) \\ &= -c_v\sum_{\gamma=u,l}\Theta_\gamma\hat{\eta}_v + c_v\tilde{V}.\end{aligned} \tag{44}$$

Since $-\sum_{\gamma=u,l}\Theta_\gamma$ is Hurwitz and $\tilde{V}$ is bounded, we similarly obtain that $\hat{\eta}_v$ is UUB. Note that $\eta_v = \tilde{V} + \hat{\eta}_v$, we then finally obtain that η_v is UUB. ■

***Remark* 3:** As shown in Theorem 1, by integrating the virtual resilient layer (29) and (30) with the original cyber-physical layer (28), we construct a stable system matrix for the augmented estimation error dynamics with bounded disturbances. This guarantees the uniform ultimate boundedness of the overall system.

***Remark* 4:** The idea of a virtual system with a hidden network, that interconnects with the original network, is given in [43] to address leaderless consensus of undirected graphs against attacks with linear dynamics. The extension of this idea in [44] addresses leader-follower consensus of directed graphs under attacks with nonlinear dynamics. Note that these studies deal with *bounded* injections.

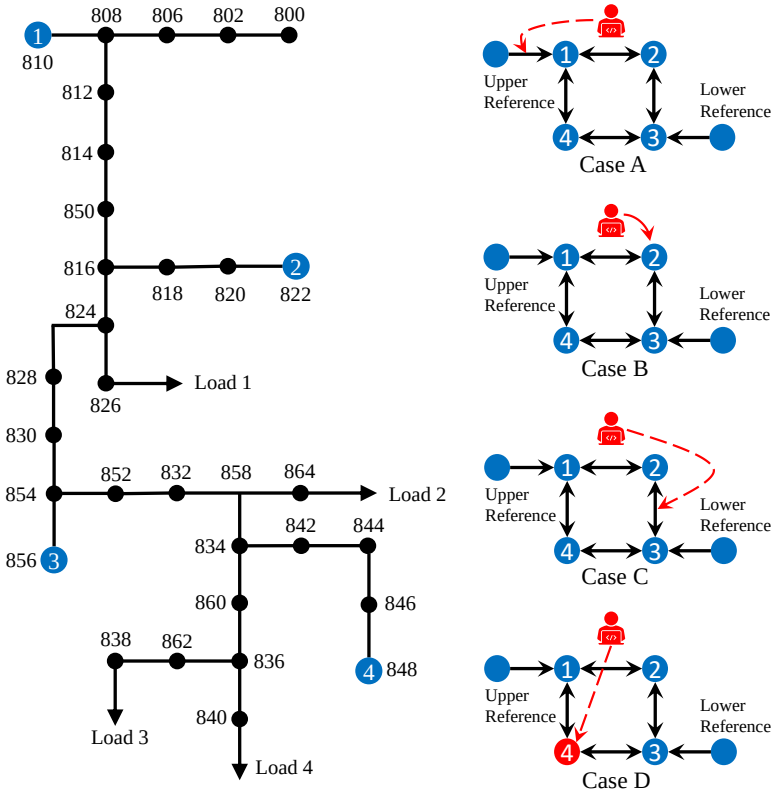

Fig. 3: Islanded IEEE 34-bus system augmented with four inverters and their communication networks under different attack scenarios.

***Remark* 5:** Our method provides resiliency to unbounded attacks without isolating the compromised agents. This is in contrast to the existing defense mechanisms [12]–[19], where an agent simply discards the corrupted data/information from the neighbors. This could damage the network connectivity, and compromise the network-level consensus performance. On the other hand, the existing attack detection and correction method usually requires that at least half of the total number of agents needs to be intact [20], [21]. Whereas, our resilient control protocols do not have any restrictions on the number of compromised agents.

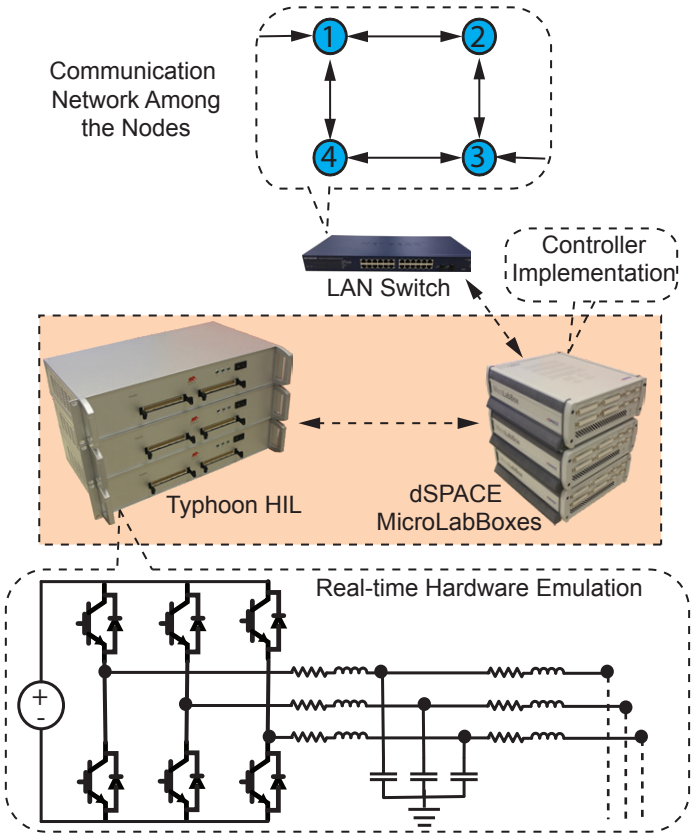

Fig. 4: Physical components like inverters, their interconnections, filters, and the distribution bus are emulated on Typhoon HILs. Distributed controllers are implemented on dSPACE systems. The communication network is realized partly through a LAN switch.

VI. Experimental Evaluation

A. AC Microgrid Testbed

The proposed distributed resilient control method is implemented on an IEEE 34-bus balanced test feeder upgraded with four inverters [27], as illustrated in Fig. 3. This feeder is isolated from the legacy grid at bus 800. The inverters and distribution lines specifications are adopted from [37] and [45], respectively, with slight modifications. This work employs inverters with identical component ratings ($R_{ci} = 0.03\Omega$, $L_{ci} = 0.35\,\mathrm{mH}$, $R_{fi} = 0.1\Omega$, $L_{fi} = 1.35\,\mathrm{mH}$, and $C_{fi} = 50\,\mu\mathrm{F}$). Inverters are interfaced with the distribution network via Y-Y, 480 V/24.9 kV, 400 kVA transformers. Each load

is represented by a balanced three-phase RL branch connected in a star arrangement equivalent to 20 kW and 20 kVAr active and reactive powers, respectively. The upper and lower reference points, for the inverter's voltage, are given as 340 V and 330 V, respectively. The reference frequency is set to 60 Hz. Inverters and the distribution network are emulated in Typhoon HIL 604 units, distributed control routines are implemented in dSPACE DS 1202 MicroLab Boxes (MLBX), and the communication among MLBX is achieved via a Netgear ProSAFE 24-port Ethernet Smart Switch as shown in Fig. 4.

B. Controller Performance Assessment

As shown in Fig. 3, there are four inverters, two leaders, and one attacker. In the following case studies, we use agent 1, 2, 3 and 4 to represent the four inverters, and agent 5 to represent the attacker. Four types of malicious attacks are considered: a) the injections to the communication links from the leaders, b) the direct relative information injected from the attackers, c) the injections to the communication links among inverters, and d) the injections to the local state-feedback of an inverter. All unbounded cyber attacks are initiated at $t = 5s$. The parameters of the resilient control protocols (28) to (30) are set as $c_{vi} = 10$, $c_{fi} = 20$, $a_{ij} = 1$, $g_i^u = 1$, and $g_i^l = 1$.

Case A: The attack on the communication link from the upper reference leader to inverter 1 is modeled using (17). Therein, $\bar{V}_{1,\mathrm{ref}}^u(t) = V_{\mathrm{ref}}^u(t) + \sigma_{1\,\mathrm{ref}}^v(t)$, where $\sigma_{1\,\mathrm{ref}}^v(t) = 4t$. Correspondingly, the frequency injection is $\sigma_{1\,\mathrm{ref}}^{\omega}(t) = 0.1t$.

Case B: Inverter 2 receives a direct injection from the attacker, where $V_5 = 2t$ and $\omega_{n5} = 0.05t$, with the edge weights $h_{25}^v = 1$ and $h_{25}^{\omega} = 0.01$ for voltage and frequency control, respectively.

Case C: The attack on the communication channel from inverter 2 to inverter 3 is modeled using (19). Therein, $\bar{V}_{3,2}(t) = V_2(t) + \sigma_{32}^v(t)$, where $\sigma_{32}^v(t) = 4t$. Correspondingly, the frequency injection is set as $\sigma_{32}^{\omega}(t) = 0.1t$.

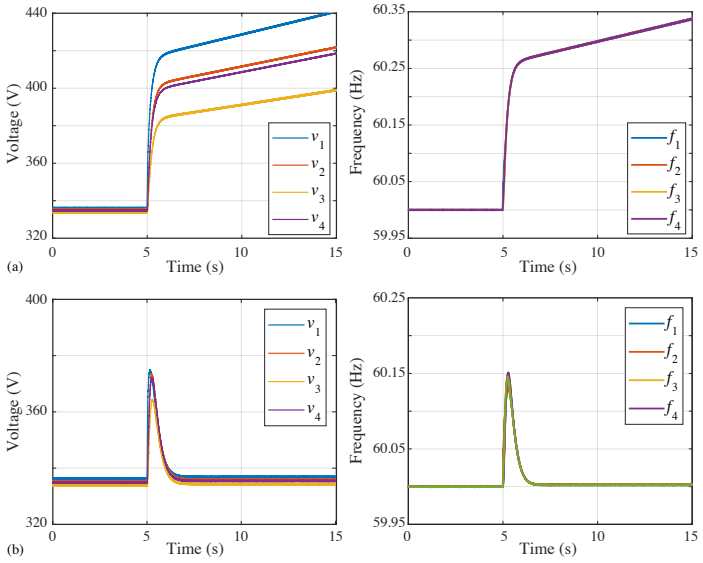

Fig. 5: Inverters' variables in Case A for the a) conventional cooperative control and the b) proposed resilient cooperative control.

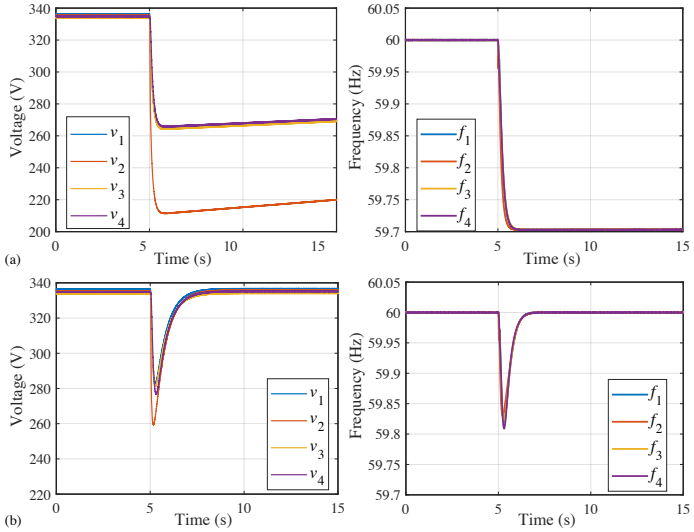

Fig. 6: Inverters' variables in Case B for the a) conventional cooperative control and the b) proposed resilient cooperative control.

Case D: The attack on the state feedback of inverter 4 is modeled using (19). Therein, $\bar{V}_{4,4}(t) = V_4(t) + \sigma^v_{44}(t)$, where $\sigma^v_{44}(t) = -2t$. Correspondingly, the frequency injection is set as $\sigma^\omega_{44}(t) = -0.05t$.

We have also listed the attack values in Table I.

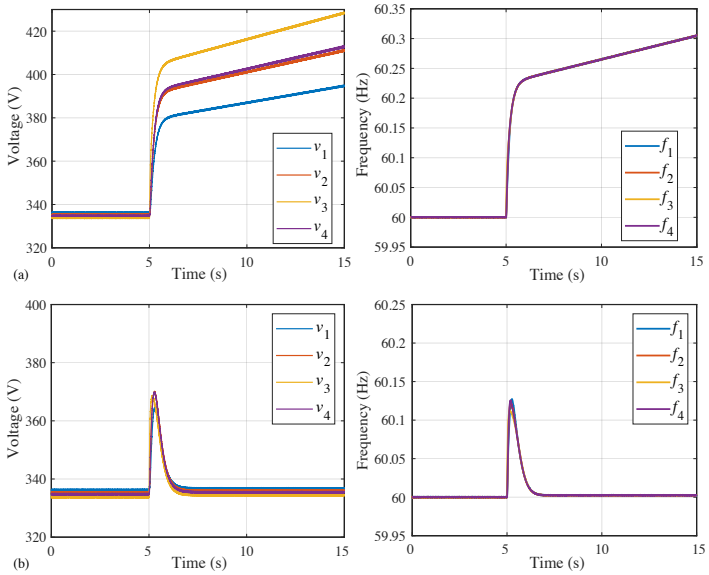

Fig. 7: Inverters' variables in Case C for the a) conventional cooperative control and the b) proposed resilient cooperative control.

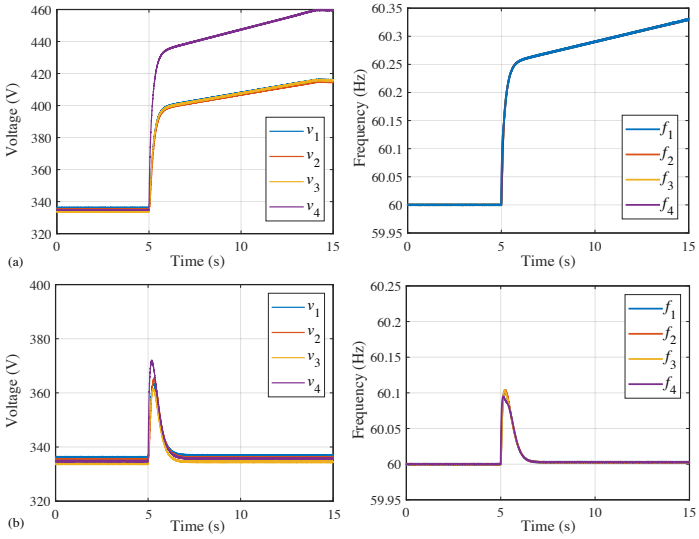

Fig. 8: Inverters' variables in Case D for the a) conventional cooperative control and the b) proposed resilient cooperative control.

The proposed resilient controller composed of (28), (29), and (30) is compared with the conventional cooperative controller (18) for the considered scenarios A, B, C, and D in Fig. 5, Fig. 6, Fig. 7, and Fig. 8, respectively. The voltage control module acts on filtered measurements being shared among the inverters, and the same voltages are used

TABLE I: Values of the Attacks to the Voltage and Frequency Loops

	Voltage	Frequency
Case A	$\sigma^{v}_{1\,\mathrm{ref}}(t) = 4t$	$\sigma^{\omega}_{1\,\mathrm{ref}}(t) = 0.1t$
Case B	$V_5 = 2t$	$\omega_{n5} = 0.05t$
Case C	$\sigma^{v}_{32}(t) = 4t$	$\sigma^{\omega}_{32}(t) = 0.1t$
Case D	$\sigma^{v}_{44}(t) = -2t$	$\sigma^{\omega}_{44}(t) = -0.05t$

to produce the corresponding figures. One can see that, in the presence of unbounded attacks for all four different scenarios, the conventional cooperative controller fails to maintain the overall system stability, but the proposed resilient approach maintains the magnitude of the bus voltage within the prescribed range and achieves UUB regulation on the frequency term. That is, the resilient secondary voltage and frequency synchronization problems, for networked AC microgrids, are solved under unbounded cyber attacks.

VII. Conclusion

We have introduced a networked AC microgrid that has cooperative and adversarial elements consisting of leaders, inverters, and attackers. We have considered four types of unbounded cyber attacks: injections to the communication links from the leaders to local inverters, hijacking inverter signals or pretending to be an inverter where there is none, injections to the communication links among inverters, and distorting the local state-feedback of an individual inverter. We have proposed a fully distributed control framework consisting of the original cooperative and adversarial multi-inverter physical

systems and a virtual MAS with hidden and secure networks. The performance of this approach, in maintaining the overall system stability and attaining the bounded frequency regulation and voltage containment, has been verified in a CHIL environment.

ACKNOWLEDGMENT

The authors thank Ajay P. Yadav for his help in initial HIL modeling efforts and graphics.

REFERENCES

[1] S. Gorman, "Electricity grid in us penetrated by spies," *The Wall Street J.*, vol. 8, Apr. 2009.

[2] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 645-658, Dec. 2011.

[3] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proc. ACM Conf. Comput. Commun. Security*, 2009, pp. 21-32.

[4] X. Liu et al., "Microgrid risk analysis considering the impact of cyber attacks on solar pv and ess control systems," *IEEE Trans. Smart Grid*, vol. 8, no. 3, pp. 1330-1339, May 2017.

[5] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber-physical system security for the electric power grid," *Proc. IEEE*, vol. 100, pp. 210– 224, Jan. 2012.

[6] H. He and J. Yan, "Cyber-physical attacks and defences in the smart grid: a survey," *IET Cyber-Phys. Syst., Theory Appl.*, vol. 1, no. 1, pp. 13-27, June 2016.

[7] A. Mohsenian-Rad, and A. Leon-Garcia, "Distributed internet-based load altering attacks against smart power grids," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 667-674, Dec. 2011.

[8] J. W. Simpson-Porco, F. Dörfler, and F. Bullo, "Synchronization and power sharing for droop-controlled inverters in islanded microgrids," *Automatica*, vol. 49, no. 9, pp. 2603-2611, Sep. 2013.

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

[10] 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.

[11] S. Zuo, A. Davoudi, Y. Song, and F. L. Lewis, "Distributed finite-time voltage and frequency restoration in islanded ac microgrids," *IEEE Trans. Ind. Electron.*, vol. 63, no. 10, pp. 5988–5997, Jun. 2016.

[12] 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.

[13] S. Sridhar and M. Govindarasu, "Model-based attack detection and mitigation for automatic generation control," *IEEE Trans. Smart Grid*, vol. 5, pp. 580–591, Mar. 2014.

[14] Y. Huang et al., "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, Jun. 2016.

[15] 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.

[16] 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, Mar. 2014.

[17] L. Y. Lu, H. J. Liu, and H. Zhu, "Distributed secondary control for isolated microgrids under malicious attacks," in *North American Power Symposium*, 2016, pp. 1-6.

[18] L.Che, X. Liu and Z. Li, "Fast screening out high risk lines under false data injection attacks," *IEEE Trans. Smart Grid*, vol. 1, no. 1, pp. 1-1, Jun. 2018.

[19] Z. Peng, R. Deng, and H. Liang, "False data injection attacks against state estimation in multiphase and unbalanced smart distribution systems," *IEEE Trans. Smart Grid*, vol. 10, no. 6, pp. 6000-6013, Nov. 2019.

[20] Z. Tang, M. Kuijper, M. S. Chong, and I. Mareels, "Linear system security-detection and correction of adversarial sensor attacks in the noise-free case," *Automatica*, vol. 101, pp. 53–59, 2019.

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

[22] J. Kim and L. Tong, "On topology attack of a smart grid: undetectable attacks and countermeasures," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 7, pp. 1294–1305, Jul. 2013.

[23] G. Hug and J. A. Giampapa, "Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks," *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1362–1370, Sep. 2012.

[24] G. Liang, J. Zhao, and F. Luo, , "A review of false data injection attacks against modern power systems," *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1630 - 1638, Jul. 2017.

[25] 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.

[26] J. Kim, L. Tong, and R. J. Thomas, "Data framing attack on state estimation with unknown network parameters," in *Proc. Asilomar Conf. Signals, Syst. Comput.*, 2013, pp. 1388–1392.

[27] S. Abhinav, I. D. Schizas, F. L. Lewis, and A. Davoudi, "Distributed noise-resilient networked synchrony of active distributed systems," *IEEE Trans. Smart Grid*, vol. 9, no. 2, pp. 836–846, Mar. 2018.

[28] N. M. Dehkordi, H. R. Baghaee, N. Sadati, and J. M. Guerrero, "Distributed noise-resilient secondary voltage and frequency control for islanded microgrids," *IEEE Trans. Smart Grid*, vol. 10, no. 4, pp. 3780–3790, Jul. 2019.

[29] M. Blanke, M. Kinnaert, J. Lunze, and M. Staroswiecki, *Diagnosis and Fault-Tolerant Control*. New York, NY, USA: Springer-Verlag, 2006.

[30] S. Liu, Z. Hu, X. Wang, and L. Wu, "Stochastic stability analysis and control of secondary frequency regulation for islanded microgrids under random denial of service attacks," *IEEE Trans. Ind. Inform.*, vol. 15, no. 7, pp. 4066-4075, Jul. 2019.

[31] S. Qobad, 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.

[32] J. W. Simpson-Porco et al., "Secondary frequency and voltage control of islanded microgrids via distributed averaging," *IEEE Trans. Ind. Electron.*, vol. 62, no. 11, pp. 7025-7038, Nov. 2015.

[33] L. Meng et al., "Distributed voltage unbalance compensation in islanded microgrids by using a dynamic consensus algorithm," *IEEE Trans. Power Electron.*, vol. 31, no. 1, pp. 827-838, Jan. 2016.

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

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

[36] R. Han, L. Meng, G. Ferrari-Trecate, E. A. Alves Coelho, J. C. Vasquez, and J. M. Guerrero, "Containment and consensus-based distributed coordination control to achieve bounded voltage and precise reactive power sharing in islanded ac microgrids," *IEEE Trans. Ind. Appl.*, vol. 53, no. 6, pp. 5187-5199, Nov. 2017.

[37] A. Bidram, F. L. 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.

[38] H. K. Khalil, *Nonlinear systems*. Upper Saddle River, NJ: Prentice Hall, 3rd edition, 2002.

[39] R. T. Rockafellar, *Convex analysis*. Princeton university press, 2015.

[40] S. Zuo, Y. Song, F. L. Lewis, and A. Davoudi, "Output containment control of linear heterogeneous multi-agent systems using internal model principle," *IEEE Trans. Cybern.*, vol. 47, no. 8, pp. 2099–2109, Aug. 2017.

[41] D. Kreutz, F. M. Ramos, P. E. Verissimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, "Software-defined networking: A comprehensive survey," *Proceedings of the IEEE*, vol. 103, no. 1, pp. 14-76, 2015.

[42] D. Jin et al., "Toward a cyber resilient and secure microgrid using software-defined networking," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2494-2504, Sep. 2017.

[43] B. Gharesifard and T. Basar, "Resilience in consensus dynamics via competitive interconnections," in *3rd IFAC Workshop on Estimation and Control of Networked Systems*, pp. 234–239, Santa Barbara, California, September 14-15, 2012.

[44] A. Gusrialdi, Z. Qu, and M. A. Simaan, "Competitive interaction design of cooperative systems against attacks," *IEEE Trans. Autom. Control*, vol. 63, no. 9, pp. 3159-3166, Sep. 2018.

[45] 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 4

DISTRIBUTED RESILIENT SECONDARY CONTROL OF DC MICROGRIDS AGAINST UNBOUNDED ATTACKS[1]

Authors: Shan Zuo, Tuncay Altun, Frank L. Lewis, and Ali Davoudi.

Reprinted, with permission from all the co-authors.

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

DOI: 10.1109/TSG.2020.2992118

Distributed Resilient Secondary Control of DC Microgrids against Unbounded Attacks

Shan Zuo, Tuncay Altun, Frank L. Lewis, *Life Fellow, IEEE*,
Ali Davoudi, *Senior Member, IEEE*

Abstract

This paper develops a fully distributed attack-resilient secondary control framework for DC microgrids, in the presence of unknown unbounded attacks on control input channels. The secondary control of each converter consists of an average consensus-based voltage regulator and a consensus-based current regulator that use relative information from neighboring converters. This distributed control manner relies on localized control and a sparse communication network and, therefore, could be prone to malicious attacks that deteriorate the consensus performance and even destabilize the overall microgrids. In contrast to the existing remedies for bounded disturbances/noises, this paper considers unknown attacks that are intentionally unbounded to maximize their damage on the microgrid. A fully distributed adaptive attack-resilient secondary control framework is established for DC microgrids to mitigate the adverse effect of unbounded attacks. Rigorous proofs, based on Lyapunov techniques, show that the proposed method guarantees the uniformly ultimately bounded convergence for both global voltage regulation and proportional load sharing objectives under unbounded attacks. Moreover, the asymptotic stability of the overall closed-loop system is achieved in the presence of bounded attacks. Experimental results are illustrated in a hardware-in-the-loop environment to validate the effectiveness of the proposed approach.

This work was supported in part by the ONR grant N00014-17-1-2239.

Shan Zuo, Tuncay Altun, Frank L. Lewis, and Ali Davoudi are with the Electrical Engineering Department, The University of Texas, Arlington, TX 76019, USA (e-mail: shan.zuo@uta.edu; tuncay.altun@mavs.uta.edu; lewis@uta.edu; davoudi@uta.edu).

Index Terms

DC microgrid, distributed control, resilient control, unbounded attacks.

I. Introduction

Direct current (DC) microgrids are gaining popularity given the DC nature of emerging distributed energy resources, storage units, and modern loads [1]–[3]. In their control hierarchy [4], [5], the secondary control adjusts the voltage setpoints for the primary control (usually, implemented through droop mechanisms) and eliminates the steady-state voltage drift and/or loading mismatch. The control objectives are global voltage regulation, where the average voltage over the distribution line is regulated at a reference value, and proportional load sharing, where power electronics converters share the total load among themselves based on their power ratings. The distributed implementation of the secondary control level has become popular due to its improved efficiency, scalability, and robustness [5]–[11]. For example, the cooperative control framework in [7] supplements the voltage reference for each converter by two voltage correction terms. The average voltage across the distribution line is estimated by a voltage observer and then compared with the global reference voltage. The difference is then given to a proportional-integral (PI) controller to produce the first voltage correction term. The mismatch between the current of a converter and its neighbors, fed into a PI controller, computes the second voltage correction term. Enhanced dynamic performance [8], finite settling time [9], or reduced communication traffic [10], [11] have been studied. All such cooperative control methods rely on message passing among power electronics converters on a communication network, local sensing of voltage/current, and decentralized droop mechanisms.

Cyber manipulation has already been a subject of research in power systems. DC microgrids have became a cyber-physical system by integrating the physical layer of

power electronics and the distribution network with the cyber layer of distributed local controllers and a sparse communication network. The distributed cooperative control framework makes these microgrids potentially vulnerable to malicious attacks and infiltration, as this control framework depends on local sensing and networked control on a sparse communication network [12]–[14]. Cyber risk assessment for industrial control systems, including supervisory or distributed control systems, has been detailed in [15] to quantify the attack probability and its impact. The vulnerability assessments of the false data injections on the state estimation process are studied in [16], [17] for power systems.

To address attacks for cyber-physical systems, misbehaving agents are detecked, identified, and then removed/overcome in [18]–[25]. Recently, [26]–[28] have investigated attack detection strategies for DC microgrids. This line of approach usually has strict requirements on the number of misbehaving agents. For example, [20], [21] show the impracticality involved in reconstructing the system state if less than half of the sensors are healthy. Moreover, simply removing/isolating the compromised agents could potentially damage the connectivity of the communication network and hence compromise the consensus performance. Sufficient and necessary conditions, for undetectable attacks to exist, are discussed in [12], [29], [30]. Malicious attacks can bypass existing detection methods by exploring the configuration of the power system. The fundamental limitations of existing attack-detection methods are thoroughly analyzed in [31].

In general, it will be virtually impossible to eliminate every potential attack threats for microgrids, and a path toward resilience is deemed indispensable. Recently, distributed resilient control protocols deal with external disturbances/noises without detecting, identifying, and removing/overcoming the compromised agents [7], [32]–[36]. A noise-resilient voltage observer in developed in [7] to estimate the average voltage

across the DC microgrids. Recently, [37] mitigated attacks on communication links and controller hijacking using a trust-based cooperative control paradigm. Note that the disturbances/noises/faults considered in the above literature have been treated as bounded signals. In practice, malicious attackers may intentionally launch unbounded injections at the cyber-physical system to maximize their damage [20]. Therefore, control strategies resilient to unknown unbounded attacks are of great importance to assure reliability and security of DC microgrids.

This paper considers the cooperative secondary control of DC microgrids in the presence of unknown unbounded attacks injected to the control input channels. The salient contributions are summarized as follows.

• The secondary control of multi-converter based DC microgrid is transformed into the consensus problem of the first-order linear multi-agent systems (MAS), where an auxiliary control input is generated using the relative measurement of each converter with respect to its neighboring converters. This formulation provides a faster response compared to the double PI controllers in [7] for voltage and current regulators.

• An smooth adaptive control framework ensures resilience to unknown attacks on local control input channel. The proposed control protocol is fully distributed without requiring any global-level information and, hence, is scalable with plug-and-play capability. In contrast to existing remedies in the literature for bounded disturbances/noises/faults, our approach considers more realistic unbounded attacks.

• Rigorous proofs based on Lyapunov techniques show that the uniformly ultimately bounded (UUB) and asymptotically stable (AS) convergences are achieved for global voltage regulation and proportional load sharing against unbounded and bounded attacks, respectively. That is, the proposed approach guarantees the bounded voltage and current regulations in the case of unbounded attacks, and maintains the exact voltage and current regulations in the case of bounded attacks by completely compensating aggregated

adverse effects.

• Experimental results validate the proposed attack-resilient controller, including robust performance under communication link failure and load change, and performance comparison with the standard secondary control protocols to show resilience against both unbounded and bounded attacks.

The remainder of the paper is organized as follows. In section II, the preliminaries on graph theory are reviewed, and the notations used in this paper are presented. In Section III, the standard cooperative secondary control of DC microgrids is proposed. The attack-resilient secondary control problems are formulated for unbounded and bounded attacks, and offered a fully distributed remedy for DC microgrids, in Section IV. In Section V, experimental results in a hardware-in-the-loop (HIL) environment validate the proposed results. Finally, Section VI provides the conclusion of the paper.

II. Preliminaries and Notations

A physical islanded DC microgrid system is mapped to a communication digraph. This time-invariant communication digraph $\mathscr{G}$ is composed of N converters, one leader node, and some adversarial nodes (attackers). The leader node issues the reference value to the neighboring converters. Each converter receives direct relative information from its neighboring converters and possibly the leader on the sparse communication digraph. The connections among local converters are represented by $\mathscr{G}_f = (\mathcal{W}, \mathcal{E}, \mathcal{A})$ with a nodes set $\mathcal{W}$, an edges set $\mathcal{E} \subset \mathcal{W} \times \mathcal{W}$, and an adjacency matrix $\mathcal{A} = [a_{ij}]$. A graph edge, indicating the information flow from converter j to converter i, is shown by (w_j, w_i), with the weight of a_{ij}. If $(w_j, w_i) \in \mathcal{E}$, then $a_{ij} > 0$; Otherwise, $a_{ij} = 0$. Node j is considered as the neighbor of node i if $(w_j, w_i) \in \mathcal{E}$. The set of neighbors of node i is denoted as $\mathcal{N}_i = \{j | (w_j, w_i) \in \mathcal{E}\}$. $\mathcal{D} = \mathrm{diag}(d_i) \in \mathbb{R}^{N \times N}$, with $d_i = \sum_{j \in \mathcal{N}_i} a_{ij}$, is called the in-degree matrix. $\mathcal{L} = \mathcal{D} - \mathcal{A}$ represents the Laplacian matrix. $\mathscr{G}_f$ is assumed bidirectional, i.e., $a_{ij} = a_{ji}$. Hence $\mathcal{L}$ is symmetric. g_i is the pinning gain for the link

from the leader to the i^{th} converter. $g_i > 0$ if the leader links to the i^{th} converter; Otherwise, $g_i = 0$. $\mathcal{G} = \mathrm{diag}\left(g_i\right), \forall i = 1, ..., N$, represents a diagonal matrix composed of pinning gains. $\mathbf{1}_N \in \mathbb{R}^N$ is a vector with all entries of one. $|\cdot|$ is the absolute value of a real number. $\mathrm{diag}\left\{\cdot\right\}$ constitutes a diagonal matrix from its set of elements.

III. Standard Cooperative Secondary Control

Fig. 1 illustrates the physical, control, and communication layers of the DC microgrids. As seen from the standard secondary control block, each converter transmits $\mathrm{X}_i = \left[\bar{V}_i, R_i^{\mathrm{vir}} I_i\right]$ to its neighboring converters on a communication graph. $\bar{V}_i$ is the estimated average voltage across the microgrid, I_i is the output current of the i^{th} converter, and R_i^{vir} is a virtual impedance tuned as $R_i^{\mathrm{vir}} = k \big/ I_i^{\mathrm{rated}}$, where k is a design parameter and I_i^{rated} is the rated current of the i^{th} converter. Note that $R_i^{\mathrm{vir}} I_i = k I_i \big/ I_i^{\mathrm{rated}}$. Hence, achieving the proportional load sharing is equivalent to achieving the consensus on terms of $R_i^{\mathrm{vir}} I_i$.

We present a standard cooperative secondary control method for DC microgrids, by transforming it to the consensus control for first-order linear MAS. The two main objectives of the secondary/primary control are to regulate the average voltage across the microgrids to a global reference value and proportionally share the load. As illustrated in Fig. 1, the standard secondary control uses the relative information of a converter with respect to the neighboring converters to adjust its local voltage setpoint V_i^*. The primary-level droop mechanism acts on local information and models the converter's output impedance with a virtual impedance R_i^{vir}. Cooperative secondary control among neighboring converters helps properly tune the local voltage setpoint V_i^* and attenuate the voltage and current residuals. The local voltage setpoint is given as

$$V_i^* = V_{n_i} + V_{\mathrm{ref}} - R_i^{\mathrm{vir}} I_i, \tag{1}$$

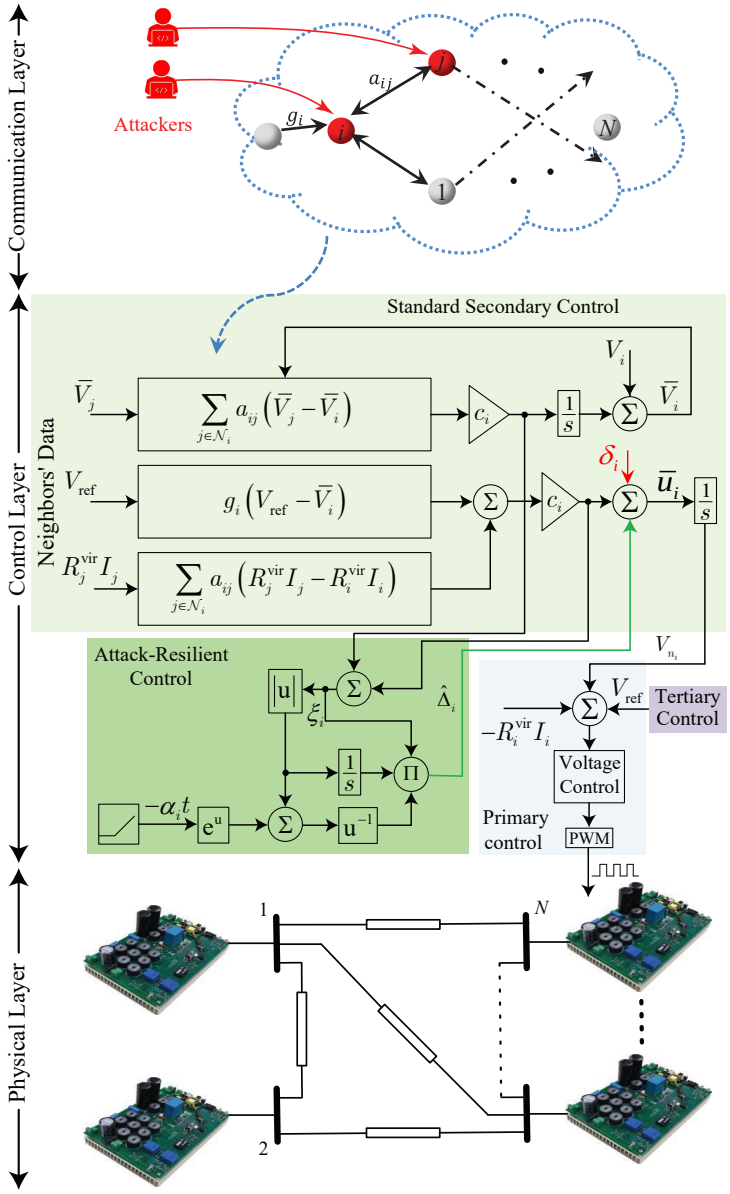

Fig. 1: Cyber-physical DC microgrids: Communication layer for data exchange among converters, control layer including standard and resilient cooperative control modules, and the physical layer including converters, distribution line, and sources/loads.

where V_{n_i} is the reference for the primary control level and is selected at the secondary control level.

To achieve the global voltage regulation and proportional load sharing, the secondary control provides V_{n_i} locally for each converter by exchanging data with its neighboring

converters. Using input-output feedback linearization techniques, we differentiate the voltage droop mechanism in (1) to obtain

$$\dot{V}_{n_i} = \dot{V}_i^* + R_i^{\text{vir}} \dot{I}_i = u_i, \tag{2}$$

where u_i is the control input. (2) computes the primary control reference V_{n_i} from u_i. The secondary control of DC microgrids is then transformed to a consensus problem for first-order linear MAS. In order to provide global voltage regulation and proportional load sharing, the cooperative secondary control law at each converter, based on the relative information with respect to the neighboring converters, is given by

$$u_i = c_i \left(g_i \left(V_{\text{ref}} - \bar{V}_i \right) + \sum_{j \in \mathcal{N}_i} a_{ij} \left(R_j^{\text{vir}} I_j - R_i^{\text{vir}} I_i \right) \right), \tag{3}$$

where $c_i \in \mathbb{R} > 0$ is the coupling gain. $\bar{V}_i$ is the estimate of the global average voltage value at converter i and is given by

$$\dot{\bar{V}}_i = \dot{V}_i + c_i \sum_{j \in \mathcal{N}_i} a_{ij} \left(\bar{V}_j - \bar{V}_i \right), \tag{4}$$

where V_i is the local measured voltage. The secondary control setpoint for the primary control, V_{n_i}, is then computed from u_i as

$$V_{n_i} = \int u_i \, \mathrm{d}\, t. \tag{5}$$

Assume that the converter produces the demanded voltage, i.e., $V_i^* = V_i$. Combining (2), (3), and (4) yields

$$\dot{\bar{V}}_i + R_i^{\text{vir}} \dot{I}_i = c_i \left(\sum_{j \in \mathcal{N}_i} a_{ij} \left(\bar{V}_j - \bar{V}_i \right) + g_i \left(V_{\text{ref}} - \bar{V}_i \right) + \sum_{j \in \mathcal{N}_i} a_{ij} \left(R_j^{\text{vir}} I_j - R_i^{\text{vir}} I_i \right) \right), \tag{6}$$

which are further formulated as

$$\begin{aligned}\dot{\bar{V}}_i + R_i^{\text{vir}}\dot{I}_i = c_i \Bigg(& \sum_{j\in\mathcal{N}_i} a_{ij}\left(\left(\bar{V}_j + R_j^{\text{vir}} I_j\right) - \left(\bar{V}_i + R_i^{\text{vir}} I_i\right)\right) \\ & + g_i\left(\left(V_{\text{ref}} + R_i^{\text{vir}} I_i\right) - \left(\bar{V}_i + R_i^{\text{vir}} I_i\right)\right)\Bigg).\end{aligned} \tag{7}$$

[7] gives the detailed steady-state analysis to show that the cooperative secondary control achieves both voltage and current regulation objectives, due to the relationship between the supplied currents and the bus voltage through the microgrid admittance matrix. Similarly, we obtain that, in the steady state, $R_i^{\text{vir}} I_i$ converges to a certain constant value kI_{ss}^{pu}. Denote $\Theta_i = \bar{V}_i + R_i^{\text{vir}} I_i$ and $\Theta_{\text{ref}} = V_{\text{ref}} + kI_{ss}^{\text{pu}}$. Then,

$$\begin{aligned}\dot{\Theta}_i &= c_i\left(\sum_{j\in\mathcal{N}_i} a_{ij}\left(\Theta_j - \Theta_i\right) + g_i\left(\Theta_{\text{ref}} - \Theta_i\right)\right) \\ &= c_i\left(-\left(d_i + g_i\right)\Theta_i + \sum_{j\in\mathcal{N}_i} a_{ij}\Theta_j + g_i\Theta_{\text{ref}}\right).\end{aligned} \tag{8}$$

The global form of (8) is

$$\dot{\Theta} = -\operatorname{diag}\left(c_i\right)\left(\mathcal{L} + \mathcal{G}\right)\left(\Theta - \mathbf{1}_N\Theta_{\text{ref}}\right), \tag{9}$$

where $\Theta = [\Theta_1^T, ..., \Theta_N^T]^T$.

Define the following global cooperative regulation error

$$\varepsilon = \Theta - \mathbf{1}_N\Theta_{\text{ref}}, \tag{10}$$

where $\varepsilon = [\varepsilon_1^T, ..., \varepsilon_N^T]^T$. The following assumption is needed for the communication network.

***Assumption* 1:** The digraph $\mathcal{G}$ includes a spanning tree, where the leader node is the root.

***Lemma* 1 ([38]):** Given Assumption 1, $(\mathcal{L} + \mathcal{G})$ is non-singular and positive-definite.

***Lemma* 2:** Given Assumption 1, by designing the auxiliary control input as (3) and

(4), the global voltage regulation and proportional load sharing are both achieved.

***Proof*:** Use (9) and (10) to obtain

$$\dot{\varepsilon} = -\operatorname{diag}(c_i)(\mathcal{L}+\mathcal{G})\varepsilon. \tag{11}$$

From Lemma 1, $(\mathcal{L}+\mathcal{G})$ is positive-definite. Hence, $\varepsilon \to 0$ asymptotically, i.e., $\Theta_i \to \Theta_{\text{ref}}$. Due to the relationship between the supplied currents and the bus voltage, we obtain that $\bar{V}_i \to V_{\text{ref}}$ and $R_i^{\text{vir}} I_i \to k I_{ss}^{\text{pu}}$, simultaneously. Steady-state analysis in [7] shows that since $\mathcal{L}$ is symmetric, $\bar{V}_i$ converges to the global average voltage value by using observer (4). Hence, the average value of $V_i, \forall i = 1, ..., N$ converges to V_{ref}. That is, both the global voltage regulation and proportional load sharing are achieved. This completes the proof. ■

***Remark* 1:** Using the input-output feedback linearization techniques, we have transformed the secondary control problem of DC microgrids to the tracking synchronization problem of first-order linear MAS. Then, by using the standard cooperative control protocols for the first-order linear MAS, we have proposed the standard secondary control protocols (3) and (4) to achieve the global voltage regulation and proportional load sharing. Compared to the double PI controllers in [7], our formulation provides a faster dynamic response.

IV. Resilient Secondary Control

In this section, we first formulate the attack-resilient secondary control problems for DC microgrids under unknown unbounded and bounded attacks, respectively. Then, we develop a fully-distributed adaptive control framework to address these problems. Rigorous proofs based on Lyapunov techniques show that UUB and AS convergences are achieved for voltage and current regulations against unbounded and bounded attacks, respectively.

A. Attack-Resilient Secondary Control Problem Formulation

As illustrated in Fig. 1, malicious attackers may inject unknown unbounded exogenous signals to perturb the local control input channel of each converter. Hence, instead of (2), we have

$$\dot{V}_{n_i} = \dot{V}_i^* + R_i^{\text{vir}} \dot{I}_i = \bar{u}_i = u_i + \delta_i, \tag{12}$$

where $\bar{u}_i$ is the corrupted control input and δ_i denotes the potential unbounded injections into the local control input channel. The attacker aims at destabilizing the cooperative regulation system by inserting these unbounded attacks.

***Assumption* 2:** For each converter, $\dot{\delta}_i$ is bounded.

***Remark* 2:** The attackers' injections, δ_i, can be any unbounded signals satisfying Assumption 2 or any bounded signals. Compared with the noise-resilient control protocols for DC microgrids in [7], [37], which deal with bounded noises/disturbances, we consider the more practical and challenging case of unbounded attack injections.

Consider the attack injections in (12) and use the standard secondary control protocols (3) and (4). Then, instead of the closed-loop error dynamics in (11), we obtain

$$\dot{\varepsilon} = -\operatorname{diag}(c_i)(\mathcal{L} + \mathcal{G})\varepsilon + \delta, \tag{13}$$

where $\delta = [\delta_1^T, ..., \delta_N^T]^T$ is the attack vector. Since δ is unbounded, $\varepsilon \to \infty$. That is, the standard secondary control fails to preserve the stability of the DC microgrids in the presence of unbounded attacks. It is hence important to develop advanced attack-resilient control approach to address such unbounded attacks for microgrids.

To evaluate the convergence results of the attack-resilient method to be designed, we define the following stability result.

***Definition* 2 ([39]):** $x(t) \in \mathbb{R}$ is UUB with the ultimate bound b, if there exist constants $b, c > 0$, independent of $t_0 \geq 0$, and for every $a \in (0, c)$, there exists $t_1 =$

$t_1(a,b) \geq 0$, independent of t_0, such that

$$|x(t_0)| \leq a \quad \Rightarrow \quad |x(t)| \leq b, \forall t \geq t_0 + t_1 \tag{14}$$

Now, we formulate the attack-resilient secondary control problems for DC microgrids against unbounded and bounded attacks, respectively.

***Problem* 1:** Under the unknown unbounded cyber attacks on local control input channels, design local control protocols u_i in (12) for each converter using only the local measurement such that, for all initial conditions, ε in (10) is UUB. That is, the bounded global voltage regulation and proportional load sharing are both achieved.

***Problem* 2:** Under the unknown bounded attacks on local control input channels, design local control protocols u_i in (12) for each converter using only the local measurement such that, for all initial conditions, ε in (10) is AS. That is, the exact global voltage regulation and proportional load sharing are both achieved.

B. Distributed Attack-Resilient Secondary Controller Design

For convenience, we denote

$$\xi_i = c_i \left(\sum_{j \in \mathcal{N}_i} a_{ij} \left(\bar{V}_j - \bar{V}_i \right) + g_i \left(V_{\text{ref}} - \bar{V}_i \right) + \sum_{j \in \mathcal{N}_i} a_{ij} \left(R_j^{\text{vir}} I_j - R_i^{\text{vir}} I_i \right) \right). \tag{15}$$

To ensure bounded global voltage regulation and proportional load sharing under unknown unbounded attacks, we propose the following attack-resilient secondary control protocols

$$u_i = c_i \left(g_i \left(V_{\text{ref}} - \bar{V}_i \right) + \sum_{j \in \mathcal{N}_i} a_{ij} \left(R_j^{\text{vir}} I_j - R_i^{\text{vir}} I_i \right) \right) + \hat{\Delta}_i, \tag{16}$$

$$\hat{\Delta}_i = \frac{\xi_i \vartheta_i}{|\xi_i| + \exp(-\alpha_i t)}, \tag{17}$$

$$\dot{\vartheta}_i = \gamma_i |\xi_i|, \tag{18}$$

where $\hat{\Delta}_i$ is an adaptive compensational term, ϑ_i is an adaptive updating parameter, α_i and γ_i are positive constants. For convenience, set $\gamma_i \geq 1$. The uniform continuous function $\exp(-\alpha_i t)$ constructs a smooth control approach for practical implementation purpose.

Next, we give the main result of solving the attack-resilient secondary control problems for DC microgrids.

***Theorem* 1:** Given Assumptions 1 and 2, under the unknown unbounded attacks in (12), let the resilient control protocols consist of (4), (16), (17), and (18), then the cooperative regulation error ε in (10) is UUB. That is, Problem 1 is solved.

***Proof*:** Use (4), (12), and (16) to obtain the time-derivative of (15)

$$\begin{aligned}\dot{\xi}_i &= c_i\left(-\left(d_i+g_i\right)\dot{\Theta}_i+\sum_{j\in\mathcal{N}_i}a_{ij}\dot{\Theta}_j\right)\\ &= -c_i\left(d_i+g_i\right)\left(\xi_i+\delta_i+\hat{\Delta}_i\right)+c_i\sum_{j\in\mathcal{N}_i}a_{ij}\left(\xi_j+\delta_j+\hat{\Delta}_j\right).\end{aligned} \tag{19}$$

Denote $\Delta_i = \delta_i - \frac{1}{(d_i+g_i)}\sum_{j\in\mathcal{N}_i}a_{ij}\left(\xi_j+\delta_j+\hat{\Delta}_j\right)$. Given Assumption 2, we obtain that $\dot{\Delta}_i$ is bounded. (19) is then written as

$$\dot{\xi}_i = -c_i\left(d_i+g_i\right)\left(\xi_i+\Delta_i+\hat{\Delta}_i\right). \tag{20}$$

Consider the following Lyapunov function candidate

$$V_i = \frac{1}{2}\left(|\xi_i| - \frac{\mathrm{d}\,|\Delta_i|}{\mathrm{d}\,t}\right)^2, \tag{21}$$

and its time-derivative is given as

$$\dot{V}_i = \left(|\xi_i| - \frac{\mathrm{d}\,|\Delta_i|}{\mathrm{d}\,t}\right)\left(\frac{\mathrm{d}\,|\xi_i|}{\mathrm{d}\,t} - \frac{\mathrm{d}^2\,|\Delta_i|}{\mathrm{d}\,t^2}\right). \tag{22}$$

Since $\dot{\Delta}_i$ is bounded, and note that $\frac{\mathrm{d}|\Delta_i|}{\mathrm{d}\,t} = \frac{\Delta_i\dot{\Delta}_i}{|\Delta_i|} \leq \left|\dot{\Delta}_i\right|$, both $\frac{\mathrm{d}|\Delta_i|}{\mathrm{d}\,t}$ and $\frac{\mathrm{d}^2|\Delta_i|}{\mathrm{d}\,t^2}$ are

bounded. Note that

$$\begin{aligned}\frac{\mathrm{d}\left|\xi_i\right|}{\mathrm{d}\,t} &= \frac{\xi_i\dot{\xi}_i}{\left|\xi_i\right|}\\ &= \frac{-c_i\left(d_i+g_i\right)\xi_i\left(\xi_i+\Delta_i+\hat{\Delta}_i\right)}{\left|\xi_i\right|}\\ &= -c_i\left(d_i+g_i\right)\left(\left|\xi_i\right|+\frac{\xi_i\Delta_i}{\left|\xi_i\right|}+\frac{\xi_i\hat{\Delta}_i}{\left|\xi_i\right|}\right).\end{aligned} \tag{23}$$

Substituting (23) into (22) yields

$$\dot{V}_i = \left(\left|\xi_i\right|-\frac{\mathrm{d}\left|\Delta_i\right|}{\mathrm{d}\,t}\right)\left(-c_i\left(d_i+g_i\right)\left|\xi_i\right|-\frac{\mathrm{d}^2\left|\Delta_i\right|}{\mathrm{d}\,t^2}-c_i\left(d_i+g_i\right)\left(\frac{\xi_i\Delta_i}{\left|\xi_i\right|}+\frac{\xi_i\hat{\Delta}_i}{\left|\xi_i\right|}\right)\right). \tag{24}$$

Use (17) to obtain

$$\begin{aligned}&-c_i\left(d_i+g_i\right)\left(\frac{\xi_i\Delta_i}{\left|\xi_i\right|}+\frac{\xi_i\hat{\Delta}_i}{\left|\xi_i\right|}\right)\\ &= -c_i\left(d_i+g_i\right)\frac{\xi_i\Delta_i}{\left|\xi_i\right|}-c_i\left(d_i+g_i\right)\frac{\left|\xi_i\right|\vartheta_i}{\left|\xi_i\right|+\exp\left(-\alpha_i t\right)}\\ &\leq c_i\left(d_i+g_i\right)\left|\Delta_i\right|-c_i\left(d_i+g_i\right)\frac{\left|\xi_i\right|\vartheta_i}{\left|\xi_i\right|+\exp\left(-\alpha_i t\right)}\\ &\leq c_i\left(d_i+g_i\right)\frac{\left|\xi_i\right|\left|\Delta_i\right|+\exp\left(-\alpha_i t\right)\left|\Delta_i\right|-\left|\xi_i\right|\vartheta_i}{\left|\xi_i\right|+\exp\left(-\alpha_i t\right)}.\end{aligned} \tag{25}$$

Choosing $\left|\xi_i\right| > \frac{\mathrm{d}\left|\Delta_i\right|}{\mathrm{d}\,t}$ yields $\dot{\vartheta}_i > \frac{\mathrm{d}\left|\Delta_i\right|}{\mathrm{d}\,t}$. Since $\frac{\mathrm{d}\left|\Delta_i\right|}{\mathrm{d}\,t}$ is bounded, $\exp\left(-\alpha_i t\right)\left|\Delta_i\right| \to 0$. Hence, $\exists\tau_1 > 0$, such that for all $t \geq \tau_1$, we have

$$\left|\xi_i\right|\left|\Delta_i\right|+\exp\left(-\alpha_i t\right)\left|\Delta_i\right|-\left|\xi_i\right|\vartheta_i \leq 0. \tag{26}$$

Then, use (25) and (26) to obtain

$$-c_i\left(d_i+g_i\right)\left(\frac{\xi_i\Delta_i}{\left|\xi_i\right|}+\frac{\xi_i\hat{\Delta}_i}{\left|\xi_i\right|}\right) \leq 0, \quad t \geq \tau_1 \tag{27}$$

Combining (24) and (27) yields

$$\dot{V}_i \leq \left(|\xi_i| - \frac{\mathrm{d}\,|\Delta_i|}{\mathrm{d}\,t}\right)\left(-c_i\,(d_i+g_i)\,|\xi_i| - \frac{\mathrm{d}^2\,|\Delta_i|}{\mathrm{d}\,t^2}\right), \forall t \geq \tau_1. \tag{28}$$

Choosing $|\xi_i| \geq -\frac{1}{c_i(d_i+g_i)}\frac{\mathrm{d}^2|\Delta_i|}{\mathrm{d}\,t^2}$ yields

$$\dot{V}_i \leq 0, \quad \forall t \geq \tau_1 \tag{29}$$

That is, ξ_i is UUB. Moreover, using the LaSalle's invariance principle, ξ_i is bounded by

$$\max\left\{\frac{\mathrm{d}\,|\Delta_i|}{\mathrm{d}\,t}, -\frac{1}{c_i\,(d_i+g_i)}\frac{\mathrm{d}^2\,|\Delta_i|}{\mathrm{d}\,t^2}\right\}. \tag{30}$$

Note that

$$\xi = -\operatorname{diag}(c_i)\,(\mathcal{L}+\mathcal{G})\,\varepsilon, \tag{31}$$

where $\xi = [\xi^T, ..., \xi_N^T]^T$. Since ξ_i is UUB and $(\mathcal{L}+\mathcal{G})$ is non-singular, ε is UUB. This completes the proof. ■

Finally, we show that the global voltage regulation and proportional load sharing are maintained under bounded attacks. That is, the adverse effects of the bounded attacks are completely compensated by the proposed protocols.

***Theorem* 2:** Consider the unknown bounded attacks in (12). Let the resilient control protocols consist of (4), (16), (17), and (18). Then, the cooperative regulation error ε in (10) is AS. That is, Problem 2 is solved.

***Proof*:** Consider the error dynamics (20). Since δ_i is bounded, Δ_i is also bounded. Denote the supremum value of $|\Delta_i|$ as $\chi_i = \sup_{t\geq 0}|\Delta_i(t)|$. Note that χ_i is constant. Hence, $\dot{\chi}_i = 0$. Let $\tilde{\vartheta}_i = \chi_i - \vartheta_i$, and consider the following Lyapunov function candidate

$$V_i' = \frac{1}{2}\xi_i^2 + \frac{1}{2}\frac{c_i\,(d_i+g_i)}{\gamma_i}\tilde{\vartheta}_i^2. \tag{32}$$

Then, its time-derivative is given as

$$\begin{aligned}\dot{V}_i' &= \xi_i\dot{\xi}_i - \frac{c_i\left(d_i+g_i\right)}{\gamma_i}\tilde{\vartheta}_i\dot{\vartheta}_i \\ &= -c_i\left(d_i+g_i\right)\left(\xi_i^2+\Delta_i\xi_i+\hat{\Delta}_i\xi_i\right) - c_i\left(d_i+g_i\right)\left(\chi_i-\vartheta_i\right)|\xi_i| \\ &\leq -c_i\left(d_i+g_i\right)|\xi_i|^2 - c_i\left(d_i+g_i\right)\left(\chi_i|\xi_i| - |\Delta_i||\xi_i| + \hat{\Delta}_i\xi_i - \vartheta_i|\xi_i|\right).\end{aligned} \tag{33}$$

Let $\varpi_i = \chi_i - |\Delta_i|$. Then, we obtain

$$\begin{aligned}\dot{V}_i' &\leq -c_i\left(d_i+g_i\right)|\xi_i|^2 - c_i\left(d_i+g_i\right)\left(\varpi_i|\xi_i| + \frac{|\xi_i|^2\vartheta_i}{|\xi_i|+\exp\left(-\alpha_i t\right)} - \vartheta_i|\xi_i|\right) \\ &\leq -c_i\left(d_i+g_i\right)|\xi_i|^2 - c_i\left(d_i+g_i\right)\left(\varpi_i|\xi_i| - \frac{\exp\left(-\alpha_i t\right)\vartheta_i|\xi_i|}{|\xi_i|+\exp\left(-\alpha_i t\right)}\right).\end{aligned} \tag{34}$$

Note that $\varpi_i \geq 0$ and $\exp\left(-\alpha_i t\right)\vartheta_i \to 0$. Hence, $\exists\tau_2 > 0$, such that for all $t \geq \tau_2$, $\dot{V}_i' \leq 0$. $\dot{V}_i' = 0$ if and only if $|\xi_i| = 0$. Hence, ξ_i is AS. Furthermore, we obtain $\lim_{t\to\infty}\varepsilon_i\left(t\right) = 0$. This completes the proof. ■

***Remark* 3:** The proposed controller design is fully distributed, i.e., it does not need any information on the communication graph topology or the number of converters. Hence, the proposed approach is scalable and can be applied in a plug-and-play manner.

V. HARDWARE-IN-THE-LOOP VALIDATION

A. DC Microgrid HIL Testbed

In this section, we implement the proposed attack-resilient cooperative control protocols on a DC microgrid testbed as illustrated in Fig. 2. This testbed consists of eight DC-DC converters emulated on a Typhoon HIL 604 system [40] and passing messages on a bidirectional communication graph, the distributed local controllers implemented on a dSPACE DS 1202 MicroLabBoxes [41], and a desktop computer that has an Intel Xeon 3.6 GHz processor and 64 GB RAM. DC-DC buck converter parameters are

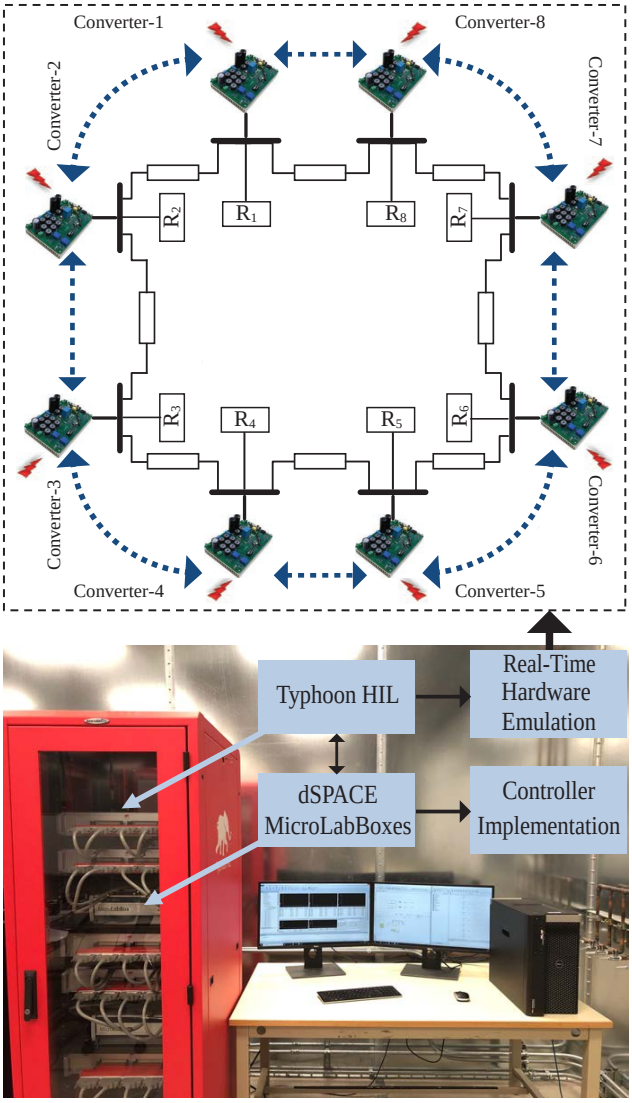

Fig. 2: The microgrid has eight DC-DC converters on a bidirectional ring communication network and distributed local controllers, implemented on a Typhoon HIL604 system and a dSPACE MicroLabBoxes, respectively.

$C = 2.2\,\mathrm{mF}$, $L = 2.64\,\mathrm{mH}$, $R_L = 10\Omega$, $f_s = 60\,\mathrm{kHz}$, and $V_{\mathrm{ref}} = 48\,\mathrm{V}$. The adjacency

matrix and the diagonal matrix of pinning gains are chosen as

$$\mathcal{A} = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix},$$

$$\mathcal{G} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix},$$

respectively. The control system parameters are chosen as

$$I_1^{\text{rated}} = I_4^{\text{rated}} = I_5^{\text{rated}} = I_8^{\text{rated}} = 1,$$

$$I_2^{\text{rated}} = I_3^{\text{rated}} = I_6^{\text{rated}} = I_7^{\text{rated}} = 2,$$

$$R_1^{\text{vir}} = R_4^{\text{vir}} = R_5^{\text{vir}} = R_8^{\text{vir}} = 2,$$

$$R_2^{\text{vir}} = R_3^{\text{vir}} = R_6^{\text{vir}} = R_7^{\text{vir}} = 1,$$

$$c_i = 10, \quad \alpha_i = 0.1, \quad \gamma_i = 5, \quad \forall i = 1, 2, ..., 8.$$

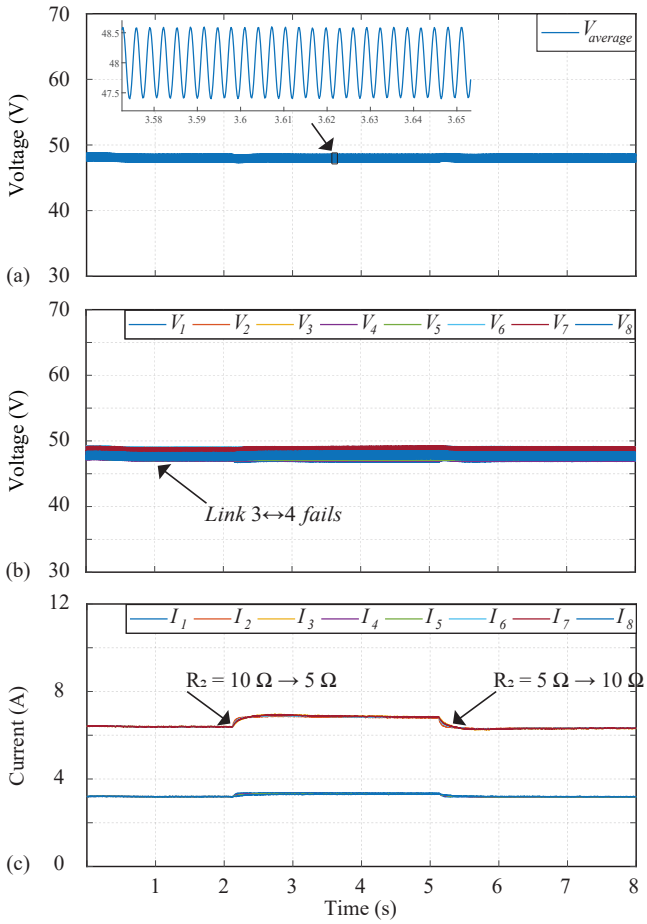

Fig. 3: Response of the proposed attack-resilient secondary controller to the link failure and load change: (a) Average voltage, (b) Terminal voltages, (c) Supplied currents.

B. Response to the Link Failure and Load Change

Herein, we study the response of the proposed attack-resilient controller to the link failure and load change. First, the communication link $3 \leftrightarrow 4$ fails at $t = 1s$. Then, the load at bus two, R_2, changes in step between 10Ω and 5Ω. Fig. 3 shows the performance of the average voltage, the terminal voltages and supplied currents using the proposed attack-resilient secondary controller. As shown in Fig. 3, the link failure has almost no impact on the control objectives since the communication digraph stays connected after link $3 \leftrightarrow 4$ fails. Moreover, the controller readjusts the voltages and properly

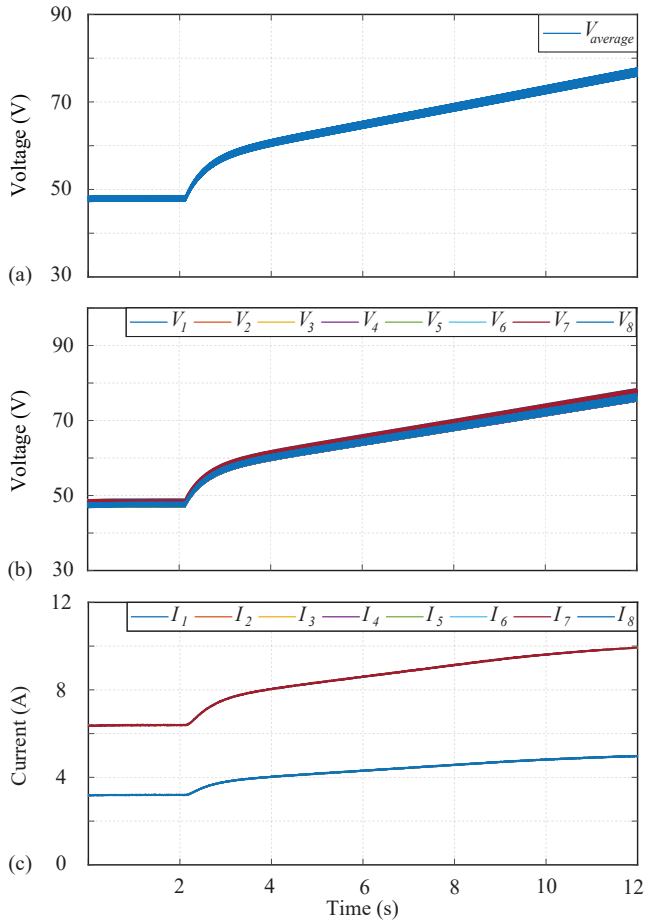

Fig. 4: Performance of the standard secondary control in the case of unbounded attack signals $\delta_i = 3t$: (a) Average voltage, (b) Terminal voltages, (c) Supplied currents.

updates the load sharing in case of load change to satisfy the global voltage regulation and proportional load sharing objectives. Fig. 3(a) shows that the average voltage is regulated at the set point, i.e., $V_{\text{ref}} = 48\,\text{V}$.

C. Performance Assessment Under Unknown Unbounded Attacks

In this section, we consider the attack model described in (12), where the attacks are injected at local control input of each converter by selecting $\delta_i = 3t,\ \forall i = 1, 2, ..., 8$. As seen these attacks are unbounded. We construct the proposed control protocols for each

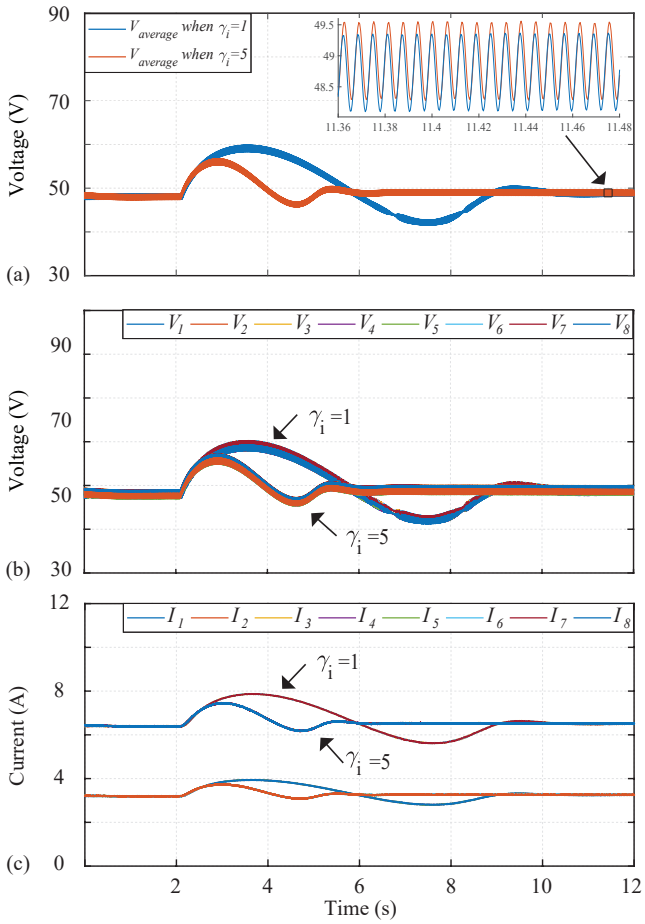

Fig. 5: Performance of the proposed attack-resilient control in the case of unbounded attack signals $\delta_i = 3t$: (a) Average voltage, (b) Terminal voltages, (c) Supplied currents.

converter using (4), (16), (17), and (18). For comparison, we also run the experiment using the standard secondary control protocols consisting of (3) and (4).

Note that the uniform continuous function $\exp(-\alpha_i t)$ in (17) is used only to construct a smooth control method when $|\xi_i| = 0$. Hence, the influence of different values of α_i on the convergence rate can be neglected. Whereas, in addition to tuning the coupling gain c_i, the adaptive tuning parameter in (18), γ_i, can tune the convergence rate of the system performance. In the following, we verify this behavior by running the experiment for different values of γ_i.

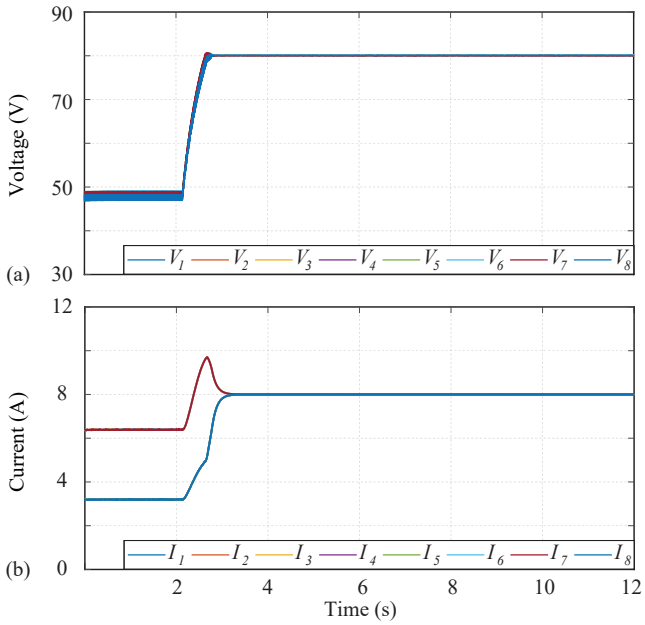

Fig. 6: Performance of the standard secondary control in the case of unbounded attack signals $\delta_i = 30t$: (a) Terminal voltages, (b) Supplied currents.

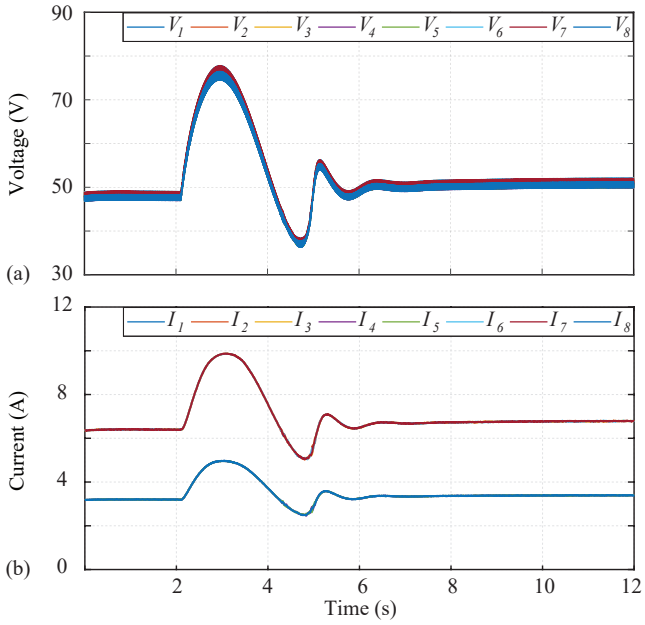

Fig. 7: Performance of the proposed attack-resilient control in the case of unbounded attack signals $\delta_i = 30t$: (a) Terminal voltages, (b) Supplied currents.

The experimental results, using the standard and the proposed attack-resilient methods, are comparatively illustrated in Fig. 4 and Fig. 5, respectively. Fig. 4 shows that the terminal voltages and the supplied currents, using the standard control protocols, diverge when unbounded attacks are applied. Whereas, Fig. 5(a) and Fig. 5(b) show that, by using the proposed resilient control method, the average voltage stays bounded around $48\,\mathrm{V}$ and the tight voltage regulation is maintained for each converter. Fig. 5(c) shows that the supplied currents are properly shared despite the unbounded attacks. These studies verify the effectiveness of the proposed resilient approach in solving Problem 1, i.e., maintaining bounded global voltage regulation and proportional load sharing under unbounded attacks. Moreover, as seen in Fig. 5, the convergence rate is increased by properly increasing γ_i.

To verify the capabilities of the proposed method in handling large attack signals, we run comparative experiments by selecting $\delta_i = 30t,\ \forall i = 1, 2, ..., 8$. The experimental results using the standard and the proposed resilient methods are comparatively illustrated in Fig. 6 and Fig. 7, respectively. Fig. 6 shows that the terminal voltages and the supplied currents, using the standard secondary control, diverge after initiating the large unbounded attack signals and reach the saturation value fairly quickly. Whereas, Fig. 7 shows that the terminal voltages stay bounded around $48\,\mathrm{V}$, and the proportional load sharing is still carried out, using the proposed method, even under fairly large unbounded injections.

D. Performance Assessment under Unknown Bounded Attacks

In this section, we consider the bounded attack signals by selecting $\delta_i = 15,\ \forall i = 1, 2, ..., 8$. The experimental results using the standard method and the proposed resilient method under bounded attack injections are comparatively illustrated in Fig. 8 and Fig. 9, respectively. Fig. 8 shows that the terminal voltages and the supplied currents, using the standard secondary control, stay bounded. The upper bounds for the local voltage and

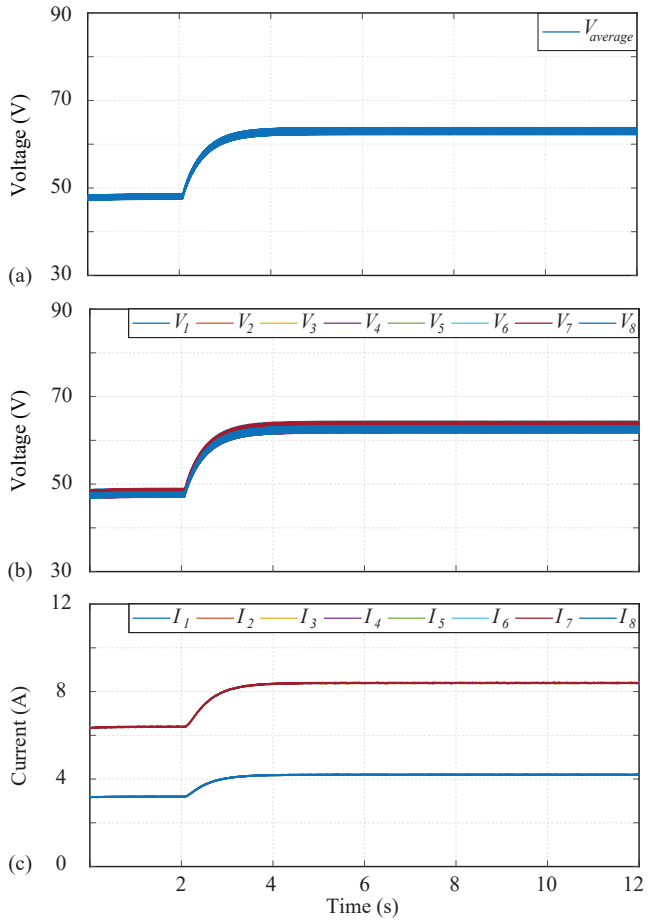

Fig. 8: Performance of the standard secondary control in the case of bounded attack signals $\delta_i = 15$: (a) Average voltage, (b) Terminal voltages, (c) Supplied currents.

current are determined by the values of attack signals. For example, the upper bound for the average voltage is almost $65\,\mathrm{V}$ under the current attack injections. Without implementing the resilient control protocol, the voltage and current performance will further deteriorates under larger attack values. As shown in Fig. 9(a), the average voltage is properly regulated at $48\,\mathrm{V}$, i.e., the adverse effects of bounded attacks are completely compensated. This is also validated by observing the current waveforms in Fig. 9(c).

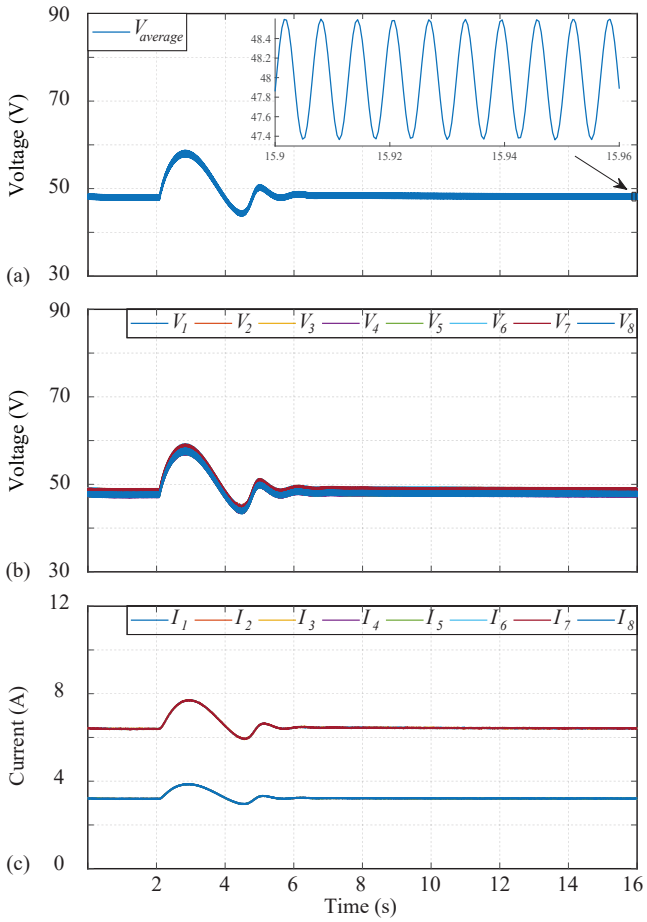

Fig. 9: Performance of the proposed attack-resilient control in the case of bounded attack signals $\delta_i = 15$: (a) Average voltage, (b) Terminal voltages, (c) Supplied currents.

VI. Conclusion

We have formulated the distributed attack-resilient secondary control problems for DC microgrids in the presence of unknown unbounded and bounded attacks, respectively. A fully distributed adaptive control framework has been developed to simultaneously achieve UUB and AS convergence on global voltage regulation and proportional load sharing under unbounded and bounded attacks, respectively. Experimental results and comparisons between the proposed attack-resilient and the standard secondary controllers under unbounded and bounded attacks demonstrate the efficacy of the proposed

approach. The secondary voltage and frequency restorations of AC microgrids can be formulated as a consensus problem of first-order linear MAS [42]–[45], similar to the formulation used here for the secondary control of DC microgrid. The proposed attack-resilient control approach can then be extended to the secondary control of AC microgrids against malicious unbounded or bounded attacks.

ACKNOWLEDGMENT

The authors sincerely thank Dr. O. A. Beg and Dr. D. Pullaguram for their help in initial setup of experiments and graphics.

REFERENCES

[1] A. Kwasinski, "Quantitative evaluation of dc microgrids availability: Effects of system architecture and converter topology design choices," *IEEE Transactions on Power Electronics*, vol. 26, no. 3, pp. 835–851, March 2011.

[2] Y. Gu, X. Xiang, W. Li, and X. He, "Mode-adaptive decentralized control for renewable dc microgrid with enhanced reliability and flexibility," *IEEE Transactions on Power Electronics*, vol. 29, no. 9, pp. 5072–5080, September 2014.

[3] A. Kwasinski and C. N. Onwuchekwa, "Dynamic behavior and stabilization of dc microgrids with instantaneous constant-power loads," *IEEE Transactions on Power Electronics*, vol. 26, no. 3, pp. 822–834, March 2011.

[4] J. M. Guerrero, J. C. Vasquez, J. Matas, L. G. de Vicuna, and M. Castilla, "Hierarchical control of droop-controlled ac and dc microgrids—a general approach toward standardization," *IEEE Transactions on Industrial Electronics*, vol. 58, no. 1, pp. 158–172, January 2011.

[5] T. Dragičević, X. Lu, J. C. Vasquez, and J. M. Guerrero, "Dc microgrids—part i: A review of control strategies and stabilization techniques," *IEEE Transactions on Power Electronics*, vol. 31, no. 7, pp. 4876–4891, July 2016.

[6] S. Anand, B. G. Fernandes, and J. Guerrero, "Distributed control to ensure proportional load sharing and improve voltage regulation in low-voltage dc microgrids," *IEEE Transactions on Power Electronics*, vol. 28, no. 4, pp. 1900–1913, April 2013.

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

[8] P. Wang, X. Lu, X. Yang, W. Wang, and D. Xu, "An improved distributed secondary control method for dc microgrids with enhanced dynamic current sharing performance," *IEEE Transactions on Power Electronics*, vol. 31, no. 9, pp. 6658–6673, September 2016.

[9] S. Sahoo and S. Mishra, "A distributed finite-time secondary average voltage regulation and current sharing controller for dc microgrids," *IEEE Transactions on Smart Grid*, vol. 10, no. 1, pp. 282–292, January 2019.

[10] D. Pullaguram, S. Mishra, and N. Senroy, "Event-triggered communication based distributed control scheme for dc microgrid," *IEEE Transactions on Power Systems*, vol. 33, no. 5, pp. 5583–5593, September 2018.

[11] R. Han, L. Meng, J. M. Guerrero, and J. C. Vasquez, "Distributed nonlinear control with event-triggered communication to achieve current-sharing and voltage regulation in dc microgrids," *IEEE Transactions on Power Electronics*, vol. 33, no. 7, pp. 6416–6433, July 2018.

[12] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inf. Syst. Secur.*, vol. 14, no. 1, Jun. 2011.

[13] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 645–658, December 2011.

[14] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, "A review of false data injection attacks against modern power systems," *IEEE Transactions on Smart Grid*, vol. 8, no. 4, pp. 1630–1638, July 2017.

[15] P. A. S. Ralston, J. H. Graham, and J. L. Hieb, "Cyber security risk assessment for scada and dcs networks," *ISA Transactions*, vol. 46, no. 4, pp. 583–594, July 2007.

[16] G. Hug and J. A. Giampapa, "Vulnerability assessment of ac state estimation with respect to false data injection cyber-attacks," *IEEE Transactions on Smart Grid*, vol. 3, no. 3, pp. 1362–1370, September 2012.

[17] J. Liang, L. Sankar, and O. Kosut, "Vulnerability analysis and consequences of false data injection attack on power system state estimation," *IEEE Transactions on Power Systems*, vol. 31, no. 5, pp. 3864–3872, September 2016.

[18] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Transactions on Automatic Control*, vol. 58, no. 11, pp. 2715–2729, November 2013.

[19] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "Distributed fault detection and isolation resilient to network model uncertainties," *IEEE Transactions on Cybernetics*, vol. 44, no. 11, pp. 2024–2037, November 2014.

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

[21] Z. Tang, M. Kuijper, M. S. Chong, I. Mareels, and C. Leckie, "Linear system security—detection and correction of adversarial sensor attacks in the noise-free case," *Automatica*, vol. 101, pp. 53–59, March 2019.

[22] 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 Transactions on Control of Network Systems*, vol. 1, no. 4, pp. 370–379, December 2014.

[23] J. Zhao, G. Zhang, M. La Scala, Z. Y. Dong, C. Chen, and J. Wang, "Short-term state forecasting-aided method for detection of smart grid general false data injection attacks," *IEEE Transactions on Smart Grid*, vol. 8, no. 4, pp. 1580–1590, July 2017.

[24] Y. He, G. J. Mendis, and J. Wei, "Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2505–2516, September 2017.

[25] A. Ashok, M. Govindarasu, and V. Ajjarapu, "Online detection of stealthy false data injection attacks in power system state estimation," *IEEE Transactions on Smart Grid*, vol. 9, no. 3, pp. 1636–1646, May 2018.

[26] O. A. Beg, T. T. Johnson, and A. Davoudi, "Detection of false-data injection attacks in cyber-physical dc microgrids," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 5, pp. 2693–2703, October 2017.

[27] O. A. Beg, L. V. Nguyen, T. T. Johnson, and A. Davoudi, "Signal temporal logic-based attack detection in dc microgrids," *IEEE Transactions on Smart Grid*, vol. 10, no. 4, pp. 3585–3595, July 2019.

[28] S. Sahoo, S. Mishra, J. C. Peng, and T. Dragičević, "A stealth cyber-attack detection strategy for dc microgrids," *IEEE Transactions on Power Electronics*, vol. 34, no. 8, pp. 8162–8174, August 2019.

[29] J. Kim and L. Tong, "On topology attack of a smart grid: Undetectable attacks and countermeasures," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 7, pp. 1294–1305, July 2013.

[30] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, "A review of false data injection attacks against modern power systems," *IEEE Transactions on Smart Grid*, vol. 8, no. 4, pp. 1630–1638, July 2017.

[31] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Transactions on Automatic Control*, vol. 58, no. 11, pp. 2715–2729, November 2013.

[32] E. Arabi, T. Yucelen, and W. M. Haddad, "Mitigating the effects of sensor uncertainties in networked multiagent systems," in *2016 American Control Conference (ACC)*, July 2016, pp. 5545–5550.

[33] G. De La Torre, T. Yucelen, and J. D. Peterson, "Resilient networked multiagent systems: A distributed adaptive control approachy," in *53rd IEEE Conference on Decision and Control*, December 2014, pp. 5367–5372.

[34] C.-H. Xie and G.-H. Yang, "Decentralized adaptive fault-tolerant control for large-scale systems with external disturbances and actuator faults," *Automatica*, vol. 85, pp. 83–90, November 2017.

[35] X. Jin, W. M. Haddad, and T. Yucelen, "An adaptive control architecture for mitigating sensor and actuator attacks in cyber-physical systems," *IEEE Transactions on Automatic Control*, vol. 62, no. 11, pp. 6058–6064, November 2017.

[36] Z. Feng, G. Wen, and G. Hu, "Distributed secure coordinated control for multiagent systems under strategic attacks," *IEEE Transactions on Cybernetics*, vol. 47, no. 5, pp. 1273–1284, May 2017.

[37] S. Abhinav, H. Modares, F. L. Lewis, and A. Davoudi, "Resilient cooperative control of dc microgrids," *IEEE Transactions on Smart Grid*, vol. 10, no. 1, pp. 1083–1085, January 2019.

[38] J. A. Fax and R. M. Murray, "Information flow and cooperative control of vehicle formations," *IEEE Transactions on Automatic Control*, vol. 49, no. 9, pp. 1465–1476, September 2004.

[39] H. K. Khalil, *Nonlinear systems*, 3rd ed. Upper Saddle River, N.J: Prentice Hall, 2002.

[40] *Typhoon HIL 603 Technical Manual*. Somerville, MA, USA: Typhoon HIL, Inc., 2017.

[41] *MicroLabBox Product Information*. Paderborn, Germany: dSPACE GmbH, 2017.

[42] A. Bidram, A. Davoudi, and F. L. Lewis, "A multiobjective distributed control framework for islanded ac microgrids," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 3, pp. 1785–1798, August 2014.

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

[44] F. Guo, C. Wen, J. Mao, and Y. Song, "Distributed secondary voltage and frequency restoration control of droop-controlled inverter-based microgrids," *IEEE Transactions on Industrial Electronics*, vol. 62, no. 7, pp. 4355–4364, July 2015.

[45] S. Zuo, A. Davoudi, Y. Song, and F. L. Lewis, "Distributed finite-time voltage and frequency restoration in islanded ac microgrids," *IEEE Transactions on Industrial Electronics*, vol. 63, no. 10, pp. 5988–5997, October 2016.

CHAPTER 5

RESILIENT AC MICROGRIDS AGAINST CORRELATED ATTACKS[1]

Authors: Shan Zuo, Deepak Pullaguram, Frank L. Lewis, and Ali Davoudi.

Reprinted, with permission from all the co-authors.

(Under Preparation)

[1]Used with permission of all the co-authors, 2020.

Resilient AC Microgrids against Correlated Attacks

Shan Zuo, Deepak Pullaguram, *Member, IEEE*, Frank L. Lewis, *Life Fellow, IEEE*, and Ali Davoudi, *Senior Member, IEEE*

Abstract

Multi-inverter AC microgrids increasingly rely on local embedded controllers and distributed communication networks to meet operational requirements, which make the microgrids vulnerable to physical and cyber attacks. Conventional resilient control strategies generally assume that the attack signals are bounded and uncorrelated. In this paper, we study the ramifications of allowing the antagonistic inputs to be unbounded and correlated. We consider a two-layer hierarchy for a networked multi-agent system with opposing teams on two different directed communication graphs: a control protagonist team with cooperative multi-inverter microgrids and an attack antagonist team with interacting attackers. Concerted malicious behaviors can bypass the standard attack-detection methods and undermine the cooperative performance and even system stability. We propose a fully distributed control framework that is resilient to external correlated sensor attacks from interacting antagonists, as well as unknown unbounded attacks on actuator commands and communication channels. The proposed distributed control framework guarantees uniform ultimate boundedness for the secondary frequency regulation and voltage containment of AC microgrids. The proposed

This work was supported, in part, by the ONR grant N00014-17-1-2239. D. Pullaguram was supported by The University of Texas at Arlington.

S. Zuo, F. L. Lewis, and A. Davoudi are with the Electrical Engineering Department, The University of Texas at Arlington, TX 76019, USA (e-mail: shan.zuo@uta.edu; lewis@uta.edu; davoudi@uta.edu). D. Pullaguram was with The University of Texas at Arlington. He is currently with the National Institute of Technology, Warangal, India (email: drp@nitw.ac.in).

results are validated on a modified IEEE 34-bus test feeder system, which is emulated in a controller/hardware-in-the-loop environment.

Index Terms

Attack-resilient control, correlated attacks, containment, inverters, microgrids, regulation, unbounded attacks.

I. Introduction

Multi-inverter AC microgrid systems increasingly rely on distributed control paradigms with information exchanged among local controllers of inverters on a sparse communication network [1]–[3]. Multi-agent consensus and containment results are employed to reach frequency regulation [4] and voltage containment [5], respectively. The communication network among inverters poses a security vulnerability [6], [7], particularly as individual inverters lack the global perspective with limited information from their neighbors. Malicious attackers could simultaneously launch attacks, at times in a coordinated fashion, on the sensors, actuators, or communication channels to undermine microgrid performance and even its stability. It is, therefore, necessary to seek reliable and secure remedies against malicious attacks.

The first approach to address attacks on microgrids is to detect the compromised inverters [8]–[10]. One could then remove the compromised inverters. This could undermine the graphical connectivity, and jeopardize the consensus protocol fundamental to distributed control approaches. Hence, a restriction on communication graph connectivity is generally required. Alternatively, distributed resilient control protocols preserve an acceptable level of performance by mitigating the propagated impact of external disturbances [11]–[15]. The main idea is to devise local distributed control approaches to enhance the self-resilience of the microgrids against malicious attacks, instead of removing the corrupted agents.

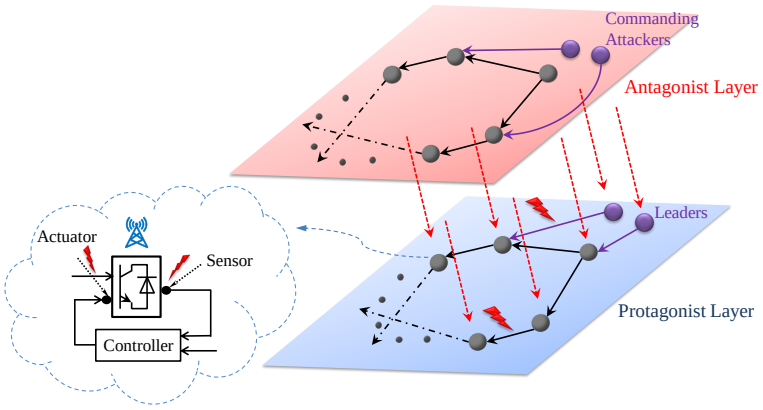

Fig. 1: A two-layer networked MAS hierarchy with two opposing teams: a control protagonist layer consisting of networked multi-inverter AC microgrid and an attack antagonist layer.

With very few exceptions, e.g., [16], existing distributed resilient control methods for microgrids mostly deal with bounded injections. This may not be practical since the real-world attack injections can be purposely devised to undermine their target to the maximum extent and, hence, cannot be assumed bounded [17]. Moreover, the conventional attack-detection methods usually worked well for independent and non-interacting bad measurements. The malicious and intelligent attackers may launch simultaneous and coordinated attacks to introduce correlated errors into system states while successfully bypassing some detection techniques [18], [19]. The vulnerability assessment of such unobservable correlated attack injections, in the context of state estimations in power system, has already been studied [20]–[22]. For microgrids that could be deployed in mission-critical applications, local resilient control protocols are urgently needed to deal with intelligently interacting attack injections and/or general unbounded attack signals.

In this paper, we consider the simultaneous and coordinated attacks to the multi-inverter microgrids, where the correlation among sensor attacks is formulated using a layer of communication network. In particular, we consider a two-layer networked multi-agent systems (MAS) hierarchy with two opposing players, a control protagonist team of networked cooperative multi-inverters and a coordinated attack antagonist team,

on two different communication digraphs, as illustrated in Fig. 1. The antagonists are modeled as rational decision makers in the sense that their decisions on sensor attack injections to the protagonist layer are made in a real-time and feedback manner, being highly correlated with each other and following two unbounded commanding antagonists. Moreover, the malicious attackers could launch general unbounded attacks on the communication channels and input control signals of individual inverters. These could severely deteriorate, and even destabilize, the synchronization mechanism of the AC microgrid system. Note that although the unbounded attacks can be detected, isolating compromised agents under such simultaneous and coordinated attacks could easily lead to communication network failure. In this regard, the local resilient controller design makes the microgrid self-resilient to such attacks without the need to detect and isolate the compromised agents. There are two main contributions in this paper:

- A two-layer networked MAS hierarchy is introduced, consisting of the control protagonist team with cooperative multi-inverter microgrid and the antagonist team with interacting attackers. We consider three kinds of unbounded injections launched from the antagonist layer, i.e., attack injections on the communication links among inverters and/or between the inverters and leaders, actuator attacks on the control input signals of local inverters, and the correlated attacks on the sensor measurements.
- A distributed resilient secondary control framework mitigates the effect of unbounded attacks. By analyzing the resulting performance and overall closed-loop system stability, this method is refined to guarantee the uniformly ultimately bounded (UUB) convergence for both frequency regulation and voltage containment, without the need for any global information.
- The proposed attack-resilient control framework is validated by experimental results in a controller/hardware-in-the-loop (CHIL) setup for AC microgrids to show resilience in different attack scenarios.

The remainder of this paper is organized as follows: Section II offers preliminaries on graph theory, communication network, and notations used. Section III presents the conventional cooperative secondary control protocols for AC microgrids. Section IV introduces the unbounded attack models and formulates the resilient secondary control problem for AC microgrids. The distributed resilient controller design is presented in Section V and verified in Section VI using a CHIL setup. The conclusion is drawn in Section VII.

II. PRELIMINARIES

Graph theory: Suppose that the interactions among the multi-inverter protagonist layer and the antagonist layer are represented by time-invariant weighted digraphs $\mathscr{G}_p$ and $\mathscr{G}_a$, respectively. $\mathscr{G}_p = (\mathcal{V}_p, \mathcal{E}_p, \mathcal{A}_p)$ (respectively, $\mathscr{G}_a = (\mathcal{V}_a, \mathcal{E}_a, \mathcal{A}_a)$) with a finite set of N nodes $\mathcal{V}_p = \{v_1^p, v_2^p, \ldots, v_N^p\}$ (respectively, $\mathcal{V}_a = \{v_1^a, v_2^a, \ldots, v_N^a\}$), a set of edges $\mathcal{E}_p \subset \mathcal{V}_p \times \mathcal{V}_p$ (respectively, $\mathcal{E}_a \subset \mathcal{V}_a \times \mathcal{V}_a$), and the associated adjacency matrix $\mathcal{A}_p = [a_{ij}^p] \in \mathbb{R}^{N\times N}$ (respectively, $\mathcal{A}_a = [a_{ij}^a] \in \mathbb{R}^{N\times N}$). a_{ij}^p and a_{ij}^a are the weights of edge (v_{j_p}, v_{i_p}) and (v_{j_a}, v_{i_a}), respectively. $a_{ij}^p > 0$ and $a_{ij}^a > 0$ if $(v_{j_p}, v_{i_p}) \in \mathcal{E}_p$ and $(v_{j_a}, v_{i_a}) \in \mathcal{E}_a$, respectively, otherwise, $a_{ij}^p = 0$ and $a_{ij}^a = 0$. In-degree matrices are shown as $\mathcal{D}_p = \mathrm{diag}(d_i^p) \in \mathbb{R}^{N\times N}$ and $\mathcal{D}_a = \mathrm{diag}(d_i^a) \in \mathbb{R}^{N\times N}$ with $d_i^p = \sum_{j=1}^N a_{ij}^p$ and $d_i^a = \sum_{j=1}^N a_{ij}^a$, respectively. Corresponding Laplacian matrices are $\mathcal{L}^p = \mathcal{D}^p - \mathcal{A}^p$ and $\mathcal{L}^a = \mathcal{D}^a - \mathcal{A}^a$, respectively. $\mathscr{F}$ and $\mathscr{L}$ are used to represent $\{1, 2, ..., N\}$ and $\{N+1, N+2\}$, respectively.

Communication network: There are N inverters and two leader nodes on the protagonist layer $\mathscr{G}_p$. The upper (lower) leader node launches the upper (lower) reference value to the neighboring inverters. Likewise, there are N following attackers and two leading attackers on the antagonist layer $\mathscr{G}_a$. g_{ik}^p is the pinning gain from the (either the upper or the lower) k^{th} leader to the i^{th} inverter on the protagonist layer. Likewise, g_{ik}^a is the one connecting the k^{th} commanding attacker and the i^{th} following attacker

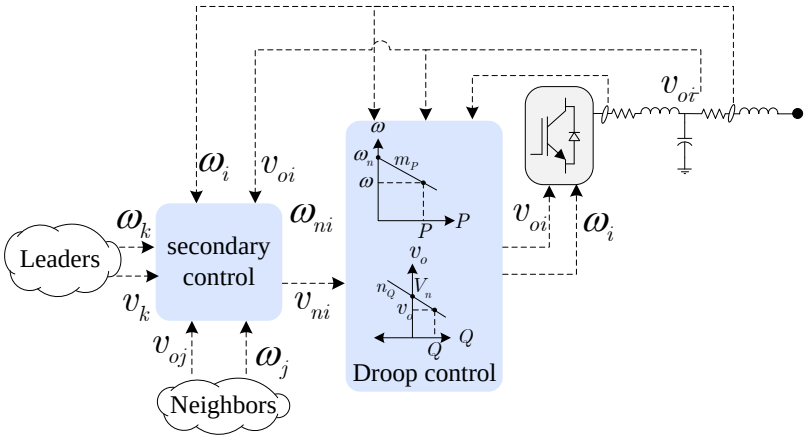

Fig. 2: Hierarchical cooperative control of an inverter.

on the antagonist layer. $g_{ik}^{p} > 0$ (respectively, $g_{ik}^{a} > 0$) for a connection between the k^{th} leader (respectively, k^{th} commanding attacker) and the i^{th} inverter (respectively, i^{th} following attacker); Otherwise, $g_{ik}^{p} = 0$ (respectively, $g_{ik}^{a} = 0$). $\mathcal{G}_k^p = \mathrm{diag}\,(g_{ik}^{p})$ and $\mathcal{G}_k^a = \mathrm{diag}\,(g_{ik}^{a})$. Note that $\mathscr{G}_p$ and $\mathscr{G}_a$ can be different.

Notations: $\sigma_{\min}(X)$ and $\sigma_{\max}(X)$ are the minimum and maximum singular values of matrix X, respectively. $\mathrm{diag}\{\cdot\}$ denotes the block diagonal matrix. The Kronecker product is shown by $\otimes$.

III. Conventional Cooperative Secondary Control

As illustrated in Fig.2, in a hierarchical cooperative control structure for the i^{th} inverter, the secondary control level acts as an actuator and provides the setpoints for the frequency and voltage to the decentralized primary droop control. The $P-\omega$ and $Q-v$ droop characteristics are formulated as

$$\omega_i = \omega_{n_i} - m_{P_i} P_i, \tag{1}$$

$$v_{odi} = V_{n_i} - n_{Q_i} Q_i, \tag{2}$$

where P_i and Q_i are, respectively, the active and reactive powers. ω_i and v_{odi} are the operating angular frequency and the direct component of the terminal voltage. ω_{n_i} and V_{n_i} denote the droop setpoints fed from the secondary controller. m_{P_i} and n_{Q_i} are $P-\omega$ and $Q-v$ droop coefficients selected as per inverter's power ratings.

Differentiating the droop characteristics (1) and (2) gives

$$\dot{\omega}_{ni} = \dot{\omega}_i + m_{P_i}\dot{P}_i = u_{f_i}, \tag{3}$$

$$\dot{V}_{ni} = \dot{v}_{odi} + n_{Q_i}\dot{Q}_i = u_{v_i}, \tag{4}$$

where u_{f_i} and u_{v_i} are auxiliary control inputs. The distributed leader-follower containment approach is applied to accomplish the secondary frequency regulation and voltage containment for AC microgrids, by using the relative measurements from the neighboring inverters and leaders. That is,

$$u_{f_i} = c_{fi}\left(\sum_{j\in\mathscr{F}} a_{ij}^p\left(\omega_j-\omega_i\right) + \sum_{k\in\mathscr{L}} g_{ik}^p\left(\omega_k-\omega_i\right) + \sum_{j\in\mathscr{F}} a_{ij}^p\left(m_{P_j}P_j - m_{P_i}P_i\right)\right), \tag{5}$$

$$u_{v_i} = c_{vi}\left(\sum_{j\in\mathscr{F}} a_{ij}^p\left(v_{odj}-v_{odi}\right) + \sum_{k\in\mathscr{L}} g_{ik}^p\left(v_k-v_{odi}\right) + \sum_{j\in\mathscr{F}} a_{ij}^p\left(n_{Q_j}Q_j - n_{Q_i}Q_i\right)\right), \tag{6}$$

where $c_{fi}, c_{vi} \in \mathbb{R} > 0$ are the coupling gains. ω_k and v_k are the frequency and voltage references issued by the k^{th} leader, respectively. To ensure stable microgrid operation, the frequency references for both leaders are set as ω_{ref}. To bound the voltage magnitude in permissible operating limits, the upper and lower voltage leaders are v_{ref}^u and v_{ref}^l, respectively. The setpoints used in the droop control, ω_{ni} and V_{ni}, are then computed from u_{f_i} and u_{v_i} as

$$\omega_{n_i} = \int u_{f_i}\,\mathrm{d}\,t, \tag{7}$$

$$V_{n_i} = \int u_{v_i}\,\mathrm{d}\,t. \tag{8}$$

Using (5) and (6), we rewrite (3) and (4) as

$$\dot{\omega}_{n_i} = c_{fi}\left(\sum_{j\in\mathscr{F}} a_{ij}^{p}\left(\omega_{n_j}-\omega_{n_i}\right)+\sum_{k\in\mathscr{L}} g_{ik}^{p}\left(\omega_{n_k}-\omega_{n_i}\right)\right), \tag{9}$$

$$\dot{V}_{n_i} = c_{vi}\left(\sum_{j\in\mathscr{F}} a_{ij}^{p}\left(V_{n_j}-V_{n_i}\right)+\sum_{k\in\mathscr{L}} g_{ik}^{p}\left(V_{n_k}-V_{n_i}\right)\right), \tag{10}$$

respectively, where $\omega_{n_k} = \omega_k + m_{P_i}P_i$ and $V_{n_k} = v_k + n_{Q_i}Q_i$. Due to the coupling between active power (respectively, reactive power) of each inverter and its angular frequency (respectively, voltage magnitude), the control protocols (9) and (10) ensure the synchronization of the local frequency and voltage in the steady state [4]. Thus, to synchronize both ω_i and $m_{P_i}P_i$ (respectively, v_{odi} and $n_{Q_i}Q_i$), we can directly synchronize ω_{n_i} (respectively, V_{n_i}).

Next, we give the preliminaries on secondary voltage containment control with two leaders. Similar discussion can be applied in the context of the secondary frequency control. For convenience, we denote V_{n_i} as V_i hereafter.

***Definition* 1 *(Voltage Containment Control Objective)*:** The objective of the secondary voltage containment control is to make the local voltage of each inverter converge to the range of the two constant voltage references issued by the leaders, i.e., $\left\{\left[V_{\text{ref}}^{l}, V_{\text{ref}}^{u}\right]\right\}$.

Define

$$\Phi_k^p = \frac{1}{2}\mathcal{L}^p + \mathcal{G}_k^p. \tag{11}$$

Note that $\mathcal{L}^p\left(\mathbf{1}_N \otimes V_k\right) = \left(\mathcal{D}^p - \mathcal{A}^p\right)\left(\mathbf{1}_N \otimes V_k\right) = 0$. Then, the global form of (10) becomes

$$\dot{V} = -c_v \sum_{k\in\mathscr{L}} \Phi_k^p \left(V - \mathbf{1}_N \otimes V_k\right), \tag{12}$$

where $V = [V_1^T, ..., V_N^T]^T$ and $c_v = \operatorname{diag}\left(c_{vi}\right)$. We then introduce the following global

voltage containment error

$$e_v = V - \left(\sum_{r\in\mathscr{L}} \Phi_r^p\right)^{-1} \sum_{k\in\mathscr{L}} \Phi_k^p \left(\mathbf{1}_N \otimes V_k\right). \tag{13}$$

***Assumption* 1:** There exists a directed path from (at least) one leader to each inverter on the protagonist layer $\mathscr{G}_p$. Moreover, $d_i^p > 0$ for each inverter, i.e., there exists (at least) one neighbor for the i^{th} inverter.

***Lemma* 1 ([23]):** Under Assumption 1, $\sum_{k\in\mathscr{L}} \Phi_k^p$ is non-singular and positive-definite. Moreover, the voltage containment control objective is attained if $\lim_{t\to\infty} e_v\left(t\right) = 0$.

IV. Unbounded Attack Modeling and the Formulation of Attack Resiliency

Since frequency regulation with a single reference value is a special case of voltage containment with two reference values, for brevity, we only present the problem formulation and convergence results of the secondary voltage control in the following.

A. Modeling the Unbounded Attacks

We consider a two-layer networked MAS hierarchy with two opposing teams, where the malicious attackers lie on an antagonist layer, and the cooperative inverters lie on a protagonist layer, as depicted in Fig. 1. Local inverter confronts correlated sensor attacks injected from the corresponding antagonist. Moreover, the malicious attackers launch general unbounded signals to corrupt the communication channels and the control input channels of local inverters.

The antagonists are rational and try to deteriorate the performance of the AC microgrids by following two unbounded commanding attackers and launching the coordinated sensor attacks to bypass existing bad data detection schemes. It should be noted that our

proposed method can deal with any linear/nonlinear antagonist layer for sensor attacks with consensus-based interaction dynamics. For convenience, we give the following illustrative and simplified dynamics for the i^{th} attacker

$$\dot{\delta}_i^s = \sum_{j\in\mathscr{F}} a_{ij}^a \left(\delta_j^s - \delta_i^s\right) + \sum_{k\in\mathscr{L}} g_{ik}^a \left(\delta_k^s - \delta_i^s\right), \tag{14}$$

where $\delta_i^s \in \mathbb{R}$ and $\delta_k^s \in \mathbb{R}$ are the states of the i^{th} following attacker and the k^{th} commanding attacker, respectively. $\delta_k^s(t)$ can be any unbounded signals satisfying bounded $\dot{\delta}_k^s(t)$. It is seen that the decision on sensor attack injection of each following attacker is made in a real-time and feedback manner, and highly correlated with the neighboring attackers.

We consider three kinds of unbounded attack injections launched from the antagonist layer, namely, correlated attacks to the sensors, general unbounded attacks to the communication channels, and the control input channels. Hence, (10) under attacks becomes

$$\dot{V}_i = c_{vi}\left(\sum_{j\in\mathscr{F}} a_{ij}^p \left(\bar{V}_{i,j} - \bar{V}_i\right) + \sum_{k\in\mathscr{L}} g_{ik}^p \left(\bar{V}_{i,k} - \bar{V}_i\right)\right) + \delta_i^a, \tag{15}$$

where $\bar{V}_i$ denotes the corrupted sensor measurement of V_i. $\bar{V}_{i,j}$ and $\bar{V}_{i,k}$ are the compromised delivered measurements of $\bar{V}_j$ and $\bar{V}_k$ at the i^{th} inverter, respectively. In particular, we describe these compromised measurements as

$$\begin{cases} \bar{V}_i = V_i + \delta_i^s, \\ \bar{V}_k = V_k + \delta_k^s, \\ \bar{V}_{i,j} = \bar{V}_j + \delta_{ij}^c, \\ \bar{V}_{i,k} = \bar{V}_k + \delta_{ik}^c, \end{cases} \tag{16}$$

where δ_i^s and δ_k^s denote the sensor attack at the i^{th} inverter and the k^{th} leader, respectively. δ_{ij}^c denotes the injection to the communication link from the j^{th} inverter to the

i^{th} inverter, and δ_{ik}^{c} denotes the communication channel attack from the k^{th} leader to the i^{th} inverter. It is seen that the attackers can launch unbounded attacks on the AC microgrid system by corrupting the local sensor measurements as reflected in δ_{i}^{s} and δ_{k}^{s} (sensor attack), intercepting the communication channels as shown in δ_{ij}^{c} and δ_{ik}^{c} (communication channel attack), and distorting the local input control signal as shown in δ_{i}^{a} (actuator attack).

***Assumption* 2:** $\dot{\delta}_{i}^{a}$, $\dot{\delta}_{ij}^{c}$, and $\dot{\delta}_{ik}^{c}$ are bounded.

***Remark* 1:** The attackers might have limited energy to inject attack signals into the microgrid. The signals with excessively fast-varying values could be easily detected. Hence, one can suppose that Assumption 2 holds.

B. Attack-resilient Problem Formulation

We first analyze the synchronization performance for the antagonist layer. Define the global synchronization error on the antagonist layer as

$$\eta = \delta^{s} - \left(\sum_{r\in\mathscr{L}} \Phi_{r}^{a}\right)^{-1} \sum_{k\in\mathscr{L}} \Phi_{k}^{a}\left(\mathbf{1}_{N}\otimes \delta_{k}^{s}\right), \tag{17}$$

where $\eta = [\eta_{1}^{T},...,\eta_{N}^{T}]^{T}$, $\delta^{s} = [\delta_{1}^{s^{T}},...,\delta_{N}^{s}{}^{T}]^{T}$, and $\Phi_{k}^{a} = \frac{1}{2}\mathcal{L}^{a} + \mathcal{G}_{k}^{a}$. The following technical result is needed.

***Lemma* 2:** Consider the dynamic system

$$\dot{x}\left(t\right) = Ax\left(t\right) + \mu\left(t\right), \tag{18}$$

where $x\left(t\right) \in \mathbb{R}^{N}$, $A \in \mathbb{R}^{N\times N}$ is Hurwitz, and $\mu\left(t\right) \in \mathbb{R}^{N}$ is bounded and piecewise continuous for all $t \geq t_{0}$. Then, for any $x\left(t_{0}\right)$, $x\left(t\right)$ is bounded.

Proof: Since A is Hurwitz, for any $M = M^{T} \succ 0$, there exists $P = P^{T} \succ 0$ such that $PA + A^{T}P = -M$. One can pick the following Lyapunov function candidate

$$V = x^{T}Px \geq 0, \tag{19}$$

where its time-derivative is given as

$$\dot{V} = -x^T M x + 2x^T P \mu. \tag{20}$$

Using Sylvester's inequality, $\forall \|x\| \geq \frac{\sigma_{\max}(P)\|\mu\|}{\sigma_{\min}(M)}$, we obtain

$$\dot{V} \leq -\sigma_{\min}(M) \|x\|^2 + \sigma_{\max}(P) \|x\| \|\mu\| \leq 0. \tag{21}$$

Since μ is bounded, from the LaSalle's invariance principle [24], x is bounded by $\frac{\sigma_{\max}(P)\|\mu\|}{\sigma_{\min}(M)}$. ■

***Lemma* 3:** Consider the attackers' dynamics in (14). Then, the sensor attack δ_i^s in (16) is unbounded if there is a directed path from at least one commanding attacker to the i^{th} following attacker on the antagonist layer.

Proof: Use (14) to obtain

$$\dot{\delta}^s = -\sum_{k\in\mathscr{L}} \Phi_k^a \left(\delta^s - \mathbf{1}_N \otimes \delta_k^s\right) = -\left(\sum_{k\in\mathscr{L}} \Phi_k^a\right) \eta. \tag{22}$$

Use (17) and (22) to obtain

$$\dot{\eta} = -\left(\sum_{k\in\mathscr{L}} \Phi_k^a\right) \eta - \left(\sum_{r\in\mathscr{L}} \Phi_r^a\right)^{-1} \sum_{k\in\mathscr{L}} \Phi_k^a \left(\mathbf{1}_N \otimes \dot{\delta}_k^s\right). \tag{23}$$

Using Lemma 1, we similarly obtain that $\sum_{k\in\mathscr{L}} \Phi_k^a$ is positive-definite, hence $-\left(\sum_{k\in\mathscr{L}} \Phi_k^a\right)$ is Hurwitz. Using Lemma 2, the global synchronization error η in (17) is UUB. Hence, we obtain that δ_i^s stays in the small neighborhood around the range spanned by δ_k^s. Since δ_k^s is unbounded, δ_i^s is also unbounded. This completes the proof. ■

Next, we present the vulnerability assessment of the conventional secondary voltage control under unbounded and correlated attacks, and then introduce the resilient voltage containment problem.

Rewrite (15) as

$$\begin{aligned}\dot{V}_i &= c_{vi}\left(\sum_{j\in\mathscr{F}} a_{ij}^p\left(\bar{V}_{i,j}-\bar{V}_i\right)+\sum_{k\in\mathscr{L}} g_{ik}^p\left(\bar{V}_{i,k}-\bar{V}_i\right)\right)+\delta_i^a \\ &= c_{vi}\left(\sum_{j\in\mathscr{F}} a_{ij}^p\left(V_j-V_i\right)+\sum_{k\in\mathscr{L}} g_{ik}^p\left(V_k-V_i\right)\right)+\varpi_i,\end{aligned} \tag{24}$$

where

$$\varpi_i = c_{vi}\left(\sum_{j\in\mathscr{F}} a_{ij}^p\left(\delta_j^s+\delta_{ij}^c-\delta_i^s\right)+\sum_{k\in\mathscr{L}} g_{ik}^p\left(\delta_k^s+\delta_{ik}^c-\delta_i^s\right)\right)+\delta_i^a, \tag{25}$$

which can be considered as the overall attack information gathered at the i^{th} inverter due to the network propagation. Since δ_i^s, δ_k^s, δ_{ij}^c, δ_{ik}^c, and δ_i^a are unbounded, the conventional secondary control fails in maintaining the system stability and achieving the voltage regulation. It is necessary to design a secure and attack-resilient control method to guarantee the closed-loop stability and voltage containment performance. The following result is needed to formulate our problem.

***Definition* 2 ([25]):** Signal $x(t)$ is UUB with the ultimate bound $b>0$ if there exists a constant $c>0$, independent of $t_0\geq 0$, and for every $a\in(0,c)$, there exists $\tau=\tau(a,b)\geq 0$, independent of t_0, such that $\|x(t_0)\|\leq a \;\Rightarrow\; \|x(t)\|\leq b,\;\; \forall t\geq t_0+\tau$.

The resilient voltage containment problem is then introduced.

***Definition* 3 *(Resilient Voltage Containment Problem)*:** Consider a two-layer hierarchical communication network. The resilient voltage containment problem is to design local input u_{v_i} in (4) such that e_v in (13) is UUB under the unbounded actuator and communication channel attacks and the correlated sensor attacks described in (15) and (16). That is, the local voltage term converges within a small neighborhood around the range of the two voltage references. ■

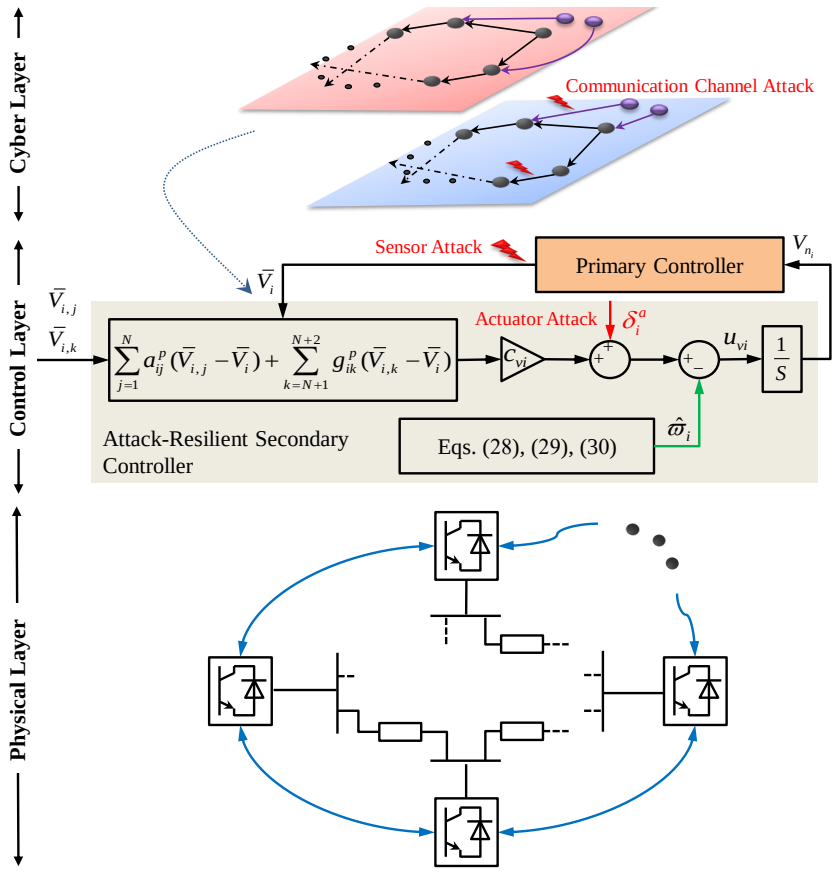

Fig. 3: Cyber-physical AC microgrids: Cyber layer with two hierarchical communication networks, control layer including the primary control and the attack-resilient secondary voltage containment control, and the physical layer including inverters, distribution lines, and sources/loads. The attack-resilient secondary frequency regulation is also considered, but not shown here.

V. Fully Distributed Resilient Design

Consider the following measurable error term

$$\theta_i = \bar{V}_i - \hat{V}_i - \hat{\delta}_i^s, \tag{26}$$

where $\hat{V}_i$ is the estimation of the uncorrupted voltage term, $\hat{\delta}_i^s$ is the estimation of the sensor attack. To cope with the correlated sensor attacks and unbounded actuator and communication channel attacks, we present the following overall attack-resilient control

framework

$$\dot{V}_i = c_{vi}\left(\sum_{j\in\mathscr{F}} a_{ij}^p(\bar{V}_{i,j}-\bar{V}_i)+\sum_{k\in\mathscr{L}} g_{ik}^p(\bar{V}_{i,k}-\bar{V}_i)\right)+\delta_i^a-\hat{\varpi}_i, \tag{27}$$

$$\dot{\hat{V}}_i = c_{vi}\left(\sum_{j\in\mathscr{F}} a_{ij}^p(\hat{V}_j-\hat{V}_i)+\sum_{k\in\mathscr{L}} g_{ik}^p(V_k-\hat{V}_i)\right)+\theta_i, \tag{28}$$

$$\dot{\hat{\delta}}_i^s = c_{vi}\sum_{j\in\mathscr{F}} a_{ij}^p\left(\bar{V}_j-\hat{V}_j-\hat{\delta}_i^s\right), \tag{29}$$

$$\begin{aligned}\dot{\hat{\varpi}}_i = -c_{vi}\Bigg(&\sum_{j\in\mathscr{F}} a_{ij}^p\left(\left(\bar{V}_j-\hat{V}_j\right)-\left(\bar{V}_i-\hat{V}_i\right)\right)+\\ &\sum_{k\in\mathscr{L}} g_{ik}^p\left(\left(\bar{V}_k-V_k\right)-\left(\bar{V}_i-\hat{V}_i\right)\right)\Bigg),\end{aligned} \tag{30}$$

where $\hat{\varpi}_i$ is the estimate of ϖ_i in (25). The observers (28), (29), and (30) serve to compute the compensational signal $\hat{\varpi}_i$ to be used in (27).

Figure 3 shows the cyber-physical layer of the AC microgrids, where the proposed distributed resilient voltage containment control framework is also illustrated. A cyber layer with two opposing hierarchical communication networks is spanned among inverters. The sensor and actuator channels on the multi-inverter protagonist layer are attacked by the malicious antagonist layer.

Define the following global containment error of the voltage estimation

$$\hat{e}_v = \hat{V}-\left(\sum_{r\in\mathscr{L}}\Phi_r^p\right)^{-1}\sum_{k\in\mathscr{L}}\Phi_k^p\left(\mathbf{1}_N\otimes V_k\right), \tag{31}$$

where $\hat{e}_v=[\hat{e}_{v1}^T,...,\hat{e}_{vN}^T]^T$ and $\hat{V}=[\hat{V}_1^T,...,\hat{V}_N^T]^T$.

Next, we analyze the convergence result of the microgrids using the proposed attack-resilient method.

***Theorem* 1:** Given Assumptions 1 and 2, and using the resilient control protocols consisting of (27), (28), (29) and (30), e_v in (13) is UUB, i.e., the attack-resilient voltage containment problem is solved.

***Proof*:** We first study the convergence result of $\hat{V}_i$. Combing (28) and (31) yields

$$\begin{aligned}
\dot{\hat{e}}_v &= \dot{\hat{V}} \\
&= -c_v \left(\sum_{k \in \mathscr{L}} \Phi_k^p \hat{V} - \sum_{k \in \mathscr{L}} \Phi_k^p \left(\mathbf{1}_N \otimes V_k \right) \right) + \theta \\
&= -c_v \left(\sum_{k \in \mathscr{L}} \Phi_k^p \hat{e}_v \right) + \theta.
\end{aligned} \tag{32}$$

From Lemma 1, $-c_v \sum_{k \in \mathscr{L}} \Phi_k^p$ is Hurwitz. Using Lemma 2, we obtain that $\hat{e}_v$ is bounded if θ is bounded. Let $\tilde{V}_i = V_i - \hat{V}_i$. Next, we prove that $\tilde{V}_i$ and θ are both bounded.

Using (25), (27), and (28), and since $\theta_i = \tilde{V}_i + \tilde{\delta}_i^s$, we obtain

$$\begin{aligned}
\dot{\tilde{V}}_i &= \dot{V}_i - \dot{\hat{V}}_i \\
&= c_{vi} \left(\sum_{j \in \mathscr{F}} a_{ij}^p (\tilde{V}_j - \tilde{V}_i) - \sum_{k \in \mathscr{L}} g_{ik}^p \tilde{V}_i \right) - \theta_i + \tilde{\varpi}_i, \\
&= \left(-c_{vi} \left(d_i^p + l_i^p \right) - 1 \right) \tilde{V}_i - \tilde{\delta}_i^s + \tilde{\varpi}_i + c_{vi} \sum_{j \in \mathscr{F}} a_{ij}^p \tilde{V}_j,
\end{aligned} \tag{33}$$

where $l_i^p = \sum_{k \in \mathscr{L}} g_{ik}^p$ and $\tilde{\varpi}_i = \varpi_i - \hat{\varpi}_i$. Let $\tilde{\delta}_i^s = \delta_i^s - \hat{\delta}_i^s$. Combing (14) and (29) yields

$$\begin{aligned}
\dot{\tilde{\delta}}_i^s &= \dot{\delta}_i^s - \dot{\hat{\delta}}_i^s \\
&= \sum_{j \in \mathscr{F}} a_{ij}^a \left(\delta_j^s - \delta_i^s \right) + \sum_{k \in \mathscr{L}} g_{ik}^a \left(\delta_k^s - \delta_i^s \right) \\
&\quad - c_{vi} \sum_{j \in \mathscr{F}} a_{ij}^p \left(\bar{V}_j - \hat{V}_j - \hat{\delta}_i^s \right) \\
&= -c_{vi} \sum_{j \in \mathscr{F}} a_{ij}^p \left(\tilde{\delta}_i^s + \tilde{V}_j \right) + \Delta_i, \\
&= -c_{vi} \left(d_i^p \tilde{\delta}_i^s + \sum_{j \in \mathscr{F}} a_{ij}^p \tilde{V}_j \right) + \Delta_i,
\end{aligned} \tag{34}$$

where

$$\Delta_i = \sum_{j \in \mathscr{F}} \left(a_{ij}^a - c_{vi} a_{ij}^p \right) \left(\delta_j^s - \delta_i^s \right) + \sum_{k \in \mathscr{L}} g_{ik}^a \left(\delta_k^s - \delta_i^s \right). \tag{35}$$

Use (30) to obtain

$$\begin{aligned} \dot{\tilde{\varpi}}_i &= \dot{\varpi}_i - \dot{\hat{\varpi}}_i \\ &= c_{vi} \left(\sum_{j \in \mathscr{F}} a_{ij}^p \left(\tilde{V}_j - \tilde{V}_i \right) - \sum_{k \in \mathscr{L}} g_{ik}^p \tilde{V} \right) + \Theta_i + \dot{\varpi}_i, \\ &= -c_{vi} \left(\left(d_i^p + l_i^p \right) \tilde{V}_i - \sum_{j \in \mathscr{F}} a_{ij}^p \tilde{V}_j \right) + \Theta_i, \end{aligned} \tag{36}$$

where

$$\Theta_i = c_{vi} \left(\sum_{j \in \mathscr{F}} a_{ij}^p \left(\delta_j^s - \delta_i^s \right) + \sum_{k \in \mathscr{L}} g_{ik}^p \left(\delta_k^s - \delta_i^s \right) \right) + \dot{\varpi}_i. \tag{37}$$

Let $\xi_i = \begin{bmatrix} \tilde{\delta}_i^s \\ \tilde{V}_i \\ \tilde{\varpi}_i \end{bmatrix}$. Use (33), (34), and (36) to obtain

$$\begin{aligned} \dot{\xi}_i = & \begin{bmatrix} -c_{vi} d_i^p & 0 & 0 \\ -1 & -c_{vi} \left(d_i^p + l_i^p \right) - 1 & 1 \\ 0 & -c_{vi} \left(d_i^p + l_i^p \right) & 0 \end{bmatrix} \xi_i + \\ & c_{vi} \begin{bmatrix} -1 \\ 1 \\ 1 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 \end{bmatrix} \sum_{j \in \mathscr{F}} a_{ij}^p \xi_j + \begin{bmatrix} \Delta_i \\ 0 \\ \Theta_i \end{bmatrix} \\ & \equiv A_i \xi_i + \gamma_i, \end{aligned} \tag{38}$$

where

$$\gamma_i = c_{vi} \begin{bmatrix} -1 & 1 & 1 \end{bmatrix}^T \begin{bmatrix} 0 & 1 & 0 \end{bmatrix} \sum_{j \in \mathscr{F}} a_{ij}^p \xi_j + \begin{bmatrix} \Delta_i^T & 0 & \Theta_i^T \end{bmatrix}^T, \tag{39}$$

and

$$A_i = \begin{bmatrix} -c_{vi}d_i^p & 0 & 0 \\ -1 & -c_{vi}\left(d_i^p + l_i^p\right) - 1 & 1 \\ 0 & -c_{vi}\left(d_i^p + l_i^p\right) & 0 \end{bmatrix}. \tag{40}$$

From Lemma 3 and Assumption 2, Δ_i and Θ_i are bounded. For inverter i, consider γ_i as a bounded disturbance. In the following, we prove that A_i in (40) is Hurwitz. From Assumption 1, one has $-c_{vi}d_i^p < 0$. Let

$$\Pi_i \equiv \begin{bmatrix} -c_{vi}\left(d_i^p + l_i^p\right) - 1 & 1 \\ -c_{vi}\left(d_i^p + l_i^p\right) & 0 \end{bmatrix}. \tag{41}$$

Then, to prove that A_i is Hurwitz, we only need to prove that Π_i is Hurwitz. Introducing $U = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix}$ yields

$$U\Pi_i U^T = \begin{bmatrix} -1 & 0 \\ -c_{vi}\left(d_i^p + l_i^p\right) & -c_{vi}\left(d_i^p + l_i^p\right) \end{bmatrix}, \tag{42}$$

which is Hurwitz. Hence, Π_i is Hurwitz. Furthermore, A_i is Hurwitz. Using Lemma 2, we obtain that ξ_i is bounded. Therefore, $\tilde{V}$ and $\theta_i = \tilde{V}_i + \tilde{\delta}_i^s$ are both bounded. Hence, $\hat{e}_v$ is also bounded. Note that

$$e_v = \tilde{V} + \hat{e}_v. \tag{43}$$

Hence, e_v is also UUB. This completes the proof. ■

VI. Controller/hardware-in-the-loop Evaluation

A. Multi-inverter AC Microgrid Testbed

We evaluate the proposed results on a IEEE 34-bus feeder system, islanded from the bulk grid at bus 800 and modified to include four inverters and two leader references, as shown in Fig. 4. The power distribution network and inverter data are chosen as in

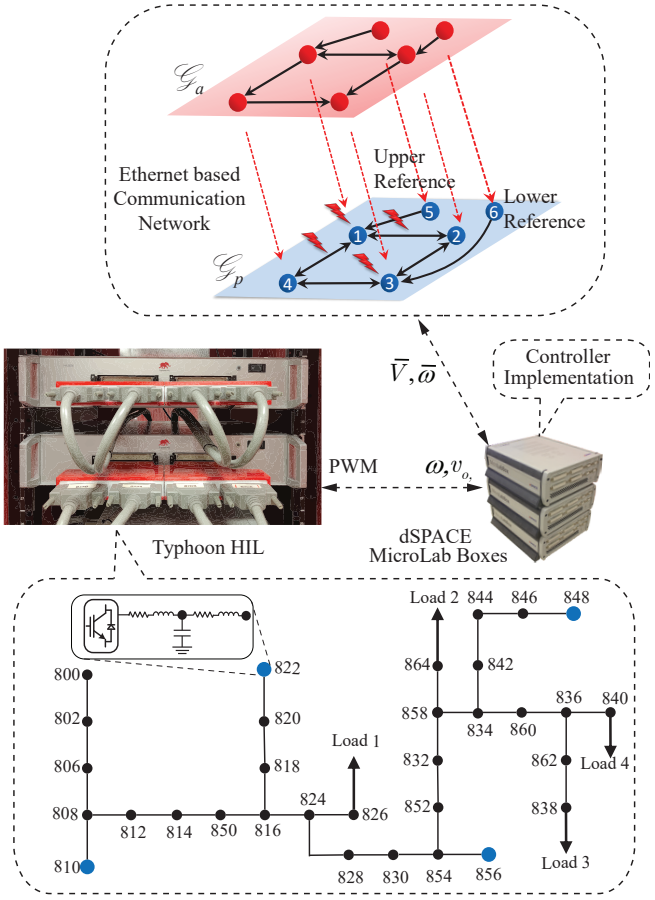

Fig. 4: Physical components are emulated on Typhoon HILs. Distributed controllers are realized on dSPACE systems. The interaction among MLBXs is implemented using Ethernet protocol via local area network.

[26] and [4], respectively, with slight modifications. Each inverter is connected to the feeder lines using a Y-Y, 480 V/24.9 kV, 400 kVA transformer. The nominal reference frequency is $376.99\ rad/s$. All four loads in Fig.4 are 28.3 KVA at 0.707 lagging power factor. The upper and lower voltage setpoints are chosen with the 10% variation from the nominal voltage value. The complete test system shown in Fig. 4 is emulated in two Typhoon HIL 604 units. The proposed attack-resilient secondary control along with the local droop control are deployed on two dSPACE MicroLab Boxes (MLBX) as depicted in Fig. 4. A Netgear ProSAFE Ethernet smart switch handles communication among MLBXs. The bandwidth of the communication channel is 512Kbps.

The adjacency matrix of the four-inverter protagonist layer is $\mathcal{A}_p = [0\ 1\ 0\ 1; 1\ 0\ 1\ 0; 0\ 1\ 0\ 1; 1\ 0\ 1\ 0]$, and the pinning gains are $g_{15}^p = g_{36}^p = 1$. The coupling gains are $c_{fi} = 20$ and $c_{vi} = 10$. As shown in the communication network in Fig. 4, the antagonist layer includes four following attackers and two leading attackers with their dynamics shown in (14), where $\delta_5^s(t) = 0.1t + 5$ and $\delta_6^s(t) = 0.1t + 10$. The adjacency matrix is $\mathcal{A}_a = [0\ 20\ 0\ 0; 20\ 0\ 0\ 0; 0\ 20\ 0\ 20; 20\ 0\ 0\ 0]$ and the pining gains are $g_{15}^a = g_{26}^a = 20$. These attackers issue correlated sensor attacks and general unbounded communication and actuator attacks to the protagonist layer.

B. Attacks on Communication Links

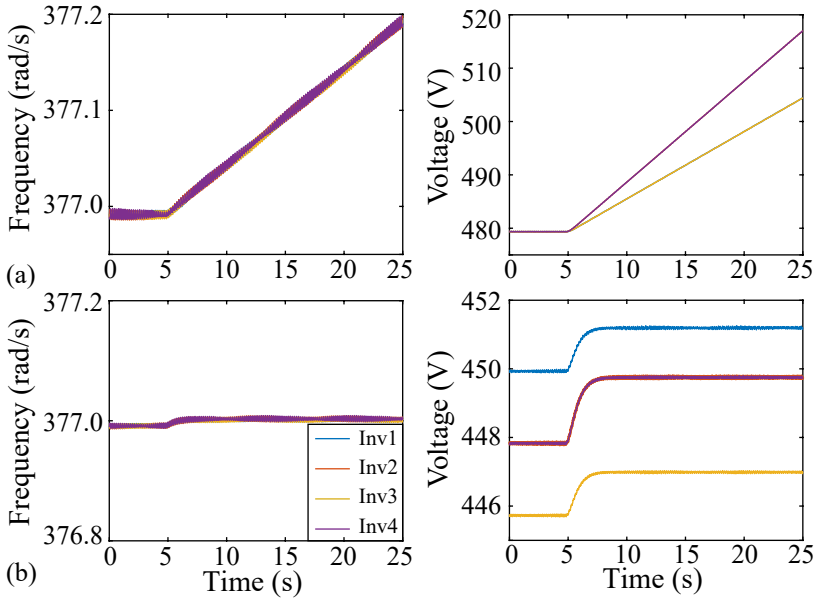

Fig. 5: Inverters' frequency and voltage under communication attack: a) conventional cooperative control, and b) proposed resilient control.

The performance of the resilient controller is compared against the conventional secondary controller under unbounded attacks on communication links. Initially, both controllers are at the steady state, as presented in Fig. 5. The frequency is at its nominal reference value. The voltage of the secondary control was held at the nominal value

whereas, with resilient control, the voltages are held between the upper and lower bounds. At $t = 5s$, an unbounded communication attack took place on communication links $1 \rightarrow 2$ and $1 \rightarrow 4$ with an attack value of $\delta_{21}^c = \delta_{41}^c = 0.01t$ and $\delta_{21}^c = \delta_{41}^c = 1t$ for frequency and voltage signals, respectively. As seen in Fig. 5(a), under the unbounded communication attacks, the conventional secondary controller fails to remain stable. In contrary, the proposed attack-resilient control achieves the UUB regulation on the frequency term and maintains the magnitudes of the bus voltages within a small neighborhood spanned by the upper and lower bounds.

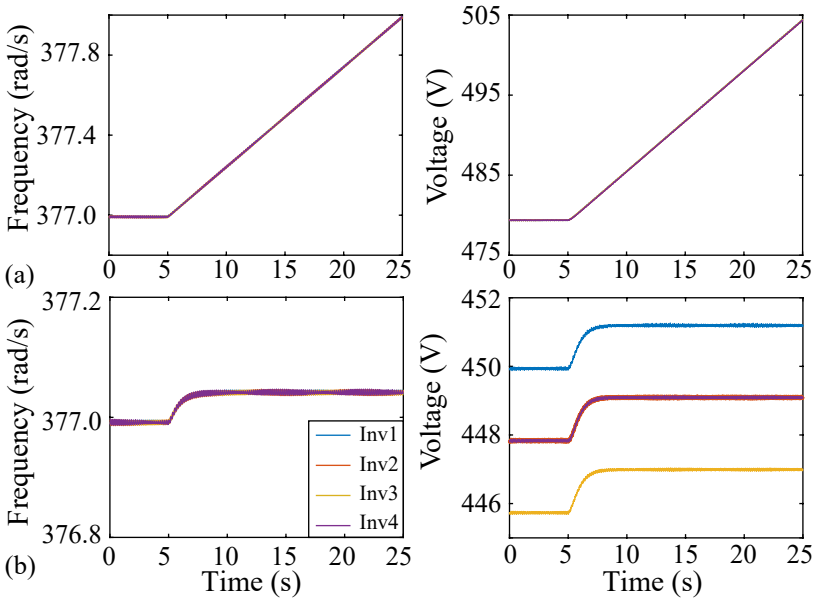

Fig. 6: Inverters' frequency and voltage under actuator attacks: a) conventional cooperative control, and b) proposed resilient control.

C. Attacks on Actuators

The control input signals of inverter 1 and 3 are under unbounded attack injections at $t = 5s$ with $\delta_1^a = \delta_3^a = t$ and $\delta_1^a = \delta_3^c = 10t$ for frequency and voltage signals, respectively. From Fig. 6(a), it is clear that the conventional secondary control is unstable for the actuator attacks whereas the resilient controller maintains the frequency at the

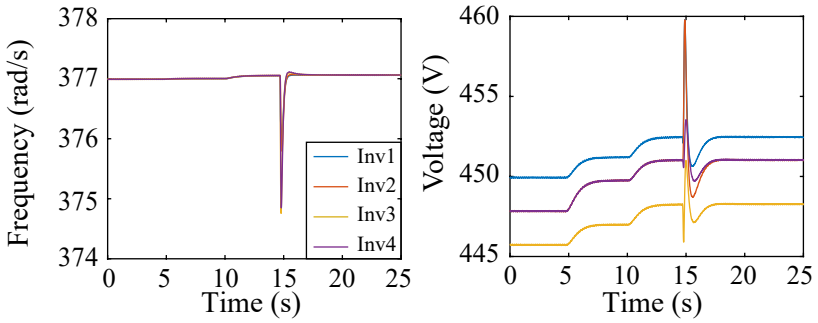

Fig. 7: Inverters' frequency and voltage with the proposed resilient control under communication, actuator, and sensor attacks.

steady value with a very slight deviation from the nominal reference value. Similarly, the voltages are held within a small neighborhood around the upper and lower bounds, as shown in Fig.6(b).

D. Attacks on Communication Lines, Actuators, and Sensors

The resilient controller is evaluated under consecutive attacks on communication, actuators, and sensors. Initially, the inverters are at the steady state employing the resilient control paradigm. The communication link attacks, described in Section VI.B, and the actuator attacks, discussed in Section VI.C, are initiated simultaneously at $t = 5s$. The correlated sensor attacks launched from the antagonist layer are initiated at $t = 15s$ for both frequency and voltage measurements. Fig.7 shows that, even under all these unbounded malicious attacks, the proposed resilient controller guarantees the system stability and achieves the UUB convergence result for both frequency regulation and voltage containment objectives.

VII. Conclusion

We have introduced a two-layer hierarchy for the networked MAS control of AC microgrids with two opposing layers, a multi-inverter protagonist layer and an antagonist layer with interacting attackers. Malicious attackers launch simultaneous and correlated

sensor attacks and general unbounded injections to the communication channels and control input channels of the AC microgrid layer. To maintain microgrid stability and preserve the UUB convergence result for the frequency regulation and voltage containment control objectives, a fully distributed resilient secondary control framework is proposed. The resilience of the proposed control technique has been verified for a modified IEEE feeder system in a CHIL environment.

REFERENCES

[1] Q. Shafiee, V. Nasirian, J. C. Vasquez, J. M. Guerrero, and A. Davoudi, "A multi-functional fully distributed control framework for ac microgrids," *IEEE Transactions on Smart Grid*, vol. 9, no. 4, pp. 3247–3258, July 2018.

[2] X. Wu, C. Shen, and R. Iravani, "A distributed, cooperative frequency and voltage control for microgrids," *IEEE Transactions on Smart Grid*, vol. 9, no. 4, pp. 2764–2776, July 2018.

[3] Y. Khayat, Q. Shafiee, R. Heydari, M. Naderi, T. Dragičević, J. W. Simpson-Porco, F. Dörfler, M. Fathi, F. Blaabjerg, J. M. Guerrero, and H. Bevrani, "On the secondary control architectures of ac microgrids: An overview," *IEEE Transactions on Power Electronics*, vol. 35, no. 6, pp. 6482–6500, June 2020.

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

[5] R. Han, L. Meng, G. Ferrari-Trecate, E. A. A. Coelho, J. C. Vasquez, and J. M. Guerrero, "Containment and consensus-based distributed coordination control to achieve bounded voltage and precise reactive power sharing in islanded ac microgrids," *IEEE Trans. Industry Applications*, vol. 53, no. 6, pp. 5187–5199, Nov. 2017.

[6] M. N. Alam, S. Chakrabarti, and A. Ghosh, "Networked microgrids: State-of-the-art and future perspectives," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 3, pp. 1238–1250, March 2019.

[7] Q. Zhou, M. Shahidehpour, A. Alabdulwahab, and A. Abusorrah, "A cyber-attack resilient distributed control strategy in islanded microgrids," *IEEE Transactions on Smart Grid*, pp. 1–1, 2020.

[8] L. Lu, H. J. Liu, H. Zhu, and C. Chu, "Intrusion detection in distributed frequency control of isolated microgrids," *IEEE Transactions on Smart Grid*, vol. 10, no. 6, pp. 6502–6515, Nov 2019.

[9] A. Mustafa, B. Poudel, A. Bidram, and H. Modares, "Detection and mitigation of data manipulation attacks in ac microgrids," *IEEE Transactions on Smart Grid*, pp. 1–1, 2019.

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

[11] S. Abhinav, I. D. Schizas, F. L. Lewis, and A. Davoudi, "Distributed noise-resilient networked synchrony of active distribution systems," *IEEE Trans. Smart Grid*, vol. 9, no. 2, pp. 836–846, Mar. 2018.

[12] N. M. Dehkordi, H. R. Baghaee, N. Sadati, and J. M. Guerrero, "Distributed noise-resilient secondary voltage and frequency control for islanded microgrids," *IEEE Trans. Smart Grid*, vol. 10, no. 4, pp. 3780–3790, Jul. 2019.

[13] M. A. Shahab, B. Mozafari, S. Soleymani, N. M. Dehkordi, H. M. Shourkaei, and J. M. Guerrero, "Distributed consensus-based fault tolerant control of islanded microgrids," *IEEE Transactions on Smart Grid*, vol. 11, no. 1, pp. 37–47, Jan 2020.

[14] A. Afshari, M. Karrari, H. R. Baghaee, G. B. Gharehpetian, and S. Karrari, "Cooperative fault-tolerant control of microgrids under switching communication topology," *IEEE Transactions on Smart Grid*, doi: 10.1109/TSG.2019.2944768, 2019.

[15] A. Bidram, B. Poudel, L. Damodaran, R. Fierro, and J. M. Guerrero, "Resilient and cybersecure distributed control of inverter-based islanded microgrids," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 3881–3894, June 2020.

[16] S. Zuo, O. A. Beg, F. L. Lewis, and A. Davoudi, "Resilient networked ac microgrids under unbounded cyber attacks," *IEEE Trans. Smart Grid*, doi:10.1109/TSG.2020.2984266, 2020.

[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, Jun. 2014.

[18] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proc. ACM Conf. Comput. Commun. Security*, 2009, pp. 21–32.

[19] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 645–658, Dec. 2011.

[20] G. Hug and J. A. Giampapa, "Vulnerability assessment of ac state estimation with respect to false data injection cyber-attacks," *IEEE Transactions on Smart Grid*, vol. 3, no. 3, pp. 1362–1370, Sep. 2012.

[21] J. Liang, L. Sankar, and O. Kosut, "Vulnerability analysis and consequences of false data injection attack on power system state estimation," *IEEE Transactions on Power Systems*, vol. 31, no. 5, pp. 3864–3872, Sep. 2016.

[22] K. Pan, A. Teixeira, M. Cvetkovic, and P. Palensky, "Cyber risk analysis of combined data attacks against power system state estimation," *IEEE Trans. Smart Grid*, vol. 10, no. 3, pp. 3044–3056, May 2019.

[23] S. Zuo, Y. Song, F. L. Lewis, and A. Davoudi, "Output containment control of linear heterogeneous multi-agent systems using internal model principle," *IEEE Trans. Cybern.*, vol. 47, no. 8, pp. 2099–2109, Aug. 2017.

[24] J. LaSalle, "Some extensions of liapunov's second method," *IRE Trans. Circuit Theory*, vol. 7, no. 4, pp. 520–527, Dec. 1960.

[25] H. K. Khalil, *Nonlinear Systems*. Upper Saddle River, NJ: Prentice Hall, 2002.

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

CHAPTER 6

ADAPTIVE RESILIENT CONTROL OF AC MICROGRIDS UNDER UNBOUNDED ACTUATOR ATTACKS[1]

Authors: Shan Zuo, Frank L. Lewis, and Ali Davoudi.

Reprinted, with permission from all the co-authors.

(Under Preparation)

[1]Used with permission of all the co-authors, 2020.

Adaptive Resilient Control of AC Microgrids under Unbounded Actuator Attacks

Shan Zuo, Frank L. Lewis, *Life Fellow, IEEE*, and

Ali Davoudi, *Senior Member, IEEE*

Abstract

Existing fault-tolerant control and H_∞ control methods for multi-inverter microgrids generally assume bounded faults or disturbances. Herein, we study unknown unbounded attacks on the input channels of both frequency and voltage control loops of inverters that could deteriorate the cooperative performance and affect microgrid stability. We propose a fully distributed control framework using adaptive control techniques that, using stability analysis with Lyapunov techniques, are shown to preserve the uniformly ultimately bounded consensus for frequency regulation and voltage containment, respectively. Moreover, the ultimate bound can be set by adjusting the tuning parameters. The proposed result is validated for a modified IEEE 34-bus test feeder benchmark system augmented with four inverters.

Index Terms

Attacks, containment, inverters, microgrids, resilience.

This work was supported, in part, by the ONR grant N00014-17-1-2239.

S. Zuo, F. L. Lewis, and A. Davoudi are with the Electrical Engineering Department, The University of Texas at Arlington, TX 76019, USA (e-mail: shan.zuo@uta.edu; lewis@uta.edu; davoudi@uta.edu).

I. Introduction

Cooperative control of AC microgrids relies on consensus and containment approaches to accomplish frequency regulation [1] and voltage containment [2], respectively. The communication network among inverters poses security concerns as individual inverters lack the global perspective with limited information exchanged among neighbors [3]–[7]. Some existing methods identify and isolate/overcome the compromised inverters [8]–[13], but would require a number of neighbors to be healthy. Inverter removal could undermine the connectivity of the communication graph and, hence, jeopardize the performance of the cooperative consensus protocol. Alternative distributed resilient control protocols are investigated recently in [14]–[18] to provide self-resilience against external attacks.

Existing resilient protocols for microgrids mainly deal with bounded disturbances, noises, or faults. In practice, malicious attackers could launch unknown unbounded injections to distort cooperative systems [19]. While the conventional detection and overcome/removal method could address such an issue, it, however, mainly handles non-interacting bad measurements [3]. Coordinated attackers could introduce correlated errors into system variables and successfully bypass general bad-data detection techniques [3], [20]–[22]. The impact of such unobservable correlated injections on AC and DC state estimations are studied in [20]–[22]. An attack-resilient control framework, using observer-based techniques, deals with unbounded injections in [2], at the cost of additional communication channels among observers. Alternatively, we explore adaptive techniques to address unknown unbounded attacks on input signals of the control loops, which are referred to as the actuator attacks. We consider the unbounded actuator attacks on both frequency and voltage control loops of an inverter, as illustrated in Fig. 1. These could severely deteriorate, and even destabilize, the synchronization mechanism among microgrid inverters. The contributions of this paper are two-fold:

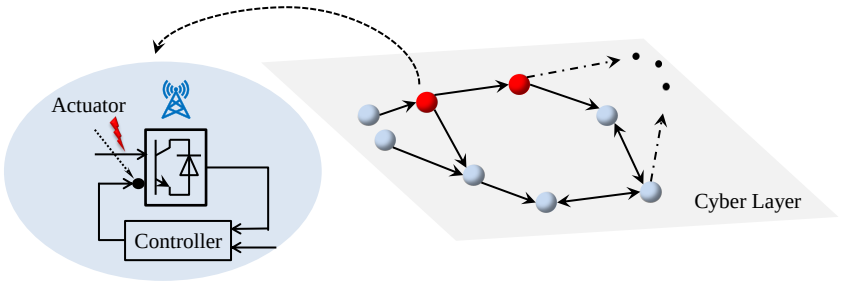

Fig. 1: A networked multi-inverter system under actuator attacks.

• A resilient control method is proposed for both secondary frequency and voltage controls in the face of unknown unbounded actuator attacks. Compared to the observer-based techniques in [2], this control method does not need extra cyber layers for information exchange among observers, offering reduced computational complexity and system vulnerability.

• Stability analysis using Lyapunov techniques show that the proposed method is resilient to unbounded actuator attacks by preserving the uniformly ultimately bounded (UUB) consensus for frequency regulation and voltage containment, respectively. Moreover, the ultimate bound can be set by adjusting the tuning parameters. That is, the frequency and voltage terms can be tuned to converge to an arbitrarily small neighborhood around their respective reference values.

The rest of this paper is organized as follows: Preliminaries on graph theory and notations are given in Section II. Section III reviews the conventional cooperative secondary control of AC microgrids. Section IV formulates the attack-resilient frequency and voltage control problems. Distributed resilient controller design is discussed in Section V. The efficacy of the proposed control method is verified for an AC microgrid in Section VI. Section VII concludes the paper.

II. Preliminaries on Graph Theory and Notations

There are N inverters, with two leader nodes, mapped on a communication network is represented by a time-invariant weighted digraph $\mathscr{G}$. The interactions among the inverters are represented by a subgraph $\mathscr{G}_f$ with the associated adjacency matrix $\mathcal{A} = [a_{ij}] \in \mathbb{R}^{N\times N}$. Define $\mathcal{D} = \mathrm{diag}(d_i) \in \mathbb{R}^{N\times N}$ ans $\mathcal{L} = \mathcal{D} - \mathcal{A}$ as the in-degree matrix and the corresponding Laplacian matrix, respectively, where $d_i = \sum_{j=1}^{N} a_{ij}$. There are two leader nodes to issue the upper and lower reference values. g_{ik} is the pinning gain from the (upper/lower) k^{th} leader to the i^{th} inverter, brought together in the diagonal matrix $\mathcal{G}_k = \mathrm{diag}\,(g_{ik})$.

$\sigma_{\min}(\cdot)$, and $\sigma_{\max}(\cdot)$ are the minimum and maximum singular values of a given matrix, respectively. $\mathscr{F}$ and $\mathscr{L}$ denote the sets of $\{1, 2, ..., N\}$ and $\{N+1, N+2\}$, respectively. $\mathbf{1}_N \in \mathbb{R}^N$ is a column vector where all entries are one. $\otimes$, $\mathrm{diag}\{\cdot\}$, $\|\cdot\|$, and $|\cdot|$ denote the Kronecker product, a block diagonal matrix, Euclidean norm of a given vector, and the absolute value of a given scalar, respectively.

III. Conventional Cooperative Secondary Control of AC Microgrids

Conventional secondary control acts as an actuator by providing the input control signals for tuning the setpoints of decentralized primary controls. These primary droop mechanisms are given by the following for the i^{th} inverter

$$\omega_i = \omega_{n_i} - m_{P_i} P_i, \tag{1}$$

$$v_{odi} = V_{n_i} - n_{Q_i} Q_i, \tag{2}$$

where P_i and Q_i are the active and reactive powers, respectively. ω_i and v_{odi} are the operating angular frequency and terminal voltage, respectively. ω_{n_i} and V_{n_i} are the setpoints for the primary droop mechanisms fed from the secondary control layer. m_{P_i} and n_{Q_i} are $P-\omega$ and $Q-v$ droop coefficients selected per inverters' power ratings.

We differentiate the droop relations in (1) and (2), with respect to time, to obtain

$$\dot{\omega}_{n_i} = \dot{\omega}_i + m_{P_i}\dot{P}_i = u_{f_i}, \tag{3}$$

$$\dot{V}_{n_i} = \dot{v}_{odi} + n_{Q_i}\dot{Q}_i = u_{v_i}, \tag{4}$$

where u_{f_i} and u_{v_i} are auxiliary control inputs. To synchronize the terminal frequency and voltage of each inverter to respective references, the leader-follower containment-based secondary control is adopted [23]. The local cooperative frequency and voltage control protocols, using the relative information with respect to the neighboring inverters and the leaders, are given by

$$u_{f_i} = c_{f_i}\left(\sum_{j\in\mathscr{F}} a_{ij}\left(\omega_j - \omega_i\right) + \sum_{k\in\mathscr{L}} g_{ik}\left(\omega_k - \omega_i\right) + \sum_{j\in\mathscr{F}} a_{ij}\left(m_{P_j}P_j - m_{P_i}P_i\right)\right), \tag{5}$$

$$u_{v_i} = c_{v_i}\left(\sum_{j\in\mathscr{F}} a_{ij}\left(v_{odj} - v_{odi}\right) + \sum_{k\in\mathscr{L}} g_{ik}\left(v_k - v_{odi}\right) + \sum_{j\in\mathscr{F}} a_{ij}\left(n_{Q_j}Q_j - n_{Q_i}Q_i\right)\right), \tag{6}$$

where c_{f_i}, c_{v_i} are positive constant coupling gains. ω_k and v_k are the frequency and voltage reference values of the k^{th} leader, respectively. The frequency reference for both leaders is set as ω_{ref}. The upper and lower leaders have their voltage reference values set as v^u_{ref} and v^l_{ref}, respectively. The setpoints for the primary-level droop control, ω_{n_i} and V_{n_i}, are, then, computed from u_{f_i} and u_{v_i} as

$$\omega_{n_i} = \int u_{f_i}\,\mathrm{d}\,t, \tag{7}$$

$$V_{n_i} = \int u_{v_i}\,\mathrm{d}\,t. \tag{8}$$

Using (5) and (6) to rewrite (3) and (4) yields

$$\dot{\omega}_{n_i} = c_{f_i}\left(\sum_{j\in\mathscr{F}} a_{ij}\left(\omega_{n_j} - \omega_{n_i}\right) + \sum_{k\in\mathscr{L}} g_{ik}\left(\omega_{n_k} - \omega_{n_i}\right)\right), \tag{9}$$

$$\dot{V}_{n_i} = c_{v_i}\left(\sum_{j\in\mathscr{F}} a_{ij}\left(V_{n_j} - V_{n_i}\right) + \sum_{k\in\mathscr{L}} g_{ik}\left(V_{n_k} - V_{n_i}\right)\right), \tag{10}$$

where $\omega_{n_k} = \omega_k + m_{P_i}P_i$ and $V_{n_k} = v_k + n_{Q_i}Q_i$. Define $\Phi_k = \frac{1}{2}\mathcal{L} + \mathcal{G}_k$. Then, the global forms of (9) and (10) are

$$\dot{\omega}_n = -\operatorname{diag}\left(c_{f_i}\right)\sum_{k\in\mathscr{L}} \Phi_k\left(\omega_n - \mathbf{1}_N \otimes \omega_{n_k}\right), \tag{11}$$

$$\dot{V}_n = -\operatorname{diag}\left(c_{v_i}\right)\sum_{k\in\mathscr{L}} \Phi_k\left(V_n - \mathbf{1}_N \otimes V_{n_k}\right), \tag{12}$$

where $\omega_n = [\omega_{n_1}^T, ..., \omega_{n_N}^T]^T$ and $V_n = [V_{n_1}^T, ..., V_{n_N}^T]^T$. Define the global frequency and voltage containment error vectors as

$$e_f = \omega_n - \left(\sum_{r\in\mathscr{L}} \Phi_r\right)^{-1}\sum_{k\in\mathscr{L}} \Phi_k\left(\mathbf{1}_N \otimes \omega_{n_k}\right), \tag{13}$$

$$e_v = V_n - \left(\sum_{r\in\mathscr{L}} \Phi_r\right)^{-1}\sum_{k\in\mathscr{L}} \Phi_k\left(\mathbf{1}_N \otimes V_{n_k}\right). \tag{14}$$

***Definition* 1 *(Secondary frequency containment control objective)*:** The secondary frequency control objective is to make the local frequency of each inverter converge to the range of the two frequency references issued by the upper and lower leaders. Since these two reference values are identical, the frequency regulation is achieved.

***Definition* 2 *(Secondary voltage containment control objective)*:** The secondary voltage containment control objective is to make each inverter voltage converge to the range spanned by the two references of the upper and lower leaders.

The following assumption is needed for the communication graph topology to guarantee the cooperative consensus [24].

***Assumption* 1:** The communication graph $\mathscr{G}$ includes a directed path from, at least, one leader to each inverter.

***Lemma* 1 ([25]):** Suppose Assumption 1 holds, $\sum_{k\in\mathscr{L}} \Phi_k$ is non-singular and

positive-definite. Moreover, the frequency and voltage containment control objectives are achieved if $\lim_{t\to\infty} e_f(t) = 0$ and $\lim_{t\to\infty} e_v(t) = 0$, respectively.

IV. Problem Formulation

This section formulates the resilient secondary frequency and voltage control problems for a networked AC microgrid. In particular, we consider the general unknown unbounded attack injections to the local input channels of both frequency and voltage control loops, that modifies (9) and (10) to

$$\dot{\omega}_{n_i} = c_{f_i}\left(\sum_{j\in\mathscr{F}} a_{ij}\left(\omega_{n_j} - \omega_{n_i}\right) + \sum_{k\in\mathscr{L}} g_{ik}\left(\omega_{n_k} - \omega_{n_i}\right)\right) + \varpi_{f_i}, \tag{15}$$

$$\dot{V}_{n_i} = c_{v_i}\left(\sum_{j\in\mathscr{F}} a_{ij}\left(V_{n_j} - V_{n_i}\right) + \sum_{k\in\mathscr{L}} g_{ik}\left(V_{n_k} - V_{n_i}\right)\right) + \varpi_{v_i}, \tag{16}$$

where ϖ_{f_i} and ϖ_{v_i} denote the unbounded attack signals injected to the input channels of frequency and voltage control loops at the i^{th} inverter, respectively. We make an slight assumption regarding the attack signals.

***Assumption* 2:** $\dot{\varpi}_{f_i}$ and $\dot{\varpi}_{v_i}$ are bounded.

***Remark* 1:** Assumption 2 is reasonable since attack signals, with an excessively-large change in values, could be easily detected in practice.

Since ϖ_{f_i} and ϖ_{v_i} are unbounded, conventional cooperative control protocols fail to regulate the frequency and voltage terms. One then needs resilient control methods to preserve the frequency regulation and voltage containment performances, and assure the closed-loop stability. The following convergence definition is needed.

***Definition* 3 ([26]):** Signal $x(t)$ is UUB with an ultimate bound b, if there exist positive constants b and c, independent of $t_0 \geq 0$, and for every $a \in (0, c)$, there exist $t_1 = t_1(a, b) \geq 0$, independent of t_0, such that $\|x(t_0)\| \leq a \Rightarrow \|x(t)\| \leq b, \forall t \geq t_0 + t_1$.

Now, the following distributed resilient secondary frequency and voltage control problems are defined.

***Definition* 4 *(Attack-resilient Frequency Control Problem)*:** The goal is to design input control signal u_{f_i} in (3) for each inverter such that e_f in (13) is UUB under unbounded attacks to the local frequency control loop. That is, inveter frequency goes to a small neighborhood around the reference value.

***Definition* 5 *(Attack-resilient Voltage Control Problem)*:** The goal is to design input control signal u_{v_i} in (4) for each inverter such that e_v in (14) is UUB under unbounded attacks to the local voltage control loop. That is, each inverter voltage goes to a small neighborhood around the range spanned by the two upper and lower references.

V. Distributed Resilient Controller Design

We propose a fully distributed control method to solve the attack-resilient frequency and voltage control problems. For convenience, denote

$$\zeta_{f_i} = \sum_{j \in \mathscr{F}} a_{ij} \left(\omega_{n_j} - \omega_{n_i}\right) + \sum_{k \in \mathscr{L}} g_{ik} \left(\omega_{n_k} - \omega_{n_i}\right), \tag{17}$$

$$\zeta_{v_i} = \sum_{j \in \mathscr{F}} a_{ij} \left(V_{n_j} - V_{n_i}\right) + \sum_{k \in \mathscr{L}} g_{ik} \left(V_{n_k} - V_{n_i}\right). \tag{18}$$

Then, we present the following resilient control framework for both frequency and voltage control loops

$$\begin{cases} \dot{\omega}_{n_i} = \left(\rho_{f_i} + \dot{\rho}_{f_i}\right) \zeta_{f_i} + \varpi_{f_i}, \\ \dot{\rho}_{f_i} = \chi_{f_i} \left|\zeta_{f_i}\right|, \end{cases} \tag{19}$$

$$\begin{cases} \dot{V}_{n_i} = \left(\rho_{v_i} + \dot{\rho}_{v_i}\right) \zeta_{v_i} + \varpi_{v_i}, \\ \dot{\rho}_{v_i} = \chi_{v_i} \left|\zeta_{v_i}\right|, \end{cases} \tag{20}$$

where χ_{f_i} and χ_{v_i} are given positive constants. ρ_{f_i} and ρ_{v_i} are time-varying coupling weights, with $\rho_{f_i}(0) \geq 0, \rho_{v_i}(0) \geq 0$. Figure 2 shows the communication network

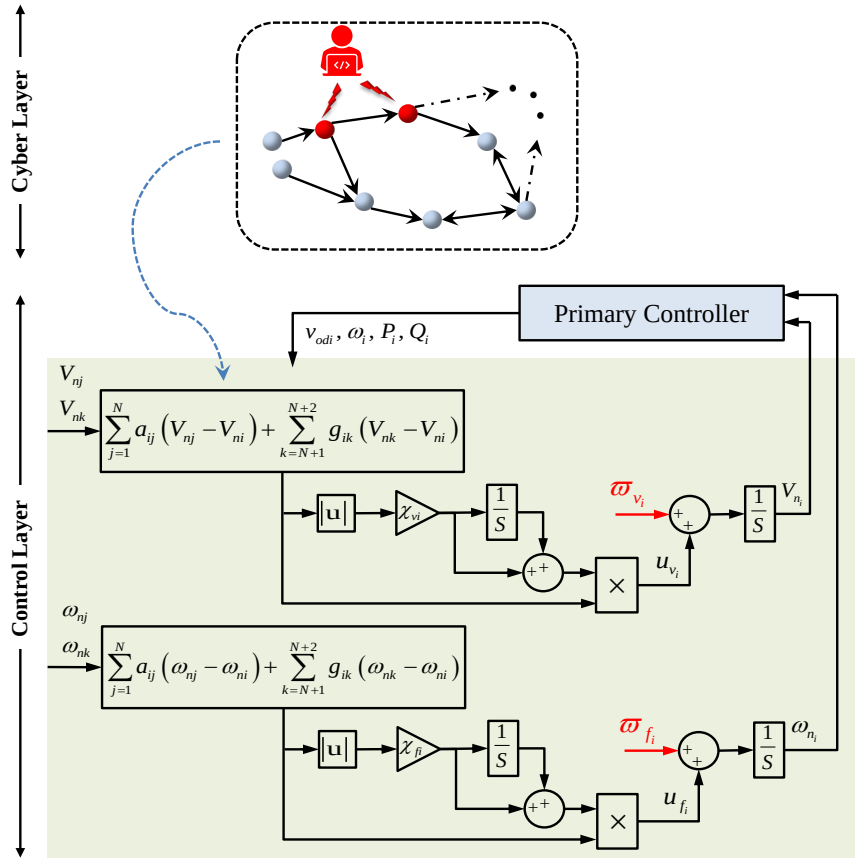

Fig. 2: Communication layer among inverters, and the proposed attack-resilient secondary control framework for an inverter.

among inverters and the proposed secondary control for an inverter.

***Theorem* 1:** Under Assumptions 1 and 2, and using the cooperative resilient frequency control protocols consisting of (17) and (19), e_f in (13) is UUB. Furthermore, by increasing χ_{f_i} in (19), the ultimate bound of e_f can be adjusted to be an arbitrarily small value, i.e., inverter frequency converges to an arbitrarily small neighborhood around the reference value.

***Proof*:** Consider the Lyapunov function candidate

$$E = \frac{1}{2}\sum_{i=1}^{N}\int_{0}^{\zeta_{f_i}^2(t)} \left(\rho_{f_i}(s) + \dot{\rho}_{f_i}(s)\right) \mathrm{d}\, s. \tag{21}$$

Combine (19) and (21) to obtain

$$\begin{aligned}\dot{E} &= \frac{1}{2}\sum_{i=1}^{N}\left(\rho_{f_i}+\dot{\rho}_{f_i}\right)2\zeta_{f_i}\dot{\zeta}_{f_i} \\ &= \zeta_f^T \operatorname{diag}\left(\rho_{f_i}+\dot{\rho}_{f_i}\right)\dot{\zeta}_f \\ &= \zeta_f^T \operatorname{diag}\left(\rho_{f_i}+\dot{\rho}_{f_i}\right)\left(-\sum_{k\in\mathscr{L}}\Phi_k\dot{\omega}_n\right) \\ &= -\zeta_f^T \operatorname{diag}\left(\rho_{f_i}+\dot{\rho}_{f_i}\right)\left(\sum_{k\in\mathscr{L}}\Phi_k\right)\left(\operatorname{diag}\left(\rho_{f_i}+\dot{\rho}_{f_i}\right)\zeta_f+\varpi_f\right),\end{aligned} \tag{22}$$

where $\zeta_f = [\zeta_{f_1}^T, ..., \zeta_{f_N}^T]^T$.

Recalling Sylvester's inequality and noting that $\sum_{k\in\mathscr{L}}\Phi_k$ is positive-definite, one then obtain

$$\begin{aligned}\dot{E} &\leq -\sigma_{\min}\left(\sum_{k\in\mathscr{L}}\Phi_k\right)\left\|\operatorname{diag}\left(\rho_{f_i}+\dot{\rho}_{f_i}\right)\zeta_f\right\|^2 \\ &\quad +\sigma_{\max}\left(\sum_{k\in\mathscr{L}}\Phi_k\right)\left\|\operatorname{diag}\left(\rho_{f_i}+\dot{\rho}_{f_i}\right)\zeta_f\right\|\left\|\varpi_f\right\| \\ &\leq -\sigma_{\min}\left(\sum_{k\in\mathscr{L}}\Phi_k\right)\left\|\operatorname{diag}\left(\rho_{f_i}+\dot{\rho}_{f_i}\right)\zeta_f\right\|\times \\ &\left(\left\|\operatorname{diag}\left(\rho_{f_i}+\dot{\rho}_{f_i}\right)\zeta_f\right\| - \frac{\sigma_{\max}\left(\sum_{k\in\mathscr{L}}\Phi_k\right)}{\sigma_{\min}\left(\sum_{k\in\mathscr{L}}\Phi_k\right)}\left\|\varpi_f\right\|\right).\end{aligned} \tag{23}$$

Next, we will prove that $\exists\tau > 0$, such that

$$\left\|\operatorname{diag}\left(\rho_{f_i}+\dot{\rho}_{f_i}\right)\zeta_f\right\| \geq \frac{\sigma_{\max}\left(\sum_{k\in\mathscr{L}}\Phi_k\right)}{\sigma_{\min}\left(\sum_{k\in\mathscr{L}}\Phi_k\right)}\left\|\varpi_f\right\|, \forall t \geq \tau. \tag{24}$$

A sufficient condition to guarantee (24) is

$$|(\rho_{f_i} + \dot{\rho}_{f_i})\,\zeta_{f_i}| \geq \frac{\sigma_{\max}\left(\sum\limits_{k\in\mathscr{L}} \Phi_k\right)}{\sigma_{\min}\left(\sum\limits_{k\in\mathscr{L}} \Phi_k\right)} |\varpi_{f_i}|\,, \quad \forall t \geq \tau. \tag{25}$$

Since both ρ_{f_i} and $\dot{\rho}_{f_i}$ are non-negative, we further obtain the following sufficient condition

$$\rho_{f_i}\,|\zeta_{f_i}| \geq \frac{\sigma_{\max}\left(\sum\limits_{k\in\mathscr{L}} \Phi_k\right)}{\sigma_{\min}\left(\sum\limits_{k\in\mathscr{L}} \Phi_k\right)} |\varpi_{f_i}|\,, \quad \forall t \geq \tau. \tag{26}$$

Note that (26) is guaranteed if both $\rho_{f_i} \geq |\varpi_{f_i}|$ and $|\zeta_{f_i}| \geq \frac{\sigma_{\max}\left(\sum_{k\in\mathscr{L}} \Phi_k\right)}{\sigma_{\min}\left(\sum_{k\in\mathscr{L}} \Phi_k\right)}$ hold. Since

$$\frac{\mathrm{d}\,|\varpi_{f_i}|}{\mathrm{d}\,t} = \frac{\varpi_{f_i}\dot{\varpi}_{f_i}}{|\varpi_{f_i}|} \leq |\dot{\varpi}_{f_i}|\,, \tag{27}$$

from Assumption 2, $\dot{\varpi}_{f_i}$ is bounded. Hence, $\frac{\mathrm{d}|\varpi_{f_i}|}{\mathrm{d}\,t}$ is also bounded. Using (19) and choosing

$$|\zeta_{f_i}| \geq \max\left\{\frac{\sigma_{\max}\left(\sum\limits_{k\in\mathscr{L}} \Phi_k\right)}{\sigma_{\min}\left(\sum\limits_{k\in\mathscr{L}} \Phi_k\right)}, \frac{1}{\chi_{f_i}}\frac{\mathrm{d}\,|\varpi_{f_i}|}{\mathrm{d}\,t}\right\}, \tag{28}$$

we then obtain that $\exists\tau > 0$, such that (26) holds. Further, we obtain that (24) holds. Using (23), we now obtain that $\forall t \geq \tau$

$$\dot{E} \leq 0, \quad \forall\,|\zeta_{f_i}| \geq \max\left\{\frac{\sigma_{\max}\left(\sum\limits_{k\in\mathscr{L}} \Phi_k\right)}{\sigma_{\min}\left(\sum\limits_{k\in\mathscr{L}} \Phi_k\right)}, \frac{1}{\chi_{f_i}}\frac{\mathrm{d}\,|\varpi_{f_i}|}{\mathrm{d}\,t}\right\}. \tag{29}$$

Therefore, ζ_{f_i} is bounded. Note that

$$\zeta_f = \sum_{k\in\mathscr{L}} \Phi_k e_f. \tag{30}$$

Hence, e_f is also bounded. Moreover, using LaSalle's invariance principle [27], it is seen from (29) that ζ_{f_i} is bounded by $\max\left\{\frac{\sigma_{\max}\left(\sum_{k\in\mathscr{L}}\Phi_k\right)}{\sigma_{\min}\left(\sum_{k\in\mathscr{L}}\Phi_k\right)}, \frac{1}{\chi_{f_i}}\frac{\mathrm{d}\left|\varpi_{f_i}\right|}{\mathrm{d}\,t}\right\}$, where $\frac{\sigma_{\max}\left(\sum_{k\in\mathscr{L}}\Phi_k\right)}{\sigma_{\min}\left(\sum_{k\in\mathscr{L}}\Phi_k\right)}$ is a positive constant. Hence, the ultimate bound can be reduced by properly increasing the adaptive tuning parameter ϖ_{f_i} in (19). ■

***Theorem* 2:** Under Assumptions 1 and 2, and using the cooperative resilient voltage control protocols consisting of (18) and (20), e_v in (14) is UUB. Furthermore, by increasing χ_{v_i} in (20), the ultimate bound of e_v can be set arbitrarily small, i.e., the inverter voltage converges to an arbitrarily small neighborhood around the range covered by the two references.

***Proof*:** The proof follows that of Theorem 1. ■

***Remark* 2:** Compared to [2], the proposed control protocols (17)-(20) have the following merits: (i) Local observers with additional communication information flow are constructed in [2] to estimate the actual state measurement. This, however, could introduce additional computational complexity. Moreover, the additional communication channels for exchanging observer states could potentially increase the system vulnerability to malicious cyber attacks; (ii) While both [2] and this paper preserve the UUB convergences for both frequency and voltage terms, in this paper, the ultimate bound can be reduced by properly increasing the adaptive tuning parameters.

VI. Case Studies

The proposed resilient control method is studied in the context of an IEEE 34-bus feeder system, islanded at bus 800 and augmented with four inverters and two leaders, as shown in Fig. 3. Specifications of inverters and its grid-interconnections are adopted from [1] and [28], respectively. Inverters 1 and 2 have twice the power ratings of inverters 3 and 4. The inverter droop gains are set as $m_{P_1} = m_{P_2} = 9.4 \times 10^{-5}$, $m_{P_3} = m_{P_4} = 18.8 \times 10^{-5}$, $n_{Q_1} = n_{Q_2} = 1.3 \times 10^{-3}$, and $n_{Q_3} = n_{Q_4} = 2.6 \times 10^{-3}$. Inverters communicate on a bidirectional communication network with the adjacency

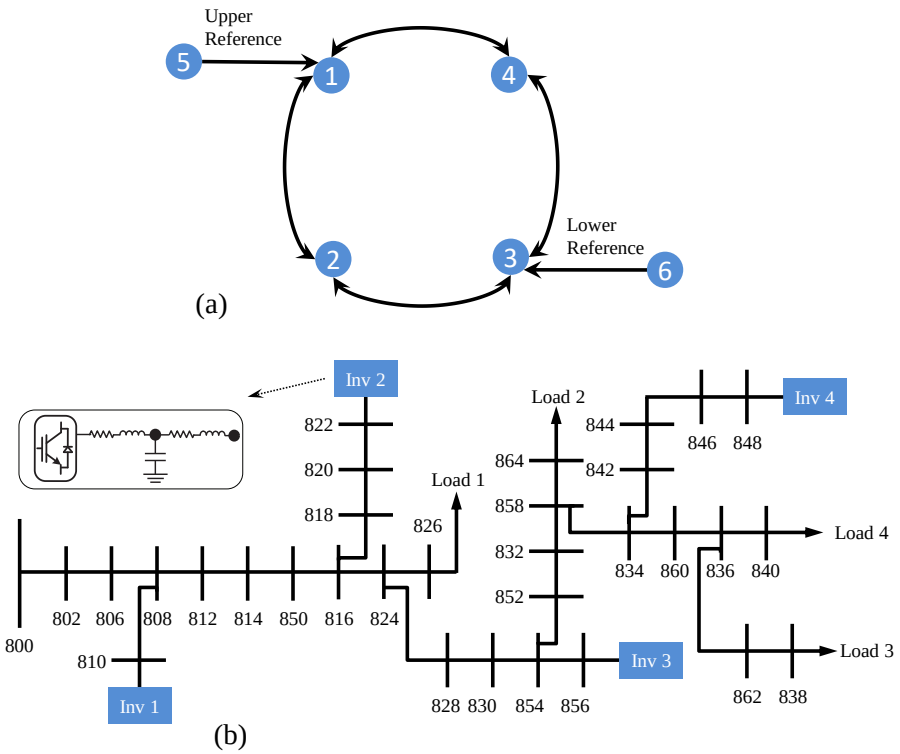

Fig. 3: Cyber-physical microgrid system: (a) Communication graph topology among four inverters and two leaders, (b) IEEE 34-bus system with four inverters.

matrix of $\mathcal{A} = [0\ 1\ 0\ 1; 1\ 0\ 1\ 0; 0\ 1\ 0\ 1; 1\ 0\ 1\ 0]$. The pinning gains are $g_{15} = g_{36} = 1$. The frequency reference, upper voltage reference, and lower voltage reference are 60 Hz, 340 V, and 330 V, respectively. The unbounded attack injections to the frequency and voltage control loops are set as $\varpi_{f_i} = 1t, i = 1, 2, 3, 4$ and $\varpi_{v_i} = 10t, i = 1, 2, 3, 4$, respectively. The performance of the resilient control protocols, (17)-(20), is compared with the conventional secondary control method in (5) and (6). The coupling gains for the conventional control protocols are set as $c_{f_i} = 10, c_{v_i} = 20, i = 1, 2, 3, 4$. The adaptive tuning parameters for the resilient control method are set as $\chi_{f_i} = 3, \chi_{v_i} = 3, i = 1, 2, 3, 4$.

Figure 4 compares the frequency response for the proposed and the conventional methods. Under ideal conditions (no attacks), inverters frequencies synchronize to $f = 60$ Hz using both control methods. Once the unbounded attack to frequency control loops

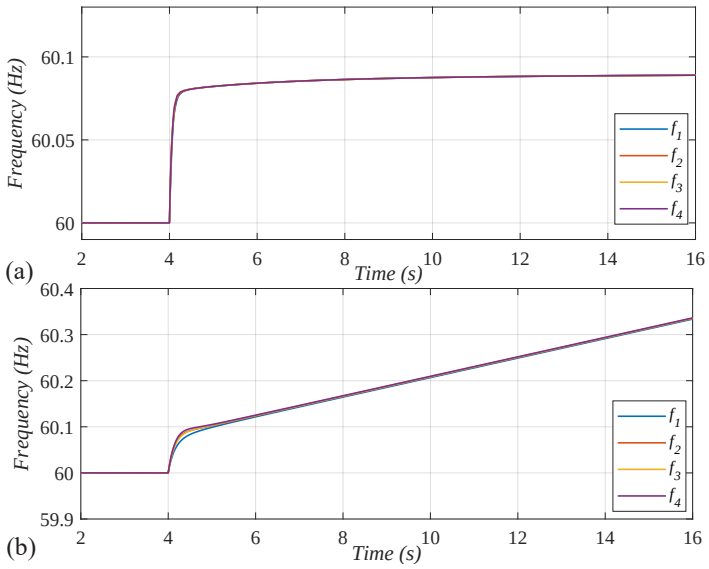

Fig. 4: Frequency response under unbounded actuator attacks: a) proposed resilient method, and b) conventional control method.

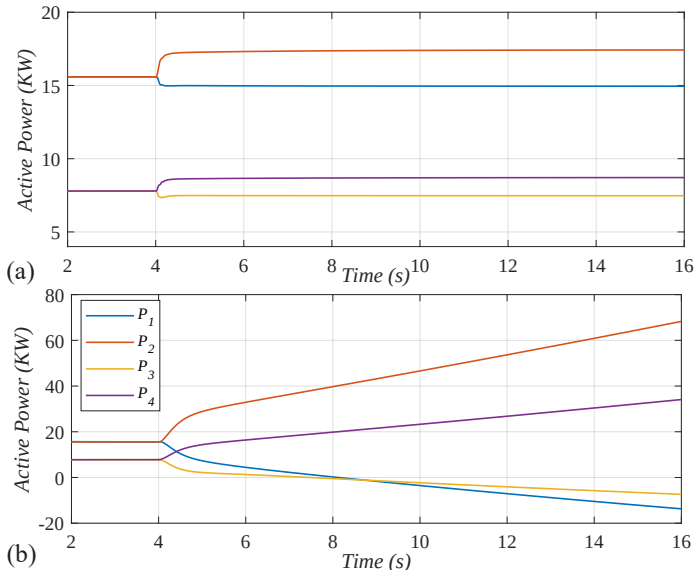

Fig. 5: Active powers of inverters subjected to unbounded actuator attacks: a) proposed resilient method and, b) conventional method.

is initiated at $t = 4s$, the conventional method fails to preserve the system stability. By contrast, the proposed resilient method contains frequencies at a small neighborhood around 60 Hz. Figure 5 shows that, without attacks, both methods share active powers

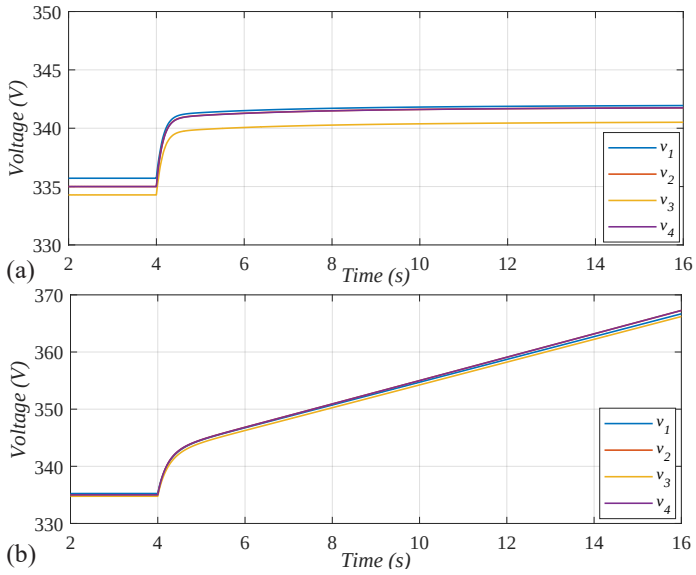

Fig. 6: Voltage performance under unbounded actuator attacks: a) proposed resilient method and, b) conventional control method.

among inverters based on their droop gains. After initiating the unbounded attacks to frequency control loops at $t = 4s$, the active power performance from the conventional method becomes unstable. Meanwhile, the proposed method contains active powers in a small neighborhood around the value of properly shared powers. Figure 6 compares inverters voltages using both control methods. Without attacks, voltage values stay in the range of $330\,\mathrm{V}$ to $340\,\mathrm{V}$. After initiating the unbounded attacks to voltage control loops at $t = 4s$, the voltages terms using the conventional method diverge, while those produced by the proposed method remain stable within $330\,\mathrm{V} \sim 340\,\mathrm{V}$.

The ultimate bound of the UUB convergence can be adjusted to be an arbitrarily small value by increasing the adaptive tuning parameters. Figures 7 and 8 show the frequency and active power waveforms, where the performance with $\chi_{f_i} = 3$ and $\chi_{f_i} = 10$ are illustrated with solid and dashed lines, respectively. As seen, the ultimate bound can be reduced by increasing χ_{f_i}.

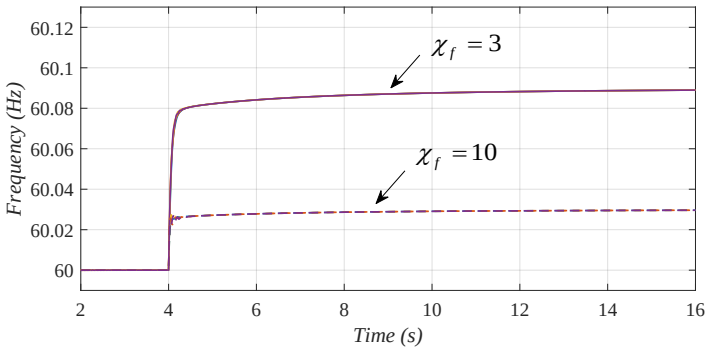

Fig. 7: Comparative frequency performance under unbounded actuator attacks with different adaptive tuning parameters.

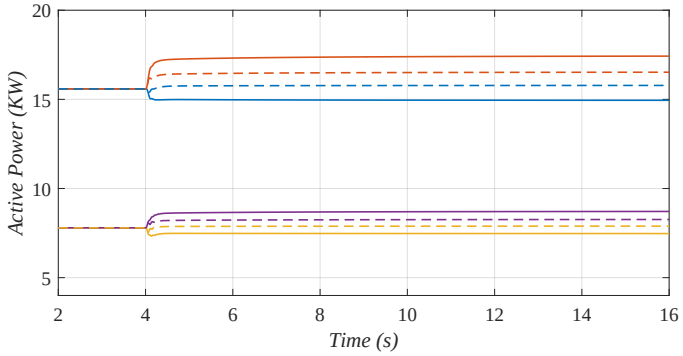

Fig. 8: Comparative active power performance under unbounded actuator attacks with different adaptive tuning parameters.

VII. Conclusion

This paper studies a resilient secondary controller for multi-inverter AC microgrids against unknown unbounded actuator attacks to both frequency and voltage control loops. An adaptive, fully-distributed control framework ensures the UUB stability of the closed-loop system by preserving the UUB regulation for both frequency and voltage terms. The resilient performance of the proposed method has been verified using a modified IEEE 34-bus system.

References

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

[2] S. Zuo, O. A. Beg, F. L. Lewis, and A. Davoudi, "Resilient networked ac microgrids under unbounded cyber attacks," *IEEE Transactions on Smart Grid*, doi: 10.1109/TSG.2020.2984266, 2020.

[3] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proceedings of the 16th ACM Conference on Computer and Communications Security*, ser. CCS '09. New York, NY, USA: ACM, 2009, pp. 21–32.

[4] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 645–658, Dec. 2011.

[5] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber–physical system security for the electric power grid," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 210–224, Jan. 2012.

[6] H. He and J. Yan, "Cyber-physical attacks and defences in the smart grid: a survey," *IET Cyber-Physical Systems: Theory Applications*, vol. 1, no. 1, pp. 13–27, 2016.

[7] R. Deng, G. Xiao, R. Lu, H. Liang, and A. V. Vasilakos, "False data injection on state estimation in power systems-attacks, impacts, and defense: A survey," *IEEE Trans. Ind. Informat.*, vol. 13, no. 2, pp. 411–423, Apr. 2017.

[8] Y. Li, P. Zhang, L. Zhang, and B. Wang, "Active synchronous detection of deception attacks in microgrid control systems," *IEEE Trans. Smart Grid*, vol. 8, no. 1, pp. 373–375, Jan. 2017.

[9] S. Sahoo, S. Mishra, J. C. Peng, and T. Dragičević, "A stealth cyber-attack detection strategy for dc microgrids," *IEEE Trans. Power Electron.*, vol. 34, no. 8, pp. 8162–8174, Aug. 2019.

[10] O. A. Beg, T. T. Johnson, and A. Davoudi, "Detection of false-data injection attacks in cyber-physical dc microgrids," *IEEE Trans. Ind. Informat.*, vol. 13, no. 5, pp. 2693–2703, Oct. 2017.

[11] O. A. Beg, L. V. Nguyen, T. T. Johnson, and A. Davoudi, "Signal temporal logic-based attack detection in dc microgrids," *IEEE Trans. Smart Grid*, vol. 10, no. 4, pp. 3585–3595, Jul. 2019.

[12] S. Sahoo, J. C. Peng, D. Annavaram, S. Mishra, and T. Dragicevic, "On detection of false data in cooperative dc microgrids-a discordant element approach," *IEEE Trans. Ind. Electron.*, pp. 1–1, 2019.

[13] S. Liu, P. Siano, and X. Wang, "Intrusion-detector-dependent frequency regulation for microgrids under denial-of-service attacks," *IEEE Systems Journal*, pp. 1–4, 2019.

[14] S. Abhinav, I. D. Schizas, F. L. Lewis, and A. Davoudi, "Distributed noise-resilient networked synchrony of active distribution systems," *IEEE Trans. Smart Grid*, vol. 9, no. 2, pp. 836–846, Mar. 2018.

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

[16] N. M. Dehkordi, H. R. Baghaee, N. Sadati, and J. M. Guerrero, "Distributed noise-resilient secondary voltage and frequency control for islanded microgrids," *IEEE Trans. Smart Grid*, vol. 10, no. 4, pp. 3780–3790, Jul. 2019.

[17] M. A. Shahab, B. Mozafari, S. Soleymani, N. M. Dehkordi, H. M. Shourkaei, and J. M. Guerrero, "Distributed

consensus-based fault tolerant control of islanded microgrids," *IEEE Transactions on Smart Grid*, vol. 11, no. 1, pp. 37–47, Jan 2020.

[18] A. Afshari, M. Karrari, H. R. Baghaee, G. B. Gharehpetian, and S. Karrari, "Cooperative fault-tolerant control of microgrids under switching communication topology," *IEEE Transactions on Smart Grid*, doi: 10.1109/TSG.2019.2944768, 2019.

[19] 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, Jun. 2014.

[20] G. Hug and J. A. Giampapa, "Vulnerability assessment of ac state estimation with respect to false data injection cyber-attacks," *IEEE Transactions on Smart Grid*, vol. 3, no. 3, pp. 1362–1370, Sep. 2012.

[21] J. Liang, L. Sankar, and O. Kosut, "Vulnerability analysis and consequences of false data injection attack on power system state estimation," *IEEE Transactions on Power Systems*, vol. 31, no. 5, pp. 3864–3872, Sep. 2016.

[22] K. Pan, A. Teixeira, M. Cvetkovic, and P. Palensky, "Cyber risk analysis of combined data attacks against power system state estimation," *IEEE Trans. Smart Grid*, vol. 10, no. 3, pp. 3044–3056, May 2019.

[23] R. Han, L. Meng, G. Ferrari-Trecate, E. A. A. Coelho, J. C. Vasquez, and J. M. Guerrero, "Containment and consensus-based distributed coordination control to achieve bounded voltage and precise reactive power sharing in islanded ac microgrids," *IEEE Trans. Ind. Appl.*, vol. 53, no. 6, pp. 5187–5199, Nov. 2017.

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

[25] S. Zuo, Y. Song, F. L. Lewis, and A. Davoudi, "Output containment control of linear heterogeneous multi-agent systems using internal model principle," *IEEE Trans. Cybern.*, vol. 47, no. 8, pp. 2099–2109, Aug. 2017.

[26] H. K. Khalil, *Nonlinear Systems*. Upper Saddle River, NJ: Prentice Hall, 2002.

[27] J. LaSalle, "Some extensions of liapunov's second method," *IRE Transactions on Circuit Theory*, vol. 7, no. 4, pp. 520–527, Dec. 1960.

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

CHAPTER 7

CONCLUSION

This dissertation considers various approaches to design resilient control strategies for MAS in general, and with applications to electric microgrids. In one approach, resilient control architectures have been proposed for general linear heterogeneous MAS to counter sensor faults and adversaries' attacks in a cooperative and adversarial multi-group system. In another approach, a fully distributed control framework using observer-based techniques has been evaluated for the secondary frequency regulation and voltage containment of multi-inverter based AC microgrids to address general unbounded attacks. The result has been further refined to deal with intelligently correlated sensor attacks. Moreover, a resilient secondary controller has been designed for DC microgrids to mitigate the adverse effect of unbounded attacks on local control input signals. Finally, a fully distributed control framework, using adaptive techniques, has been evaluated on the secondary control of AC microgrids to preserve the UUB convergence and adaptively tune the ultimate bound on convergence to an arbitrarily small value.

Future extension could explore distributed control and online learning problems related to large-scale, multi-agent, cyber-physical systems (CPS), which can have broad application to power systems. One could relax the assumptions made in this work. For example, herein, we had assumed the derivatives of the attack signals to be bounded (even though the signal itself is unbounded). What would happen if the injected signals have unbounded high-order derivatives? How can one handle general unbounded attacks to sensors?, and, eventually, How can one design a unified resilient approach to simultaneously address attacks on sensors, actuators, and communication channels? Another interesting

direction is to design distributed online learning for the cooperative control of unknown heterogeneous CPS. Conventional approaches are usually performed offline and require some modeling knowledge. We hope to bring online real-time learning analysis, together with resilient optimal control design, to improve the resilience of the heterogeneous CPS against faults, failures, and malicious attacks.

BIOGRAPHICAL STATEMENT

Shan Zuo received her B.S. and Ph.D. degrees from University of Electronic Science and Technology of China, both in electrical engineering, in 2012 and 2018, respectively. From Sep. 2014 to Sep. 2016, she was a visiting Ph.D. student at the University of Texas at Arlington. From Oct. 2016 to Apr. 2018, she was a researcher at the University of Texas at Arlington Research Institute. She is receiving her 2nd Ph.D. degree from the University of Texas at Arlington, Texas, USA, in electrical engineering, in 2020. Her research interests include multi-agent systems, resilient control, microgrids, and cyber-physical systems.