A Linear Regression Based Resilient Optimal Operation of AC Microgrids

Sahoo, Subham; Rana, Rubi; Molinas, Marta; Blaabjerg, Frede; Dragicevic, Tomislav; Mishra, Sukumar

Published in:
2020 IEEE 11th International Symposium on Power Electronics for Distributed Generation Systems (PEDG)

DOI (link to publication from Publisher):
10.1109/PEDG48541.2020.9244379

Publication date:
2020

Document Version
Publisher's PDF, also known as Version of record

A Linear Regression Based Resilient Optimal Operation of AC Microgrids

Subham Sahoo*, Rubi Rana†, Marta Molinas‡, Frede Blaabjerg*, Tomislav Dragicevic§ and Sukumar Mishra†
*Department of Energy Technology, Aalborg University, Denmark
†Department of Electrical Engineering, Indian Institute of Technology Delhi, India
‡Department of Engineering Cybernetics, Norwegian University of Science and Technology, Norway
§Department of Electrical Engineering, Technical University of Denmark, Denmark
*e-mail: sssa@et.aau.dk

***Abstract*—This paper investigates the impact of data integrity attacks (DIAs) on cooperative economic dispatch of distributed generators (DGs) in autonomous AC microgrids. To establish resiliency against such attacks and ensure optimal operation, a linear regression based control update is designed in this paper. To improve the robustness against multiple points of intrusion, the design of the resilient control update involves local measurements. As a result, any maloperation due to DIA is prevented from being propagated to the neighboring nodes. The proposed strategy acts immediately upon detection of data integrity attack to ensure maximization in the economic profit.**

***Index Terms*—AC microgrids, Cyber security, Data integrity attacks, Cyber attacks, Economic load dispatch**

I. Introduction

Due to the flexibility of their application in both grid-connected and islanded modes, microgrids were established as key enablers for the integration of renewable energy sources [1]. To facilitate its operation under transmission delay and information failure, cooperative/distributed controllers with robust performance towards cyber layer imperfections are preferred in recent times [2]. Unlike operating in longer time scales with static demand feedback in the centralized system, cooperative dispatching often allows online actions for every increase in load in real time [3]. As a result, it improves the economic profile of the generators in a given duration.

Considerably less effort has gone into analyzing cyber attacks in cooperative optimization. To name a few, Chow *et. al.* [4] have designed a reputation-based detection algorithm to detect attacks on the economic dispatch (ED) problem. However, it is not fully cooperative, as the algorithm requires a centralized control center. Since these mechanisms are highly prone to single point of failure, the optimal operation of the system can easily be disrupted [6]. To increase the generation cost, any adversarial false data in the cooperative ED optimization model is categorized as a data integrity attack (DIA) in this paper. Such attacks alter the power flows with respect to the optimal solution [7].

Further, data intrusion from stealth attacks is also possible, as demonstrated in [8]-[12]. Such attacks are capable of increasing the generation cost without causing any obvious indications of power imbalance. To formulate an attack-resilient mechanism, a two-hop neighboring information-based verification algorithm to detect and restore the system from DIAs is also reported in [5]. This algorithm is capable of detecting non-optimal and non-feasible solutions simultaneously. Nevertheless, its performance is highly dependent on the information from multiple neighbors, which may be a problem in cases of a compromised link or link failure. Many event-driven resilient strategies have also been proposed in [14]-[17], which ensure the best resiliency measures in power electronics even using a single trustworthy agent. In fact, the authors in [13] have modeled DIA, which manipulates the power dispatch of each generator to gain monetary benefits without destabilizing the system. Further, they provide a localized event-driven operation, which provides resilience against several cyber-physical disturbances. However, the design can be a complex approach.

To address these issues, this paper proposes:

1) a simple linear regression based resilient control update against data integrity attacks in cooperative microgrids to ensure optimality,
2) design of the resilient update only considering local measurements to enhance the operational flexibility.

978-1-7281-6990-3/20/$31.00 ©2020 IEEE

II. System and Attack Model

A. Control of Cooperative AC Microgrids

An autonomous AC microgrid with N inverter based DG sources is shown in Fig. 1. The considered microgrid system consists of three layer: the physical layer, control layer and cyber communication layer. The physical layer comprises of the entire microgrid network N inverters connected to a LCL filter. L_k, C_f and L_g represent per phase inductance and capacitance of the filter circuit and grid-side inductance, respectively. In the system shown in Fig. 1 which comprises of N agents, each communication graph is represented via edges to constitute an adjacency matrix $\mathbf{A} = [a_{kj}] \in R^{N\times N}$, where the communication weights are given by: $a_{kj} > 0$, if $(\Psi_k, \Psi_j) \in \mathbf{E}$, where $\mathbf{E}$ is an edge connecting two nodes with Ψ_k and Ψ_j being the local and neighboring node measurements, respectively. Otherwise, $a_{kj} = 0$. $N_k = \{j|(\Psi_k, \Psi_j) \in \mathbf{E}\}$ denotes the set of all neighbors of k^{th} agent. Further, the in-degree matrix $\mathbf{Z}_{in}$ = diag$\{z_{in}\}$ is a diagonal matrix with its elements given by $z_{in} = \sum_{j\in N_k} a_{kj}$. The Laplacian matrix $\mathbf{L}$ is defined as $\mathbf{L} = \mathbf{Z}_{in} - \mathbf{A}$.

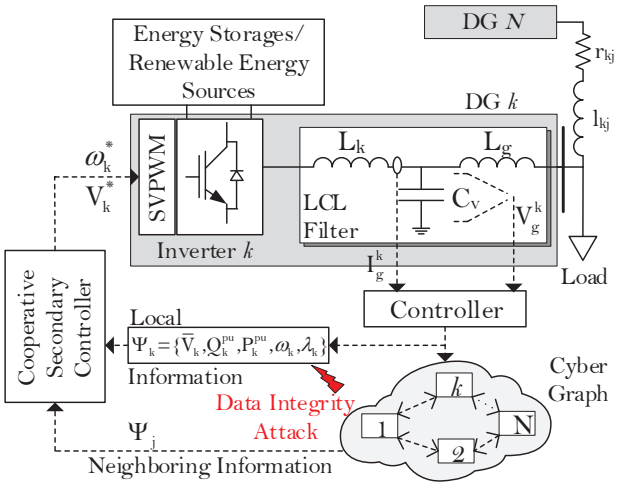

Fig. 1. Single-line diagram of a cyber-physical AC microgrid consisting of N DGs managed by a cooperative cyber topology. The data integrity attack is highlighted in red to change the cost parameters, affecting the optimal operation.

To improve their performance, neighboring inverters' measurements, which are transmitted to the local inverter and vice-versa, are used in a cooperative secondary controller to regulate their respective bus' average voltage $\bar{V}_k$ and frequency ω_k. The control objectives of the cooperative controller can be mathematically represented as:

$$\lim_{t\to\infty} \omega_k(t) = \omega^*, \ \lim_{t\to\infty} \bar{V}_k(t) = V^*, \ \forall \ k \in N \tag{1}$$

where ω^* and V^* denote the global reference for frequency and voltage, respectively. Detailed control equations of cooperative secondary controller in AC microgrids can be referred from [2]. To achieve proportionate active power sharing alongwith frequency restoration, the primary layer droop control is modified into:

$$\omega_k(t) = \omega^* - m_k(P_k(t) - P_k^{ref}(t)) \tag{2}$$

where m_k, P_k and P_k^{ref} denote the active power droop coefficient, measured active power and secondary control active power reference in the k^{th} agent, respectively. The active power control in each DG is augmented with frequency restoration to minimize the generation cost for economic operation. To this end, we consider the general quadratic cost function for each DG to provide the operational cost, given by:

$$C_k(P_k) = a_k P_k^2 + b_k P_k + c_k \tag{3}$$

where a_k, b_k and c_k are the cost coefficients of the source in k^{th} DG. Following the generation-demand balance equality constraint, the objective of optimal load sharing is to minimize the total cost of all DGs using:

$$\textbf{min } C(P) = \sum_{k=1}^{N} C_k(P_k) \tag{4}$$

$$\text{s.t.}[\sum_{k=1}^{N} P_k = P^D, \ P_k^{min} < P_k < P_k^{max}] \ \forall k \in N$$

where P^D, P_k^{min} and P_k^{max} denotes the total demand in the microgrid, minimum and maximum active power for k^{th} DG respectively. Further, (4) can be solved using its associated Lagrange function as:

$$\mathcal{L}_\lambda = \sum_{k=1}^{N} C_k(P_k) + \lambda_k \sum_{k=1}^{N} (P_k^D - P_k) \tag{5}$$

where λ_k and P_k^D denote the incremental cost and local active power demand respectively. Differentiating (5) with respect to P_k using the first-order optimality condition, we can initialize the incremental cost using:

$$\begin{cases} P_k(0) = \begin{cases} P_k^{min}, \ P_k^D < P_k^{min} \\ P_k^D, \ P_k^{min} < P_k^D < P_k^{max} \\ P_k^{max}, \ P_k^D > P_k^{max} \end{cases} \\ \lambda_k(0) = 2a_k P_k(0) + b_k \\ \eta_k(0) = P_k^D - P_k(0) \end{cases} \tag{6}$$

To minimize the total generation cost subjecting to the equality constraints, it is required that the incremental cost of each DG be equal [18], which is carried out using a power correction term ΔP_k, given by:

$$\Delta \dot{P}_k = \sum_{j \in N_k} a_{kj}(\lambda_j - \lambda_k) \tag{7}$$

Using (7), the active power reference for each DG with regulation of the local frequency can be obtained using:

$$P_k^{ref} = P_k^{initial} + g_k \int_0^\tau (\omega^* - \omega_k(t))d\tau + \Delta P_k. \tag{8}$$

Substituting (8) into (2), the active power droop control law operates to restore frequency of each bus to the rated value and participates in the optimal load sharing. Hence using (2)-(8), a unified cooperative control structure for economic dispatch is devised for AC microgrid to achieve:

$$\lim_{t\to\infty} \lambda_k = \lambda^{opt}, \lim_{t\to\infty} P_k(t) = P^{opt} \ \forall k \in N \tag{9}$$

where λ^{opt} and P^{opt} denote the optimal incremental cost and corresponding active power generation from k^{th} DG in the absence of cyber attack. However, any change in cost parameters or displacing of the incremental cost in (6) by an adversary, denoted as a data integrity attack (DIA), will cause the system to operate in an non-optimal state. As a result, such attacks reduce the energy efficiency, which needs to be identified and mitigated immediately.

B. Attack Modeling

Two types of DIAs have been considered in this paper. These attacks are given by:

$$\underbrace{\lambda_k^f(i+1) = \lambda_k(k) + \sum_{j \in N_k} w_{kj}(\lambda_j(i) - \lambda_k(i)) + \zeta u_{\lambda_k}^a}_{DIA_1} \quad (10)$$

$$\underbrace{\lambda_k^f(i) = (1-\zeta)\lambda_k(i) + \zeta\lambda_k^c}_{DIA_2} \quad (11)$$

where $u_{\lambda_i}^a$ is an exogenous attack input in i^{th} DG and ζ is a binary variable which is equal to 1 in the presence of DIA, or 0 otherwise. Moreover, λ_i^c denotes a constant valued attack element, which does not update in an iterative manner.

In (10), the attack can be injected by changing the cost parameters using:

$$u_{\lambda_k}^a = \begin{cases} -\Delta a_k P_k \\ -\Delta b_k \end{cases} \quad (12)$$

where Δa_k and Δb_k denote positive attack coefficients, when added to the cost function in (3) increase the overall generation cost. Hence, using (11), the consensus algorithm maloperates during the update process, which converges to an arbitrary value. Due to this maloperation, the control objectives in (9) are altered to:

$$\lim_{t\to\infty} \lambda_k(t) = \lambda^*, \lim_{t\to\infty} P_k(t) = P^* \ \forall k \in N \quad (13)$$

where λ^* and P^* denote the optimal setpoints for incremental cost and active power under the presence of DIA, respectively. It should be noted that there lies a considerable steady-state difference between λ^{opt} and λ^*, which has been theoretically verified in [2]. Hence, λ^* denotes the sub-optimal point of economic operation for DGs in AC microgrids.

To provide a basic understanding, a case study is done in a microgrid with N = 4 agents (the system and control parameters can be found in Appendix) in Fig. 2 to study the impact of change in cost parameters on the performance of AC microgrids. The cost parameters of each DG are provided in Table I. It can be seen that the system response is almost similar under both cases until DIA_1 is injected into DG I at t = 1 sec. As soon as DIA_1 is injected, the dotted lines show the deviation from the actual output as the incremental cost go up by a steady-state deviation of 0.6 \$/kW. Furthermore, this value will keep increasing as the power dispatch from each generator change with the increase in load. To counteract against these attacks, we propose a linear regression technique which can effectively diminish the impact of the modeled attacks by an artificial routing of the economic model parameters and ensure resilient optimal operation.

III. Proposed Resilient Mechanism

Considering $x(i) = P_k(i)$ as *input* and $y = \hat{\lambda_k}(i)$ as the *output*, which is supposed to be predicted. A pair $(x(i), y(i))$ is called a training example for i^{th} instant. Each training set comprises of m pairs. To describe the supervised learning

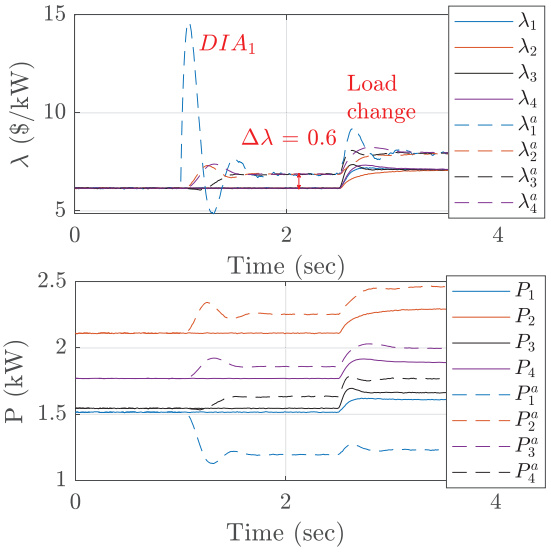

Fig. 2. Comparative evaluation of active power and incremental cost under the absence (solid lines) and presence (dotted lines) of DIA_1 – even though a steady-state solution is reached, a positive drift of 0.6 \$/kW is seen thereby increasing the generation cost and disturbing the optimal operation.

TABLE I
Cost Coefficients of DG

DG	I	II	III	IV
a_k (\$/kW^2)	0.005	0.0025	0.004	0.006
b_k (\$/kW)	1	0.6	1.8	0.45

problem more formally, our goal is, given a training set, to learn a hypothesis function h so that $h(x)$ is a *good* predictor for the corresponding value of y. When the output variable that we're trying to predict is continuous, we call the learning problem a regression problem. To perform supervised learning, we must decide how we're going to represent the hypotheses h. As an initial choice, we approximate y as a linear function of x:

$$h_\theta x(i) = x(i)^T\theta \quad (14)$$

In (14), θ is a weight, which parameterizes the space of linear functions mapping from x to y. One of the reasonable objective is to bring $h(x)$ close to y. To formalize this, we define a cost function that maps the relationship between $h(x(i))$ and $y(i)$, given by:

$$J(\theta) = \frac{1}{2}\sum_{i=1}^{m}(h_\theta x(i) - y(i))^2 \quad (15)$$

In (15), J is minimized without resorting to an iterative algorithm. In fact, it is minimized explicitly by taking its derivatives with respect to θ and setting them to zero.

Substituting (14) in (15), we get:

$$x\theta - y = \begin{bmatrix} x(1)\theta \\ x(2)\theta \\ \vdots \\ x(m)\theta \end{bmatrix} - \begin{bmatrix} y(1) \\ y(2) \\ \vdots \\ y(m) \end{bmatrix} \quad (16)$$

Thus, using the fact that for a vector z, we have that $z^T z = \sum_i z_i^2$.

$$x\theta - y = \begin{bmatrix} h_\theta x(1) - y(1) \\ h_\theta x(2) - y(2) \\ \vdots \\ h_\theta x(m) - y(m) \end{bmatrix} \quad (17)$$

Hence, the cost function can be obtained using:

$$J(\theta) = \frac{1}{2}(x\theta - y)^T(x\theta - y) = \frac{1}{2}\sum_{i=1}^{m}(h_\theta x(i) - y(i))^2 \quad (18)$$

Finally to minimize J, let's find its derivative with respect to θ. It is worth notifying that the derivative of J with respect to θ is denoted as $\Delta_\theta J(\theta)$.

The following properties of the trace operator *tr*($\circ$) are given below. Here, **A** and **B** are square matrices, and a is a real number:

- *tr*(**A**)=*tr*($\mathbf{A}^T$)
- *tr*(**A**+**B**)=*tr*(**A**) + *tr*(**B**)
- *tr*(a**A**) = a.*tr*(**A**)
- *tr*(**AB**)=*tr*(**BA**)

Furthermore, the derivative output using the trace operator is given by:

$$\Delta_A tr(\mathbf{AB}) = \mathbf{B}^T \quad (19)$$

$$\Delta_{A^T} f(\mathbf{A}) = (\Delta_A f(\mathbf{A}))^T \quad (20)$$

$$\Delta_A tr(\mathbf{ABA}^T\mathbf{C}) = \mathbf{CAB} + \mathbf{C}^T\mathbf{AB}^T \quad (21)$$

Combining (20) and (21), we get:

$$\Delta_{A^T} tr(\mathbf{ABA}^T\mathbf{C}) = \mathbf{B}^T\mathbf{A}^T\mathbf{C}^T + \mathbf{BA}^T\mathbf{C} \quad (22)$$

Using (22) to get the derivative of (18), we get:

$$\begin{aligned} \Delta_\theta J(\theta) &= \Delta_\theta \frac{1}{2}(x\theta - y)^T(x\theta - y) \\ &= \frac{1}{2}\Delta_\theta(\theta^T x^T x^\theta - \theta^T x^T y - y^T X\theta + y^T y) \end{aligned} \quad (23)$$

$$\Delta_\theta J(\theta) = \frac{1}{2}\Delta_\theta tr(\theta^T x^T x\theta - \theta^T x^T y - y^T x\theta + y^T y) \quad (24)$$

It is worth notifying that the trace of a real number is just the real number, given by $tr(\mathbf{A}) = tr(\mathbf{A})^T$. Considering this postulate, (24) can be re-written as:

$$\Delta_\theta J(\theta) = \frac{1}{2}\Delta_\theta(tr(\theta^T x^T x\theta) - 2tr(y^T x\theta)) \quad (25)$$

Comparing equation (22) and (25), we conclude:

$$\begin{aligned} \Delta_\theta J(\theta) &= \frac{1}{2}(x^T x\theta + x^T x\theta - 2x^T y) \\ &= x^T x\theta - x^T y \end{aligned} \quad (26)$$

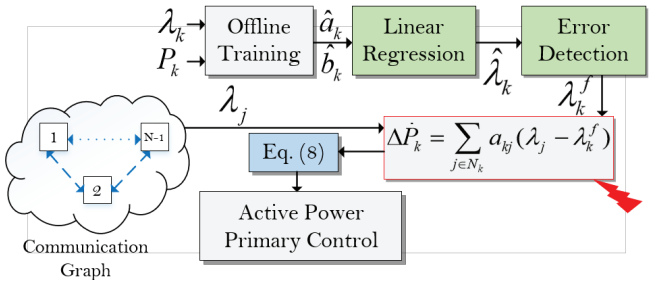

Fig. 3. Control diagram of the proposed linear regression based resilient controller for the modeled DIAs in cooperative AC microgrids.

To minimize J, we set its derivative to zero in order to obtain:

$$x^T x\theta = x^T y \quad (27)$$

Finally, the parameter θ that minimizes $J(\theta)$ can be given by:

$$\theta = (x^T x)^{-1} x^T y \quad (28)$$

With parameterization achieved to a certain degree using the offline historic data from λ_k and P_k, the estimated cost coefficients $\hat{a}_k$ and $\hat{b}_k$ are fed into the linear regression model, as shown in Fig. 3, to formalize the presence of any identification error. Finally, if an error is identified, the next update is immediately switched using:

$$\lambda_k^f = (1 - \kappa)\lambda_k + \kappa(\hat{a}_k P_k + \hat{b}_k) \quad (29)$$

Hence, the cooperative update of incremental cost is updated to ensure resiliency under these conditions. A detailed schematic of the control diagram is provided in Fig. 3.

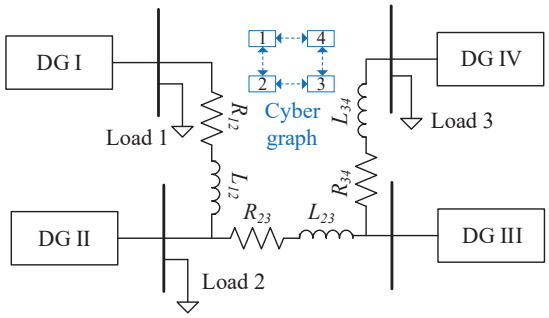

Fig. 4. Single line diagram of the cyber-physical AC microgrid with N = 4 DGs (agents).

IV. Simulation Results

The proposed localized event based attack-resilient control strategy is tested on an AC microgrid, as shown in Fig. 4, with N = 4 DGs of equal capacity of 10 kVA. The nominal frequency of the network is 60 Hz. All the system parameters can be found in Appendix. The cost parameter of each DG can be referred from Table I.

A case study on the considered system is carried out in Fig. 5(a), with DIA_1 in (5) injected by the adversary at t = 0.5

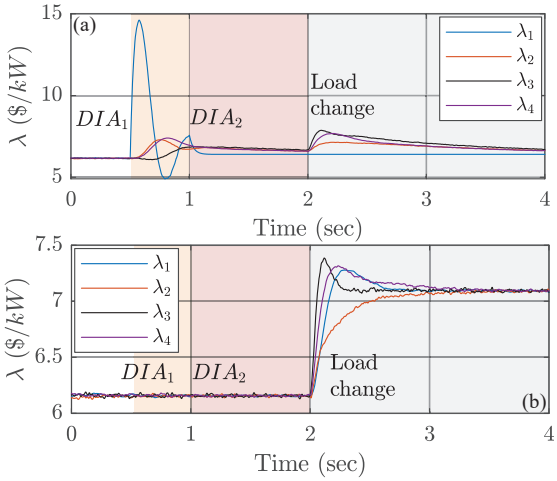

Fig. 5. Performance of AC microgrid with N= 4 DGs : (a) in the absence and, (b) in the presence of the proposed resilient controller when DIA_1 and DIA_2 are launched at t = 0.5 and 1 sec, respectively.

s. Observations in Fig. 5(a) confirm that the incremental cost of each DG start converging to a feasible solution. Further, another attack is conducted at t = 1 s, where λ_1^c = 6.5. It can be seen that as soon as λ_1 settles to 6.5, the remaining DGs track the set-point as a reference using the consensus theory. However as per the explained theory, it can be seen in Fig. 5(b) that λ_1 immediately reverts back to the normal operating conditions obeying the consensus theory using the proposed resilient mechanism.

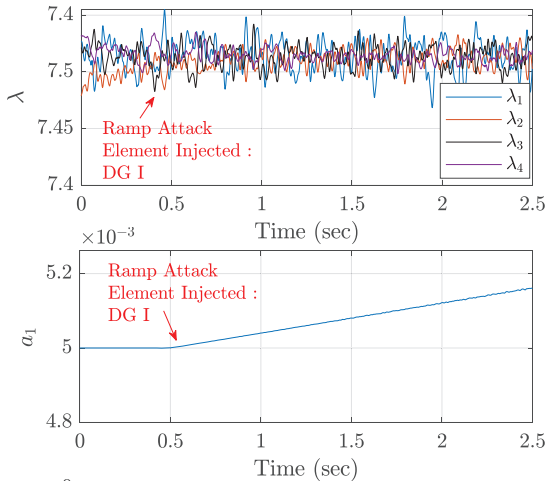

Fig. 6. Performance of AC microgrid with N =4 DGs when a ramp attack element in the form of DIA_1 is injected at t = 0.5 sec.

In Fig. 6, another case study is carried out where a ramp attack element (using the DIA_1 model in (10)) is injected into the generation cost model of DG I. It can be seen that when $\Delta a_k = -0.005t$ is injected at t = 0.5 sec, the incremental cost of each DG remain converged to the pre-attack value. Particularly, the linear regression technique substitutes the attacked signal with the estimated signal upon determination of the error as shown in Fig. 5.

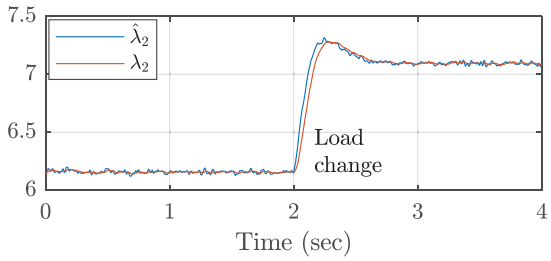

Fig. 7. Estimation by the proposed resilient mechanism under normal operating conditions.

Further in Fig. 7, it can be seen that the estimated signal follows the calculated incremental cost of DG II under normal and dynamic conditions. This allows the proposed mechanism to operate not only like a switching state (Refer to (29)) but it can always be used as a resilient controller to prevent maloperation due to cyber attacks.

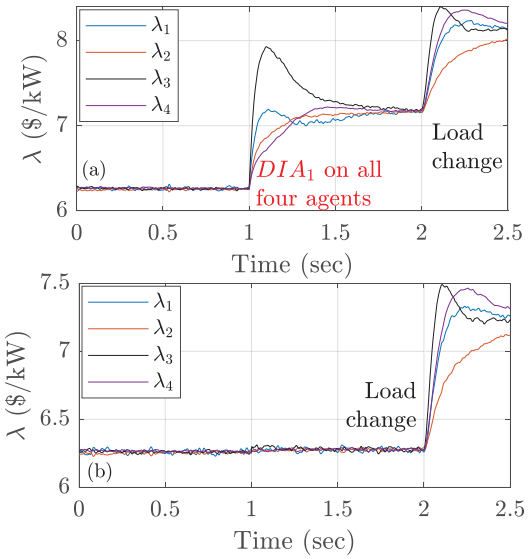

Fig. 8. Performance of AC microgrid with N= 4 DGs : (a) in the absence and, (b) in the presence of the proposed resilient controller when DIA_1 occurs on all the agents simultaneously at t = 1 sec.

Another case study is carried out in Fig. 8 where DIA_1 is conducted simultaneously at t = 1 sec. It can be seen in Fig. 8(a) that when the cost coefficient b_k of each DG (Refer to Table I) is doubled, the incremental cost increases almost by 1 $/kW, which disregards the optimal operation. Consequently for any consecutive change in load, the incremental cost always follows a non-optimal trajectory from here on. However in the presence of the proposed controller, it can be seen in Fig. 8(b) that the regression technique immediately replaces all the attacked λ_k locally with $\hat{\lambda}_k$. As soon as it is replaced, the pre-attack set-point is retained to ensure optimal operation. This highlights the robustness of using a localized

resilient strategy in handling simultaneous attacks, which can be the worse case scenario.

V. Conclusion

This paper presents a linear regression based resilient controller to defend cooperative AC microgrids from data integrity attacks (DIAs). As these attacks cause an increase in the generation cost, the attack elements need to be removed immediately from the control system to prevent divergent non-optimal solutions. In this paper, we have considered two DIAs namely DIA_1 and DIA_2, which supports and blocks the consensus iterative theory, respectively. Hence, the proposed scheme provides a faster elimination of the attacked signal by understanding the intrinsic signal properties more closely and providing an accurate estimation even under attacked conditions. Moreover, it allows to deal with the correctness of measurements in each DG locally without infringing neighbor DG's cost parameters. Due to its intrinsic localized resilient feature, this strategy can be leveraged under worse-case disturbances, such as simultaneous DIA attacks on every DG in the microgrids. Due to the decentralization, it restricts further cyber interactions to ensure the optimal operation of AC microgrids.

Appendix

It is worth notifying that the control parameters are consistent for each DG, unless stated otherwise.
Plant: R_{12}= 0.23 ohms, L_{12}= 0.000318 H , R_{23}= 0.35 ohms, L_{23}= 0.001846 H, R_{34}= 1 ohms, L_{34}= 0.001846 H, C_v = 25μF, L_k = 1.8 mH, L_g = 1.8 mH
Controller: m = 0.00014, n = 0.0013, g_k = 500, σ = 1.4, P^{min} = {0, 0, 0, 0} kW, P^{max} = {4, 4, 4, 4} kW
Inner Current Loop: $K_{pI} = 0.7$, $K_{iI} = 100$
Inner Voltage Loop: $K_{pV} = 0.35$, $K_{iV} = 400$
Frequency Secondary Control: K_{pf} = 1, K_{pf} = 2
Voltage Secondary Control: K_{pE} = 1, K_{pE} = 2
Reactive Power Secondary Control: K_{pE} = 0.0001, K_{pE} = 0.2

References

[1] N. Hatziargyriou, et al., "Microgrids," *IEEE Power and Energy Mag.*, vol. 5, no. 4, pp. 78-94, 2007.

[2] J. Lai, X. Lu, X. Yu, and A. Monti, "Cluster-oriented distributed cooperative control for multiple AC microgrids", *IEEE Trans. Ind. Inform.*, vol. 15, no. 11, pp. 5906-5918, 2019.

[3] C. Zhao, et. al., "Analysis of Consensus-Based Distributed Economic Dispatch Under Stealthy Attacks," *IEEE Trans. Ind. Electr.*, vol. 64, no. 6, pp. 5107-5117, 2017.

[4] M.-Y. Chow, Y. Zhang, and N. Rahbari-Asr, "Consensus based distributed scheduling for cooperative operation of distributed energy resources and storage devices in smart grids," *IET Gener. Transm. Distrib.*, vol. 10, no. 5, pp. 1268-1277, 2016.

[5] W. Zeng, Y. Zhang and M.-Y. Chow, "Resilient Distributed Energy Management Subject to Unexpected Misbehaving Generation Units," *IEEE Trans. Ind. Inform.*, vol. 13, no. 1, pp. 208-216, 2017.

[6] Y. Mo, R. Chabukswar, and B. Sinopoli, "Detecting integrity attacks on SCADA systems," *IEEE Trans. Control Systems Tech.*, vol. 22, no. 4, pp. 1396-1407, 2014.

[7] S. Lusk, D. Lawrence, and P. Suvana, *Cyber-intrusion Auto-response and Policy Management System (CAPMS)*, ViaSat Inc., Boston, MA (United States), 2015.

[8] S Sahoo, T Dragicevic and F Blaabjerg, "Cyber Security in Control of Grid-Tied Power Electronic Converters–Challenges and Vulnerabilities," *IEEE Journ. Emerg. and Select. Topics Power Electron.*, 2019.

[9] S. Sahoo, S. Mishra, J.C.H. Peng, and T. Dragicevic, "A Stealth Attack Detection Strategy for DC Microgrids," *IEEE Trans. Power Electron.*, vol. 34, no. 8, pp. 8162-8174, 2019.

[10] S. Sahoo, J.C.H. Peng, A. Devakumar, S. Mishra, and T. Dragicevic, "On Detection of False Data in Cooperative DC Microgrids–A Discordant Element Approach," *IEEE Trans. Ind. Electron.*, vol. 67, no. 8, pp. 6562-6571, 2019.

[11] M. Conti, N. Dragoni, and V. Lesyk, "A survey of man in the middle attacks," *IEEE Comm. Surveys and Tutorials*, vol. 18, no. 3, pp. 2027-2051, 2016.

[12] S. Sahoo, J. C. -H. Peng, S. Mishra, and T. Dragicevic, "Distributed Screening of Hijacking Attacks in DC Microgrids", *IEEE Trans. Power Electron.*, vol. 35, no. 7, pp. 7574-7582, 2019.

[13] S. Sahoo, J. C. H. Peng, "A Localized Event Driven Resilient Mechanism for Cooperative Microgrid Against Data Integrity Attacks," *IEEE Trans. Cybernet.*, 2020.

[14] S. Sahoo, T. Dragicevic and F. Blaabjerg, "An Event-Driven Resilient Control Strategy for DC Microgrids," *IEEE Trans. Power Electron.*, 2020.

[15] S. Sahoo, T. Dragicevic and F. Blaabjerg, "Resilient Operation of Heterogeneous Sources in Cooperative DC Microgrids," *IEEE Trans. Power Electron.*, 2020.

[16] S. Sahoo, J. C. H. Peng, "A Localized Event Driven Resilient Mechanism for Cooperative Microgrid Against Data Integrity Attacks," *IEEE Trans. Cybernet.*, 2020.

[17] S. Sahoo, Y. Yang and F. Blaabjerg, "Resilient Synchronization Strategy for AC Microgrids Under Cyber Attacks," *IEEE Trans. Power Electron.*, 2020.

[18] N. Rahbari-Asr, U. Ojha, Z. Zhang, and M.-Y. Chow, "Incremental welfare consensus algorithm for cooperative distributed generation/demand response in smart grid," *IEEE Trans. Smart Grid*, vol. 5, no. 6, pp. 2836-2845, Nov. 2014.