Aalborg Universitet

AALBORG UNIVERSITY

A Localized Event Driven Resilient Mechanism for Cooperative Microgrid Against Data Integrity Attacks

Sahoo, Subham; Chih-Hsien Peng, Jimmy

Published in:
I E E E Transactions on Systems, Man and Cybernetics, Part B: Cybernetics

DOI (link to publication from Publisher):
10.1109/TCYB.2020.2989225

Creative Commons License
Unspecified

Publication date:
2021

Document Version
Accepted author manuscript, peer reviewed version

Link to publication from Aalborg University

Citation for published version (APA):
Sahoo, S., & Chih-Hsien Peng, J. (2021). A Localized Event Driven Resilient Mechanism for Cooperative Microgrid Against Data Integrity Attacks. *I E E E Transactions on Systems, Man and Cybernetics, Part B: Cybernetics*, *51*(7), 3687-3698. Article 9098896. https://doi.org/10.1109/TCYB.2020.2989225

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal -

Take down policy
If you believe that this document breaches copyright please contact us at vbn@aub.aau.dk providing details, and we will remove access to the work immediately and investigate your claim.

Downloaded from vbn.aau.dk on: December 05, 2025

A Localized Event Driven Resilient Mechanism for Cooperative Microgrid Against Data Integrity Attacks

Subham Sahoo, *Member, IEEE* and Jimmy Chih-Hsien Peng, *Member, IEEE*

***Abstract*—This paper investigates the impact of data integrity attacks (DIAs) on cooperative economic dispatch of distributed generators (DGs) in an AC microgrid. To establish resiliency against such attacks and ensure optimal operation, a localized event driven attack-resilient scheme is proposed. Most of the existing works examine neighboring information to infer the presence of DIAs, where the detection is limited to events such as multiple link failures. Two kinds of DIAs are considered in this paper – namely fault and random attacks, which are segregated based on the final values of consensus updates. Firstly, to improve the robustness of the detection theory, a localized resilient control update is designed by modeling each DG with a reference incremental cost. Secondly, an event driven control signal is generated for the local incremental cost and held upon detection of attacks, to prevent malicious data from propagating to the neighboring nodes. The proposed strategy acts immediately upon detection of data integrity attack to ensure maximization in the economic profit. Further, the proposed detection approach is theoretically verified and validated using simulation conditions.**

***Index Terms*—AC microgrid, resilient control, data integrity attack, cooperative control.**

I. Introduction

ENERGY management system (EMS) is an effective mechanism to handle the generation profiles of different sources while attaining their maximum economical benefits [1]. Since renewable energy sources are rapidly being integrated into modern power systems, the complexity in solving multi-objective EMSs increases significantly owing to their intermittent nature [2]. To this end, microgrids have been identified as key enablers behind integration of renewable energy sources owing to the flexibility of their operation in both grid-connected and islanded modes [3]. To date, generation dispatching is usually carried out in a centralized manner to minimize the operational cost using hierarchical stages of optimization including, integer programming [4], artificial intelligence based techniques [5], etc. To achieve more flexibility in control under transmission delay and information failure, cooperative/distributed controllers with robust performance towards cyber layer imperfections are preferred in recent times [6]. They establish a scalable platform with an even distribution of the computational resources across the network. This preempts into increasing the reliability of operation by implementing cooperative control in microgrids to form *cooperative microgrids*. Meanwhile, many cooperative energy management schemes have been devised to incur significant reduction in the power management cost and carbon emissions [7]-[8]. In contrast to the operation in longer time scales with static demand input in the centralized scheme, cooperative dispatching also allows online actions for every load change in real-time [9]- [10]. As a result, it improves the economic profile of the generators in a given duration.

The primary assumption is that the economic dispatch (ED) operation is conducted in a reliable cyber network reporting *true* measurements [11]-[12]. Any physical violation or erroneous measurement in the EMS can cause the microgrid to operate in non-optimal and non-feasible manner [13]-[17]. Cyber attacks using illegitimate data intrusion into the EMS can interrupt optimal dispatching of sources in a microgrid. As a consequence, such events entail increase in the total generation cost.

Considerably less effort has gone into analyzing cyber attacks in cooperative optimization. To name a few, the authors in [18] have designed a reputation-based detection algorithm to detect attacks on the ED problem. However, it is not fully cooperative, as the algorithm requires a centralized control center. These centralized mechanisms are highly prone to single point-of-failure, which can easily disrupt the optimal operation of the system. A similar hypothesis on the economic impact of DC optimal power flow (DC-OPF) under cyber attacks is studied in [19]. In this study, cooperative ED behaves in a different manner as opposed to DC-OPF, following the global equality constraint for power balancing. 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.

From the perspective of an adversary, the goal is to increase the generation cost by hacking critical parameters and leading to a reduction in the energy efficiency of the system [20]. The goal of cooperative real-time ED is to ensure that the final state of convergence leads to unbiased operation inside the constrained optimization space. However, data intrusion from stealth attacks is possible, as demonstrated in [9]. Such attacks are capable of increasing the generation cost without causing any obvious indications of power imbalance. Moreover, Zeng, *et. al.* in [21] have modeled a DIA to manipulate the power dispatch of each generator to gain monetary benefits. To for-

This work was supported by the National Research Foundation (NRF) Singapore under the Singapore-ETH Centre (SEC).

S. Sahoo is with the Department of Energy Technology, Aalborg University, Aalborg 9220, Denmark (e-mail: sssa@et.aau.dk)

J. C. -H. Peng is with the Department of Electrical and Computer Engineering, National University of Singapore, Singapore, 119007 (e-mail: jpeng@nus.edu.sg)

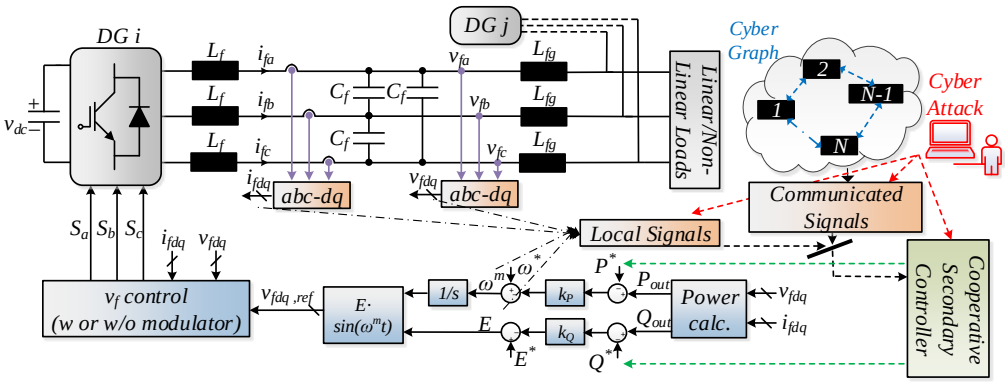

Fig. 1. A single-line diagram of a cyber-physical AC microgrid consisting of N DGs managed by a cooperative cyber topology. The data integrity attack is highlighted in red to change the cost parameters, affecting the optimal operation.

mulate an attack-resilient mechanism, a two-hop neighboring information based verification algorithm to detect and restore the system from DIAs is reported in [22]. 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 compromised link or link failure. Another limitation is that the detection approach is overly dependent on the network communication delay, which can hinder the subsequent corrective actions. Hence, the scheme suffers from coordinated attacks on the cyber links such as denial of service (DoS) [23] and man-in-the-middle (MITM) [24] attacks.

To address these limitations in the literature, this paper proposes a unified and localized attack-resilient model to prevent the impact of DIAs in cooperative AC microgrid. Two attack models have been considered, namely fault and random attacks. Basically, fault attacks cause an implicit change in cost parameters, which maloperates as per the dynamic consensus theory to reach an arbitrary value. To prevent the system from such attacks, a resilient control update is designed using the error in local measurements to cancel the effect of the mentioned attack. On the other hand, as random attacks do not update with the iterations, a localized estimation of the incremental cost model is computed using a reference model to obtain the error in cost parameters. An error in the cost parameters triggers an *event* for the same node, indicating a DIA in the node. To protect against random attacks, a localized event driven incremental cost data is held by the controller using the local measurements from the pre-triggered instant. As a result, the propagation of the attack element to the neighbors is prohibited and the held value ensures the optimal operation. This scheme serves two advantages: 1) the privacy of each unit is secured, 2) it operates without involving neighboring measurements, and hence remain unaffected by adversarial actions such as delays, link failure, DoS and MITM attacks. As opposed to the existing resilient schemes studied in [21]-[22], the proposed localized event-driven mechanism is impervious to cyber intrusions such as failure or cyber attack on a cyber link. This enhances the security of cooperative microgrids against data integrity attacks. Moreover, the proposed attack-resilient concept can be extended to cooperative grid-connected distribution systems. To sum up, the basic contributions of this paper are as follows:

1) A unified localized attack-resilient scheme is proposed to maintain optimality and feasibility of cooperative economic dispatch in AC microgrid. To the best of authors' knowledge, the proposed localized event driven resilient scheme has never been proposed in the realm of detecting DIAs in cooperative systems.
2) For fault attacks, a resilient control update is designed only using the localized error of change in cost parameters to diminish its effect. It is not susceptible to intermittent conditions or adversaries causing multiple link failures.
3) For random attacks, a localized event driven solution is used to hold the estimated value upon detection of the attack. As a result, it improves the robustness of the system to operate in its optimal state even under attacks.

The rest of the paper is organized as follows. Section II details out the cooperative active power control of AC microgrid. Using the defined theory in Section II, the problem of stealth data integrity attacks is formulated in Section III with a case study. It also provides a theoretical analysis to establish that the abovementioned attack cause an increase in generation cost. Further, Section IV depicts the proposed attack resilient scheme. It has been verified using simulation cases, which are demonstrated in Section V. Finally, Section VI provides the concluding remarks.

II. Cooperative Architecture and Control of AC Microgrid

This paper considers an autonomous AC microgrid with N distributed generators (DGs), as shown in Fig. 1. It operates using two hierarchical layers, namely primary and secondary layer. Since it utilizes cooperative control mechanism, the secondary controller operates using local and neighboring measurements only.

For the purpose of brevity of this paper, the basic equations of power controller and the low-pass filter used in autonomous inverter based systems can be referred from [6]. In the cyber layer, an undirected graph is considered, where vertices denote

the points of connections of physical DGs. Since the scope of the paper is based on mitigating data integrity attacks which alter the active power commands to disregard optimal power dispatch, only the measurements concerning active power secondary control layer are considered after this point. More details on reactive power sharing and average voltage regulation using distributed control in islanded microgrids can be referred from [25].

A. Cyber Preliminaries

Each vertex sends and receive $\psi_j = \{\lambda_j\}$ from its neighboring vertices to achieve optimal power dispatch, where λ_j denotes the incremental cost of the neighboring agents. Additionally, P_k^{out} and ω_i denote the measured active power and frequency of i^{th} DG, which are used locally. The detailed equations of the cost function of each DG and its implementation will be covered later in the paper. Each agent is represented via a node and a communication digraph via edges using an adjacency matrix $\mathbf{A} = [a_{ij}] \ \epsilon \ R^{N\times N}$. The communication weights are given by:

$$a_{ij} = \begin{cases} h, & \text{if } (x_i, x_j) \ \epsilon \ \mathbf{E} \\ 0, & \text{else} \end{cases}$$

where h denotes a positive quantity, $\mathbf{E}$ is an edge connecting two nodes, with x_i and x_j being the local and neighboring node respectively. Mathematically, the incoming information matrix can be denoted by $\mathbf{Z}_{in} = \sum_{i \ \epsilon \ N} a_{ij}$. Hence, if both matrices match each other, the Laplacian matrix $\mathbf{L}$ is *balanced*, where $\mathbf{L} = \mathbf{Z}_{in} - \mathbf{A}$ and its elements are given by:

$$l_{ij} = \begin{cases} \deg(n_i) & , i = j \\ -1 & , i \neq j \\ 0 & , \text{otherwise} \end{cases} \tag{1}$$

where $\deg(n_i)$ is the degree of i^{th} agent.

Remark I: As per the synchronization law [31], all the agents participating in cooperative control will achieve consensus using $\dot{\mathbf{x}} = -\mathbf{L}\mathbf{x}$ for a well-spanned matrix L such that $\lim_{t\to\infty} x_i(t) = c, \ \forall i \ \epsilon \ N$, where c is the steady-state reference and N is the number of agents.

B. Cooperative Control of AC Microgrid

As per the conventional droop control theory for autonomous DGs, the active power in i^{th} DG is controlled using:

$$\omega_i^m = \omega^* - m_i \Delta P_i^{pu} \tag{2}$$

where m_i and ω^* denote the active power droop gain and global frequency reference in the considered system respectively. Further, $\Delta P_i^{pu} = \frac{P_i^{out} - P_i^*}{P_i^{max}}$, where P_i^{max} is the maximum active power in i^{th} DG. To achieve different control paradigms, the hierarchical controller is interfaced into the primary control layer accordingly. Since primary controller always operates with an error, secondary controllers are employed to compensate the error for the abovementioned undirected cyber graph using the local and the neighboring information, as highlighted in Fig. 1.

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:

$$C_i(P_i) = a_i P_i^2 + b_i P_i + c_i \tag{3}$$

where a_i, b_i and c_i are the cost coefficients of i^{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:

$$\min \ C(P) = \sum_{i=1}^{N} C_i(P_i) \tag{4}$$

$$\text{s.t.} \sum_{i=1}^{N} P_i = P^D, \ P_i^{min} < P_i < P_i^{max}, \ \forall i \epsilon N$$

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

$$\mathcal{L}_\lambda = \sum_{i=1}^{N} C_i(P_i) + \lambda_i \sum_{i=1}^{N} (P_i^D - P_i) \tag{5}$$

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

$$\begin{cases} P_i(0) = \begin{cases} P_i^{min}, \ P_i^D < P_i^{min} \\ P_i^D, \ P_i^{min} < P_i^D < P_i^{max} \\ P_i^{max}, \ P_i^D > P_i^{max} \end{cases} \\ \lambda_i(0) = 2a_i P_i(0) + b_i \\ \eta_i(0) = P_i^D - P_i(0) \end{cases} \tag{6}$$

To minimize the total generation cost subjecting to the equality constraints, it is required that the incremental cost of each DG be equal [26], which is carried out using a power correction term ΔP_i, given by:

$$\Delta \dot{P}_i = \sum_{j \ \epsilon \ N_i} a_{ij}(\lambda_j - \lambda_i) \tag{7}$$

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

$$P_i^* = P_i^{initial} + k_i \int (\omega^* - \omega_i(t)) + \Delta P_i. \tag{8}$$

Substituting (8) in (2), the active power droop control law operates to restore frequency of each bus to the rated value and participates in optimal load sharing. Hence using (2)-(8), a unified cooperative control structure for active power is devised for AC microgrid. However, any change in cost parameters or displace 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. Hence, the system response under such attacks is studied in detail in the following section.

III. Modeling of Data Integrity Attacks

In this section, we first study the modeling of DIA in a cooperative microgrid. Secondly, the online stealthiness of such attacks to reach non-optimal state considering bounded generation is demonstrated using a case study. Moreover, the deviation of the cost function under attacks is verified in this section.

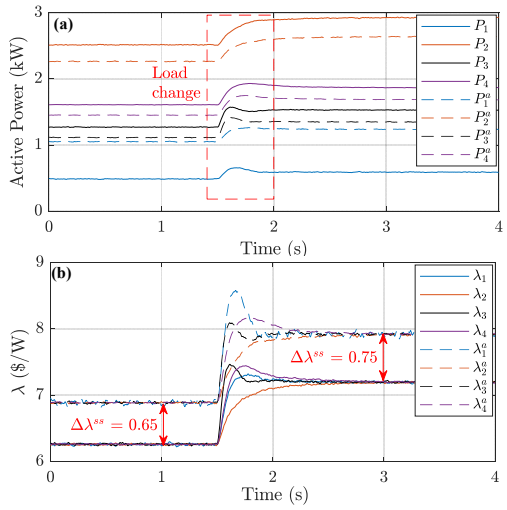

Fig. 2. Comparative evaluation of (a) active power, and (b) incremental cost of DGs under no attack (solid lines) and DIA attack (dotted lines) – Change in cost parameters causes a drift in the convergence of incremental cost λ causing a non-optimal operation.

Two types of DIAs have been considered, namely fault and random based attacks. Basically in the fault DIA, the local incremental cost λ_i is updated with every iteration using:

$$\lambda_i(k+1) = \lambda_i(k) + \sum_{j \ \epsilon \ N_i} w_{ij}(\lambda_j(k) - \lambda_i(k)) + \zeta u^a_{\lambda_i} \quad (9)$$

where $u^a_{\lambda_i}$ 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 otherwise. This can be done by changing the cost parameters in the local DG using:

$$u^a_{\lambda_i} = \begin{cases} -\Delta a_i P_i \\ -\Delta b_i \end{cases} \quad (10)$$

where Δa_i and Δb_i denote positive attack elements, when added to the cost parameters in (10) increase the generation cost per unit power and fixed cost, respectively. Using (10), it can be concluded that the consensus algorithm maloperates during the updating process to converge to an arbitrary value. Such attacks are only possible when the compromised value of the incremental cost is used locally and in the neighboring units, to provide a symmetric effect along the Laplacian graph. On the other hand for random attacks, which are also commonly referred as the byzantine attacks [27], the current estimate is substituted to another value, which hinders the update process for each iteration. Using the random DIA, λ_i settles down to a constant value using a set of attack elements, given by:

$$\lambda_i(k) = (1-\kappa)\lambda_i(k) + \kappa\lambda^c_i \quad (11)$$

where $\kappa = 1$ denote the presence of random DIA, or otherwise. Moreover, λ^c_i denotes a constant valued attack element, which does not update in an iterative manner. It behaves as a constant value in the dynamic consensus theory, providing arbitrary changes for the remaining DGs. More details on byzantine attacks in misbehaving agents are given in [28], [29].

Similar definition of both considered attacks can be found in [30]. In this study, the attacks are resolved using a two-hop neighborhood algorithm. However, this scheme is highly vulnerable to DoS or MITM attacks in the cyber layer since the incremental cost received from the neighbors could be compromised.

Using (4)-(8), the secondary controller objectives for economic dispatch in microgrids using a cooperative cyber graph can be written (detailed control formulation is presented in [10]) as:

$$\lim_{t\to\infty} \lambda_i(t) = \lambda^{opt}, \ \lim_{t\to\infty} P_i(t) = P^{opt} \ \forall \ i \in N \quad (12)$$

where λ^{opt} and P^{opt} denote the optimal incremental cost and active power in the absence of attack elements, respectively. However in the presence of cyber attacks, the attacker may cause scenarios leading to generation-demand imbalance, giving divergent solutions for (8). Such attacks may easily expose the attacker following the extended concepts of synchronization law in [31]. It is worth notifying that the attacks considered in this paper operate under the optimization space bounded by the constraints in (4). Hence, the adversary can cause online stealth attacks modeled using (10)-(11), to get:

$$\lim_{t\to\infty} \lambda_i(t) = \lambda^{a*}, \ \lim_{t\to\infty} P_i(t) = P^{a*} \ \forall \ i \in N \quad (13)$$

where λ^{a*} and P^{a*} denote the optimal incremental cost and active power in the presence of attack elements, respectively. Moreover since $\lambda^{opt} \neq \lambda^{a*}$, the system converges to a non-optimal state due to the attack thereby, reducing the overall generation cost efficiency. The convergence analysis within the constraints in the presence of such attacks can be referred from [9].

In cooperative ED problem, as long as the error in (7) between the incremental cost of local agents and neighbors is zero, the system operator in every agent would seemingly believe that an optimal solution is always reached. Therefore, determination of such attacks in cooperative networks is a challenging task.

To provide with the basic understanding of such attacks, a case study on a microgrid with N = 4 DGs in Fig. 2 is done using a fault attack using increase in the cost parameters of DG I. It can be seen that the system response is similar in both cases, in the absence of attack (represented by solid lines) and in the presence of attack (represented by dotted lines). The realism behind its operation under such attacks is unknown, when seen from a given agent since adequate information on the total active power demand is not centrally available. Moreover, it can be seen in Fig. 2(b) that the steady state value of the incremental cost initially under attacks is raised by 0.85 $/W, and it increased to 1.05 $/W with the increase in load at t = 1.5 s. It clearly suggests that minimization of (4) is violated under attacks. Hence, the abovementioned case study

raises serious concerns on detecting and mitigation of such attacks in cooperative microgrid, since the local neighborhood error in (7) converges to zero.

Considering the problem formulation of data integrity attacks in microgrids using (13), a theoretical analysis is provided to estimate the final generation under attack (in only one node) and its difference with the optimal generation cost under no attack. The analysis is separately carried out for active power generation within and outside the limits in (6).

A. Inside the Bounds $[P_i^{min}, P_i^{max}]$

Rearranging the equality constraint in (4), the final settling value of incremental cost under attack using (6) can be written as:

$$\lim_{t\to\infty} \lambda_i(t) = \lambda^{a*} = \frac{\sum_{i\epsilon N} P_i^D - \sum_{i\epsilon N} \alpha_i^{a*}}{\sum_{i\epsilon N} \beta_i^{a*}} \tag{14}$$

where $\alpha_i^{a*} = \alpha_i + \alpha_i^a$ and $\beta_i^{a*} = \beta_i + \beta_i^a$. Moreover, $\alpha_i = \frac{-b_i}{2a_i}$, $\beta_i = \frac{1}{2a_i}$ and α_i^a, β_i^a are the attacked elements to change the cost parameters of i^{th} DG. As discussed above, such attacks can be categorized as fault attacks, where the convergence is feasible, however to a non-optimal setpoint. On the other hand, for no attack, the steady state of incremental cost using (10) can be given by:

$$\lim_{t\to\infty} \lambda_i(t) = \lambda^{opt} = \frac{\sum_{i\epsilon N} P_i^D - \sum_{i\epsilon N} \alpha_i}{\sum_{i\epsilon N} \beta_i} \tag{15}$$

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

$$\lambda_i^{a*} = \frac{\lambda_i \sum_{i\epsilon N} \beta_i - \alpha_i^a}{\sum_{i\epsilon N} \beta_i + \beta_i^a} \tag{16}$$

Rearranging terms in (16), we get:

$$\lambda_i^{a*}\beta_i^a = (\lambda_i^{opt} - \lambda_i^{a*}) \sum_{i\ \epsilon\ N} \beta_i^a - \alpha_i^a \tag{17}$$

Denoting (4) in terms of α_i, β_i and γ_i, the operating cost can be expressed as:

$$C_i(P_i) = \frac{(P_i - \alpha_i)^2}{2\beta_i} + \gamma_i \tag{18}$$

where $\gamma_i = c_i - \frac{b_i^2}{4a_i}$. Furthermore, using (14)-(18), the cost function under attacks C_i^a is given by:

$$C_i^a(P_i^a) = \frac{(\lambda_i^{a*}\beta_i^{a*} + \alpha_i^a)^2}{2\beta_i} + \gamma_i \tag{19}$$

Substituting (17) in (19), we get:

$$C_i^a(P_i^a) = \frac{[\lambda_i^{a*}\beta_i^a + (\lambda_i^{opt} - \lambda_i^{a*}) \sum_{i\epsilon N} \beta_i]^2}{2\beta_i} + \gamma_i \tag{20}$$

Under no attack, (18), the cost function can be simply written as $C_i(P_i) = \frac{(\beta_i \lambda^{opt})^2}{2\beta_i} + \gamma_i$. Moreover, the difference between the cost function under attack and no attack can be formulated as:

$$C_i^a(P_i^a) - C_i(P_i)$$

$$= \frac{[\lambda_i^{a*}\beta_i^a + (\lambda_i^{opt} - \lambda_i^{a*}) \sum_{i\epsilon N} \beta_i]^2 - (\beta_i \lambda^{opt})^2}{2\beta_i} \tag{21}$$

$$= \frac{[(\beta_i^a + \sum_{i\epsilon N} \beta_i)\lambda^{opt} + (\beta_i^a - \sum_{i\epsilon N} \beta_i)\lambda^{a*}]}{2\beta_i} \tag{22}$$

However, since the cost parameters in the non-attacked nodes are unchanged, the difference in the cost function only due to the non-optimal incremental cost λ^{a*} is given by:

$$C_i(P_i) - C_i^*(P_i^a) = \frac{\beta_i[\lambda^{opt2} - \lambda^{a*2}]}{2}. \tag{23}$$

Using (22)-(23), we get:

$$\sum_{i\epsilon N, i\neq i^a} [C_i(P_i) - C_i^*(P_i^a)] + C_i(P_i) - C_i^a(P_i^a) = \frac{(\beta_i^a - \sum_{i\epsilon N} \beta_i)(\sum_{i\epsilon N} \beta_i)(\lambda^{opt} - \lambda^{a*})^2}{2\beta_i} \tag{24}$$

Remark II: Using (24), it is sufficient to prove that the cost function without and with an attack will be different since $\lambda^{a*} \neq \lambda^{opt}$. Since the change in cost parameters can induce fault attacks, it can also be concluded from (24) that large error deviation in $(\lambda^{opt} - \lambda^{a*})$ using random attacks explicitly causes large deviation in the cost parameters of the attacked node.

B. Outside the Bounds $[P_i^{min}, P_i^{max}]$

As the objective function in (4) is closely convex, there exist only one solution for P^{opt} and consequently λ^{opt}. Suppose there exists no α_i^a and β_i^a, which can change the optimal setpoint. As a result, the incremental cost and active power under attacks will satisfy $\lambda_i^{a*} = \lambda_i^{opt}$ and $P_i^{a*} = P_i^{opt}$. Hence,

$$P_i^{a*} = \begin{cases} P_i^{max}, \lambda_i^{a*} \geq \lambda_i^{max^a} \\ \beta_i^{a*}\lambda^{a*} + \alpha_i^{a*}, \lambda_i^{min^a} < \lambda_i^{a*} < \lambda_i^{max^a} \\ P_i^{min}, \lambda_i^{a*} \leq \lambda_i^{min^a} \end{cases}$$

$$= \begin{cases} P_i^{max}, \lambda_i^{opt} \geq \lambda_i^{max} \\ \beta_i\lambda^{opt} + \alpha_i, \lambda_i^{min} < \lambda_i^{opt} < \lambda_i^{max} \\ P_i^{min}, \lambda_i^{opt} \leq \lambda_i^{min} \end{cases} \tag{25}$$

holds true, where $\lambda_i^{min} = \frac{1}{\beta_i} P_i^{min} - \frac{\alpha_i}{\beta_i}$, $\lambda_i^{max} = \frac{1}{\beta_i} P_i^{max} - \frac{\alpha_i}{\beta_i}$, $\lambda_i^{min^a} = \frac{1}{\beta_i^{a*}} P_i^{min^a} - \frac{\alpha_i^{a*}}{\beta_i^{a*}}$ and $\lambda_i^{max^a} = \frac{1}{\beta_i^{a*}} P_i^{max^a} - \frac{\alpha_i^{a*}}{\beta_i^{a*}}$. However, it can be observed that α_i^a and β_i^a must exist and thus, (25) does not hold. This justifies that the operation outside the active power generation bounds due to DIAs is not possible as the unique solution for incremental cost is always bounded between $[P_i^{min}, P_i^{max}]$ for i^{th} agent.

Remark III: The optimality is lost when the mentioned attacks are injected into any of the nodes, even though a feasible solution is reached for a given loading condition. The deviation of total generation caused by these attacks are highly dependent on the magnitude of attack elements and the generation bounds. Meanwhile, the cost parameters aren't consistent for every DG, which suggests different manipulation ranges for each node.

As a result from a techno-economic perspective, such attacks cause reduction in energy efficiency. Hence, a localized event based attack resilient mechanism is proposed in this paper to defend the system against such attacks.

IV. Proposed Localized Event Driven Attack Resilient Mechanism

A. Design of Attack Resilient Mechanism

The basic philosophy behind the proposed scheme lies with the model-based event detection, which identifies the change of parameters in the cost function model. It should be noted that an event driven mechanism under conventional schemes is applicable to reduce the communication burden. By this definition, the updated data in case of events, such as load change, is transmitted to the neighboring DGs, which serves as an economic option as compared to the time-triggered schemes [33]. However since this paper is focused on identifying and mitigating DIAs, the proposed strategy is designed in a manner such that it operates using local measurements only during the events, i.e., *attacks*.

Definition 1: An ***event*** *can be defined as an element in the control system which is responsible for causing any significant changes in model parameters. Hence, detection of such events has been used to alleviate security.*

Using (24) and Definition 1, it can be proved that a DIA in any unit qualifies as a localized event. To detect such events, a reference model of the cost function is defined within the limits $[\lambda_i^{min}, \lambda_i^{max}]$, which is given by:

$$\lambda_i^r(t) = 2a_i^r P_i(t) + b_i^r \tag{26}$$

where $\bullet^r$ denote the reference value of a quantity using the local active power measurement. Since the reference model of the cost function is always constant for a DG, the local active power measurement is used to estimate the cost parameters to determine the possibility of an *event*. Hence, the estimated cost parameters for operation within the active power bound $[P_i^{min}, P_i^{max}]$ and the incremental cost bound $[\lambda_i^{min}, \lambda_i^{max}]$ are given by:

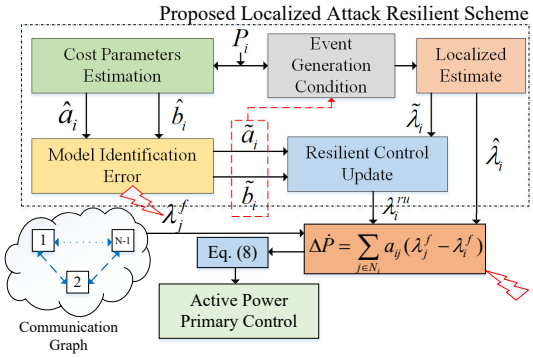

Fig. 3. Control diagram of the proposed attack resilient controller for i^{th} DG to defend against data integrity attacks - attack on the communicated λ (random) as well as on the local control input (fault).

$$\hat{a}_i(t) = \frac{\lambda_i(t) - b_i^r}{2P_i(t)} \tag{27}$$

$$\hat{b}_i(t) = \lambda_i(t) - 2a_i^r P_i(t) \tag{28}$$

where $\hat{\bullet}$ denote the estimated value of the cost parameters. Using (24)-(28), any attack on the cost parameter can be identified by monitoring non-zero values for the model identification error, calculated using:

$$\tilde{a}_i(t) = a_i^r - \hat{a}_i(t) \tag{29}$$

$$\tilde{b}_i(t) = b_i^r - \hat{b}_i(t) \tag{30}$$

where $\tilde{\bullet}$ denote the model identification error set of the cost parameters. Hence by definition, the model identification error is used to determine such attacks and is also a necessary criteria to trigger localized events.

Definition 2: Any non-zero value in the online model identification of the cost parameters in i^{th} DG indicate that a data integrity attack is conducted in the same unit.

Using Definition 2, attack based events Ξ are detected locally using:

$$\Xi = \begin{cases} 0, \text{if } ||\rho_i|| \leq \bar{e} \\ 1, \text{else} \end{cases} \tag{31}$$

where $\rho_i = [\tilde{a}_i, \tilde{b}_i]$. Similar to the event-triggered philosophy [33], the event is triggered when $||\rho_i(t)||$ reaches the upper bound $\bar{e}$, or updates to zero when otherwise. Using (31) as the event-triggering criterion, a localized estimation of $\hat{\lambda}_i$ is done using the reference cost parameters using:

$$\hat{\lambda}_i(t) = 2a_i^r P_i(t) + b_i^r, \ t \in [t_k^{\rho_i}, t_{k+1}^{\rho_i}] \tag{32}$$

where $[t_k^{\rho_i}, t_{k+1}^{\rho_i}]$ are the consecutive triggered instants. A two-fold validation in addition with (31) is done to identify the presence of such attacks, which can be ensured using:

$$\tilde{\lambda}_i(t) = \hat{\lambda}_i(t_k^{\lambda_i}) - \lambda_i(t) \tag{33}$$

Additionally, any non-zero value for $||\tilde{\lambda}_i||$ also indicates the presence of an attack. Hence, an attack resilient update λ_i^{ru} is designed for i^{th} DG using:

$$\lambda_i^{ru}(t) = ||\tilde{\lambda}||_i^{\sigma}(t)(\tilde{a}_i(t) + \tilde{b}_i(t)) \tag{34}$$

where σ is a scaling factor. As a result, the update obtained in (34) is used as a correction factor to obtain the final incremental cost λ_i^f, given by:

$$\lambda_i^f(t) = \lambda_i(t) + \lambda_i^{ru}(t) \tag{35}$$

Algorithm 1: Resilient Mechanism for Fault and Random Attacks

```
ζ = 0;
while (||ρ|| < ē) && (ζ == 1) do
    Check (31);
    if attack == fault then
        The resilient update in (34) operates
         immediately;
        Link Disable_N = No;
    else
        Link Disable_N = Yes;
        (32) operates for the attacked agent;
    end
end
```

Remark IV: The resilient update diminishes the effect of change in parameters using the large difference in (33) as an adaptive gain. This gain can be scaled up by increasing the value of σ. As a result, the final change in cost parameters taking into account the resilient update minimizes following a fault attack. Finally, the incremental cost obtained in (35) can be used in (7) for the respective DGs to defend against such attacks.

However in case of random attacks, the attacked DG controller does not update (7), which as a consequence assigns λ_i^c as the reference to be tracked by other DGs. For unprecedented values of λ_i^c causing an random attack, the solutions may diverge leading to stability issues and over generation scenarios for DG(s). To briefly summarize the proposed resilient control strategy, Algorithm I is provided with sign conventions `attack` and `fault` denoting the system operation states. Moreover, $\texttt{Link Disable}_N$ denotes disabling the cyber link with the neighbors. Since the event generation process is also co-aligned with the existing secondary controller, it is vital to inspect the stability of the algorithm.

B. Stability Analysis

To obtain input-to-state stability, we consider a quadratic Lyapunov candidate V for the system, where $V = x^T P x$ with $x = [P, \omega, \Delta P, \lambda]$. It is important to regard the state feedback law $u = -Kx$ to design V, where the inputs can be deemed as the cooperative secondary outputs using Laplacian matrix $\mathbf{L}$ as the input matrix [6]. To establish stability, a positive-definite matrix Q with ϕ_Q as its smallest singular value can be defined as:

$$(A + BK)^T P_1 + P_1(A + BK) = -Q \tag{36}$$

where P_1 is a positive-definite matrix. More details on the state and input matrices can be referred from the detailed small-signal model of cooperative AC microgrids in [32]. Taking the derivative of V, we get

$$\dot{V} = x^T[(A + BK)P + P(A + BK)]x + 2x^T PBK\rho \tag{37}$$

$$= x^T[(\hat{A} + \hat{B}K + \tilde{A} + \tilde{B}K)^T P + \\ +P(\hat{A} + \hat{B}K + \tilde{A} + \tilde{B}K)]x + 2x^T P(\hat{B} + \tilde{B})K\rho \tag{38}$$

where $\hat{A}$, $\hat{B}$ and $\tilde{A}$, $\tilde{B}$ consist of the estimated and model identification error of cost parameters in (27)-(28) and (29)-(30) respectively. Substituting (36) in (38), we get:

$$\dot{V} = -x^T Q x + x^T[(\tilde{A} + \tilde{B}K)^T P + P(\tilde{A} + \tilde{B}K)]x \\ +2x^T P(\hat{B} + \tilde{B})K\rho \tag{39}$$

Upper-bounding (39), we get:

$$\dot{V} \leq (-\phi + 4\bar{e}LP)||x||^2 + 2\bar{e}LP||x||||\rho|| \tag{40}$$

To achieve asymptotic stability, (40) is equated to zero, we get:

$$||\rho|| \leq \frac{\phi_Q - 2\bar{e}LP}{\bar{e}LP}||x|| \tag{41}$$

Remark V: In (41), it is intuitive to follow that the event-triggering is dependent on the model identification error space, governed by the value of $\bar{e}$. A lower the value of $\bar{e}$ corresponds to a higher sensitivity using the proposed mechanism and vice-versa.

TABLE I
COST COEFFICIENTS OF DG

DG	I	II	III	IV
a	0.005	0.0025	0.004	0.006
b	1	0.6	1.8	0.45

Remark VI: It should be noted that since the cooperative controllers are equipped to work under the bounded space of active power generation, the proposed resilient mechanism will perform satisfactorily regardless of the attack signal amplitude. Since the value of $\bar{e}$ is very small, any increase in the incremental cost beyond $\bar{e}$ due to a DIA will immediately be subjected to the compensating action by the resilient update.

A detailed performance evaluation for different values of $\bar{e}$ is provided in the next section. Finally, the proposed attack resilient mechanism, as shown in Fig. 3, can be used to defend the system against likely data integrity attacks to disrupt optimal operation of microgrid.

V. SIMULATION RESULTS

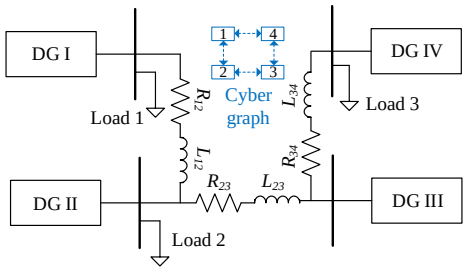

Fig. 4. Single-line diagram of the physical AC microgrid and its corresponding cyber graph (dashed arrows).

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. A distributed secondary controller is employed to regulate the error of incremental cost and frequency between the local as well as the neighboring DGs. The i^{th} DG is connected to the j^{th} DG via line parameters given by R_{ij} and L_{ij}. It should be noted that each DG has different cost function parameters. All the plant and control parameters are provided in Appendix. The cost coefficients of each DG are tabulated in Table I. All the scenarios have been discussed in MATLAB/SIMULINK environment.

Firstly, a case study on the considered system is carried out in Fig. 5(a), where λ_1 is substituted to a value of 7.8 using (11) by the adversary at t = 0.5 s. It can be seen that as soon as λ_1 settles to 7.8, the remaining DGs track the set-point as a reference using the consensus theory. Under such circumstances, the propagation of λ_i^c is first stopped by disabling the cyber link to the neighboring DGs. Upon securing

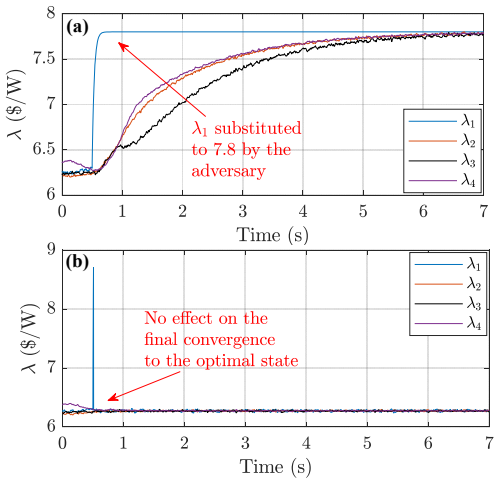

Fig. 5. Performance of AC microgrid (a) without, and (b) with the proposed attack detection scheme for random attacks at t = 0.5 s in DG I: $\hat{\lambda}_1$ is immediately held upon the detection of attack.

the operation of the remaining DGs, owing to the large error in (33), the event-generated $\hat{\lambda}_i$ is instead used locally in the attacked DG. By doing so, the local neighborhood error in (7) converges back to zero in the steady-state. Additionally, when the model identification error ρ_i settles back within the bounds indicating that the attack element is dismissed, the links to the neighboring units are restored back for normal operation. As per the explained theory, it can be seen that λ_1 immediately reverts back to the normal operating conditions obeying the consensus theory in Fig. 5(b) using the proposed mechanism.

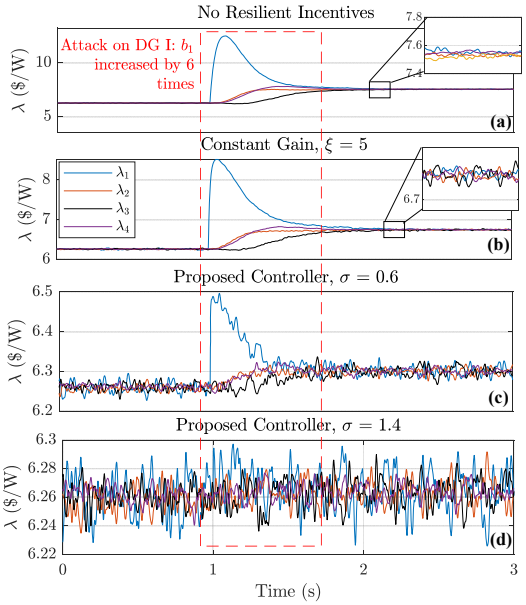

Fig. 6. Performance evaluation of AC microgrid (a) without any resilient incentive, (b) with constant gain $\xi = 5$, (c) proposed controller using (34) for $\sigma = 0.6$ and (d) $\sigma = 1.4$ for an attack at t = 1 s on DG I.

Further, the performance evaluation of the AC microgrid under an adaptive scaling factor multiplied to the model identification errors in (34) is carried out. A comparative assessment using various alternatives is presented in Fig. 6. The attack signal amplitude could be large, which may lead to a large change in the active power dispatch from DGs and may unnecessarily reach the maximum/minimum active power generation bounds. When b_1 is increased by a larger quantity, i.e. around 6 times at t = 1 s, it can be seen in Fig. 6(a) that the incremental cost of each DG converge around 7.6 $/W from a steady state-value of 6.3 $/W without any resilient incentives. Further in Fig. 6(b), when a constant gain $\xi = 5$ is multiplied to $[\tilde{a}_i(t) + \tilde{b}_i(t)]$ in (34), it can be seen that an appreciable attenuation is achieved for the same attack as compared to Fig. 6(a). It can be seen that the final convergence in Fig. 6(b) upon the attack reaches 6.6 $/W. Since the performance of a constant gain-based resilient mechanism will vary for different attack signal amplitudes, this scheme is highly dependent on the design of ξ. On the other hand, an anticipatory measure of the impact of DIA can be realized using (33), which monitors the change in incremental cost upon an attack. As the change in incremental cost is proportional to the amplitude of attack elements, it provides a direct correlation to design the resilient update. This can be clearly seen in Fig. 6(d), where the attenuation increases when $\sigma = 1.4$ since the steady-state point of incremental cost didn't get altered even in the presence of attacks. However for $\sigma < 1$ in Fig. 6(c), a minor shift of 0.05 $/W in incremental cost of each DG in the presence of attack is still present, which can be decreased with increase in σ above 1.

Additionally, a sensitivity analysis is carried out to inspect detection capabilities of the proposed strategy in Fig. 7 for different values of $\bar{e}$. A random attack is performed at t = 2 s on DG II which updates the final settling point for convergence. It can be seen that with increase in the value of $\bar{e}$, the transient peak and the settling time to the optimal set-point keeps increasing. Moreover, to provide resiliency against input and acquisition noise, $\bar{e}$ can not be assigned a very low value. The design of $\bar{e}$ is a deterministic task, which highly depends on factors such as accuracy and dynamic response.

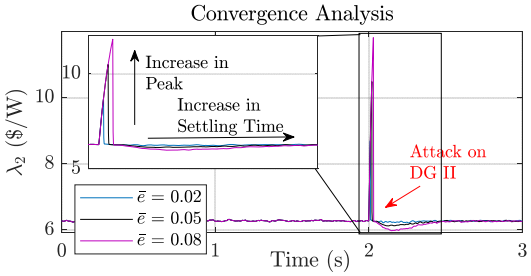

Fig. 7. Sensitivity analysis of the proposed event driven attack resilient mechanism for different values of $\bar{e}$.

Next in scenario I, the performance of the proposed method in mitigating various types of attack scenarios is presented. In Scenario I, fault attacks are conducted in the microgrid by changing the cost parameters of DG I and III at t = 0.5 and 2 s respectively. It can be seen in Fig. 8(a) that the incremental cost of each DG converges to 7.4 $/W instead of 6.6 $/W when attack 1 is carried out for the same loading condition.

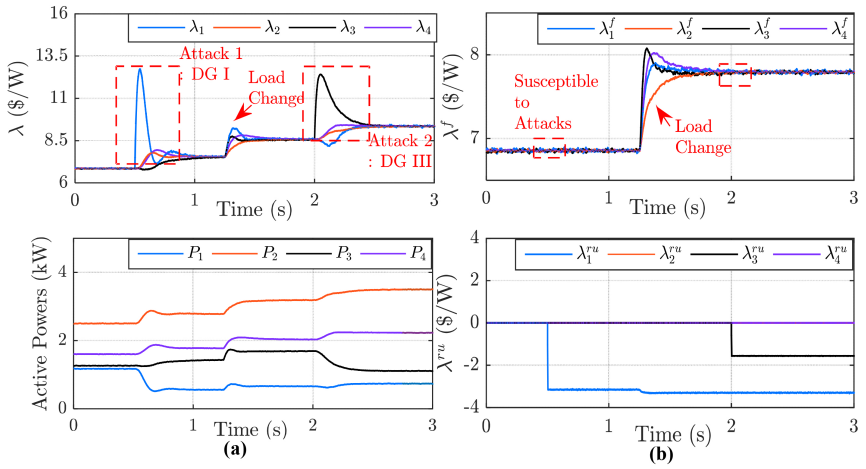

Fig. 8. Scenario I - (a) Performance of cooperative microgrid without any attack detection mechanism under fault attacks on DG I and III at t = 0.5 and 2 s respectively, (b) the proposed strategy protects the system from such attacks using local resilient control updates.

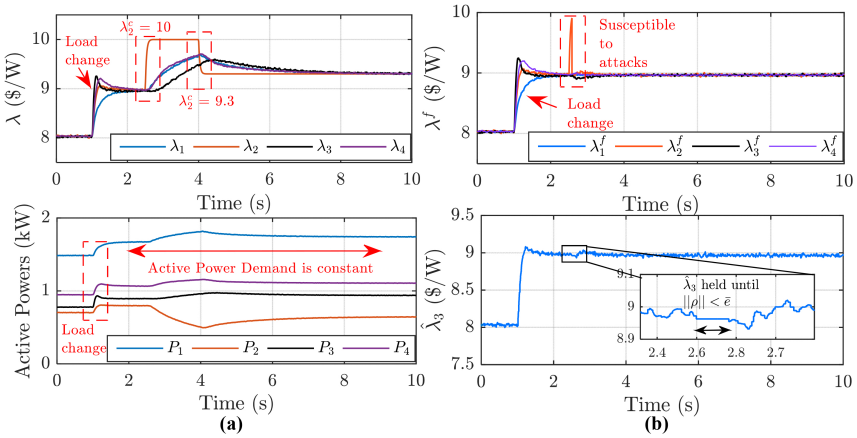

Fig. 9. Scenario II - (a) Performance of cooperative microgrid without any attack detection mechanism for random attacks on DG II at t = 2.5 and 4 s for the same loading condition, (b) the proposed strategy protects the system from such attacks using the localized event held $\hat{\lambda}_2$.

Further at t = 2 s, attack 2 is conducted on DG III, which leads to further increase in the incremental cost for the same active power demand. To defend against such attacks by using the proposed controller, it can be seen in Fig. 8(b) that the convergence of λ^f is unaffected with the inception of attacks. Moreover, the response of the resilient control update of the attacked agents, λ_1^{ru} and λ_3^{ru}, immediately go negative to compensate for the attack elements for their respective DGs.

In Scenario II, random attack is conducted twice on DG II. At t = 2.5 s, λ_2^c is initialized to a value of 10 \$/W, which disrupts the optimal operation. As already explained, the attack element acts as a reference for other DGs, as shown in Fig. 9(a). As a result, λ of the remaining DGs operate to track the reference. Another attack is initiated at t = 4 s, which sets λ_2^c to 9.3 \$/W. As each DG operate to reach a feasible solution with λ converging to 9.3 \$/W in steady state, the proposed localized estimation is used to broadcast the event generated $\hat{\lambda}_2$ to operate as soon as the event is triggered. To verify the performance of the controller, it can be seen in Fig. 9(b) that $\hat{\lambda}_2$ is held constant during the inception of attack. When $||\rho||$ resets back within bounds, the actual value of λ_2 is used. As a result, the localized estimation prevents the system from going into non-optimal states by using the last sample of active power measurement before triggering of the local event.

In Scenario III, the performance of the proposed resilient mechanism is evaluated in case of DG outage. Since the cooperative control facilitates plug-and-play capability [25], it is intuitive that the proposed localized resilient mechanism should operate seamlessly even under the outage of DGs. Referring to Fig. 10(a), a fault attack (*Attack I*) on DG III at t = 1 s resulted in a rise in the incremental cost of each DG. The active power dispatch from each DG also re-arrange for the same loading condition. At t = 2 s, DG III is disconnected from the system with its physical and communication links disabled. However, the rest of the active network still forms an undirected graph with an increased incremental cost while sharing the same demand. Meanwhile, another fault attack (*Attack II*) is injected into DG IV at t = 4 s. Upon the launch of the attack, the incremental cost of each DG further increases. It can be seen in Fig. 10(b) that the rest of the active network is fully protected from both of the abovementioned attacks owing to the proposed resilient mechanism. Since the incremental

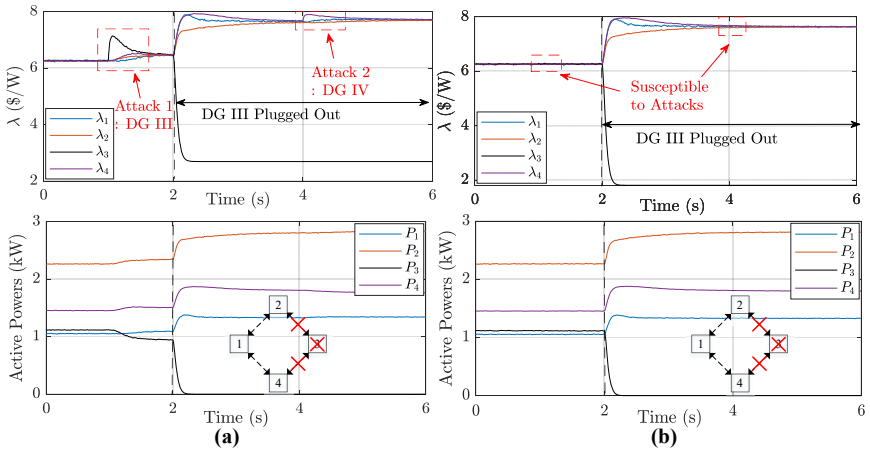

Fig. 10. Scenario III - Performance of cooperative microgrid when DG III is plugged out at t = 2 s. Further, fault attacks are carried out on DG III and IV for the same loading condition at t = 1 and 4 s respectively : (a) Without any attack resilient mechanism leading to an increase in the incremental costs of each DG upon attack, (b) the proposed strategy protects the system from such attacks using local resilient control updates.

TABLE II
COST COEFFICIENTS OF DGS IN SCENARIO IV

DG	I	II	III	IV	V	VI
a	0.005	0.0025	0.004	0.006	0.006	0.0035
b	1	0.6	1.8	0.45	1.5	0.9
DG	VII	VIII	IX	X	XI	XII
a	0.005	0.0055	0.0075	0.0038	0.006	0.0075
b	2.7	0.65	1.8	1	2.4	0.72

cost of each DG retains the same value even in the presence of attacks in Fig. 10(b), a similar behavior can be expected for the active power dispatch values as well. As a result, the optimal state of operation is always kept intact even in the presence of DIAs.

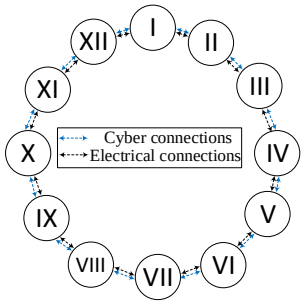

Fig. 11. Cyber and electrical connections between N = 12 DGs (Scenario IV).

In Scenario IV, the performance of the cooperative microgrid in the presence of the proposed resilient approach has been tested for N = 12 DGs to evaluate its scalability. As shown in Fig. 11, the DGs are electrically connected in a ring configuration with a similar topology of information exchange between the neighboring DGs. The cost coefficients of each DG have been tabulated in Table II. Since the proposed event-driven resilient mechanism is designed for i^{th} DG only using the localized error in the cost coefficients (see (33)), it can

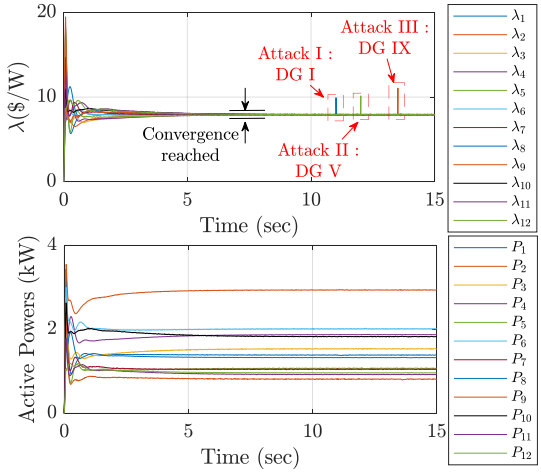

Fig. 12. Scenario IV - Performance of cooperative microgrid with N = 12 DGs in the presence of three random attacks at t = 11, 12 and 13.5 sec respectively to test the scalability of the proposed resilient approach.

be scaled to any number of agents following a spanning tree cyber connectivity. The spanning tree connectivity provides a direct measure of convergence in reaching consensus between the participating agents. As shown in Fig. 12, at t = 11, 12 and 13.5 sec, *Attack I, II* and *III* is conducted on DG I, V and IX respectively, however, the proposed resilient strategy mitigates the false data element immediately to guarantee optimality for N agents. Moreover since the computational resources are distributed across N processors in a cooperative microgrid, the computational burden is significantly reduced in this case as compared to the implementation of this strategy for N agents following centralized communication.

VI. CONCLUSION

This paper presented a localized event based attack-resilient mechanism to defend cooperative microgrids from data integrity attacks. As these attacks lead to an increase in the generation cost, they need to be mitigated immediately to prevent

divergent solutions, which may lead to instability in the worse cases. Here, an online stealth attack mechanism is presented for cooperative microgrid using two variants of attacks, namely fault and random attacks, segregated based on their respective update behavior in achieving consensus. To deal with fault attacks, the proposed mechanism provides a localized online compensation to the changes in cost parameters using a resilient control update that is designed locally. Whereas for random attacks, the localized event based incremental cost is being used via the constantly held measurement before the attack is conducted. The proposed scheme provides the following advantages: 1) ability to deal with the correctness of measurements in each DG without infringing neighbors' cost parameters, and 2) capable of operating normally even during link failure and communication delay, since the mechanism is localized. A theoretical analysis on the variance of the cost function with a change in cost parameters is provided to justify the vulnerability of the system to such attacks and techno-economic concerns. The proposed scheme has further been tested for multiple attack scenarios to support the proposed theory. Finally, the localization of this approach makes it easily scalable to protect large distribution networks from such attacks.

APPENDIX

Simulation Parameters

It is worth notifying that the control parameters are consistent for each DG, unless stated otherwise. The inner and outer control loop gains used in the controller of each DG can be found in [6].

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

Controller: m = 0.0014, n = 0.0013, k_i = 500, $\bar{e}$ = $\{0.00001, 0.01\}$, σ = 1.4, P^{min} = $\{0, 0, 0, 0\}$ kW, P^{max} = $\{4, 4, 4, 4\}$ kW.

ACKNOWLEDGEMENT

This work is an outcome of the Future Resilient Systems project at the Singapore-ETH Centre (SEC) supported by the National Research Foundation, Prime Minister's Office, Singapore under its Campus for Research Excellence and Technological Enterprise (CREATE) programme.

REFERENCES

[1] C Chen, et al., "Smart energy management system for optimal microgrid economic operation," *IET Renew. Power Gen.*, vol. 5, no. 3, pp. 258-267, 2011.

[2] S. Sahoo, and S. Mishra, "A Multi-Objective Adaptive Control Framework in Autonomous DC Microgrid," *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 4918-4929, 2017.

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

[4] R. Palma-Behnke, C. Benavides, F. Lanas, B. Severino, L. Reyes, J. Llanos, and D. Saez, "A microgrid energy management system based on the rolling horizon strategy," *IEEE Trans. Smart Grid*, vol. 4, no. 2, pp. 996- 1006, 2013.

[5] P. Siano, C. Cecati, H. Yu, and J. Kolbusz, "Real time operation of smart grids via FCN networks and optimal power flow," *IEEE Trans. Ind. Informatics*, vol. 8, no. 4, pp. 944-952, 2012.

[6] Q Shafiee, JM Guerrero, and JC Vasquez, "Distributed secondary control for islanded microgrids–A novel approach," *IEEE Trans. Power Electr.*, vol. 29, no. 2, pp. 1018-1031, 2014.

[7] J. S. Vardakas, et. al., "Electrical Energy Savings through Efficient Cooperation of Urban Buildings: The Smart Community Case of Superblocks' in Barcelona," *IEEE Comm. Magazine*, vol. 56, no. 11, pp. 102-109, 2018.

[8] X. Fang, and Q. Yang, "Cooperative energy dispatch for multiple autonomous microgrids with distributed renewable sources and storages," *Smart Power Distribution Systems*, Academic Press, pp. 127-160, 2019.

[9] 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.

[10] J Llanos, J Gomez, D Saez, D Olivares, and J. Simpson-Porco, "Economic Dispatch by Secondary Distributed Control in Microgrids," *2019 European Conf. Power Electron. and Appl. (EPE'19 ECCE)*, Genova, Italy, 2019.

[11] L Meng, et al., "Microgrid supervisory controllers and energy management systems: A literature review," *Renewable and Sustainable Energy Reviews*, vol. 60, pp. 1263-1273, 2016.

[12] AA Memon, and K Kauhaniemi, "A critical review of AC Microgrid protection issues and available solutions," *Electric Power Systems Research* vol. 129, pp. 23-31, 2015.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

[19] J Duan, W Zeng, and MY Chow, "Economic Impact of Data Integrity Attacks on Distributed DC Optimal Power Flow Algorithm," *2015 North American Power Symposium,* pp. 1-7, 2015.

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

[21] W Zeng, and MY Chow, "Resilient Distributed Control in the Presence of Misbehaving Agents in Networked Control Systems," *IEEE Trans. Cybernet.*, vol. 44, no. 11, pp. 2038-2047, 2014.

[22] J Duan, W Zeng, and MY Chow, "Resilient Distributed DC Optimal Power Flow Against Data Integrity Attack," *IEEE Trans. Smart Grid*, vol. 9, no. 4, pp. 3543-3552, 2018.

[23] P Danzi, M Angjelichinoski, C Stefanovic, T Dragicevic, and P Popovski, "Software-Defined Microgrid Control for Resilience Against Denial-of-Service Attacks," *IEEE Trans. Smart Grid*, vol. 10, no. 5, pp. 5258-5268, 2018.

[24] 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.

[25] NM Dehkordi, N Sadati, and Mohsen Hamzeh, "Fully Distributed Cooperative Secondary Frequency and Voltage Control of Islanded Microgrid," *IEEE Trans. Energy Conv.*, vol. 32, no. 2, pp. 675-685, 2017.

[26] 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.

[27] S Marano, V Matta, and L Tong, "Distributed detection in the presence of byzantine attack in large wireless sensor networks," *MILCOM 2006 IEEE Milit. Comm. Conf.*, pp. 1-4, Oct. 2006.

[28] W Zeng and MY Chow, "Resilient Distributed Control in the Presence of Misbehaving Agents in Networked Control Systems," *IEEE Trans. Cybernet.*, vol. 44, no. 11, pp. 2038-2049, 2014.

[29] W Zeng, Y Zhang and MY Chow, "Resilient Distributed Energy Management Subject to Unexpected Misbehaving Generation Units," *IEEE Trans. Ind. Inform.*, vol. 13, no. 1, pp. 208-216, 2017.
[30] J Duan, W Zeng, and MY Chow, "Resilient Cooperative Distributed Energy Scheduling against Data Integrity Attacks," *IECON 2016-42nd Ann. Conf. IEEE Ind. Electr. Soc.*, pp. 4941-4946, 2016.
[31] K Hengster-Movric, et al., "Synchronization of discrete-time multi-agent systems on graphs using Riccati design," *Automatica*, vol. 49, no. 2, pp. 414-423, 2013.
[32] EA Coelho, et. al., "Small-signal analysis of the microgrid secondary control considering a communication time delay," *IEEE Trans. Ind. Electr.*, vol. 63, no. 10, pp. 6257-6269, 2016.
[33] S Sahoo and S Mishra, "An Adaptive Event-Triggered Communication-Based Distributed Secondary Control for DC Microgrids," *IEEE Trans. Smart Grid*, vol. 9, no. 6, pp. 6674-6683, 2018.

Subham Sahoo (S'16-M'18) received the B.Tech. & Ph.D. degree in Electrical and Electronics Engineering from VSS University of Technology, Burla, India and Electrical Engineering at Indian Institute of Technology, Delhi, New Delhi, India in 2014 & 2018, respectively. He has worked as a visiting student with the Department of Electrical and Electronics Engineering in Cardiff University, UK in 2017 and as a postdoctoral researcher in the Department of Electrical and Computer Engineering in National University of Singapore in 2018-2019. He is currently working as a research fellow in the Department of Energy Technology, Aalborg University, Denmark.

He is a recipient of the Innovative Students Projects Award for Doctoral level by Indian National Academy of Engineering (INAE) for the year 2019. His current research interests include control and stability of microgrids, cyber security in cyber-physical energy systems.

Jimmy Chih-Hsien Peng (M'04) is currently an Assistant Professor with the Department of Electrical and Computer Engineering at the National University of Singapore, Singapore. Previously, he was part of the start-up team at the Masdar Institute (now part of the Khalifa University), United Arab Emirates. In 2013, he was appointed as a Visiting Scientist with the Research Laboratory of Electronics at the Massachusetts Institute of Technology (MIT), Cambridge, Massachusetts. He later became a Visiting Assistant Professor at MIT in 2014.

He currently serves as the secretary for IEEE PES Working Group on High-Performance Computing for Power Grid Analysis and Operation. He is also a committee member for SPRING Singapore's SS 535 Standard – *Code of Practice for Installation, Operation, Maintenance, Performance and Construction Requirements of Mains Failure Standby Generating Systems*. SPRING is an agency under the Ministry of Trade and Industry, Singapore. Previously, he served on the Standards New Zealand – a business unit within the Ministry of Business, Innovation and Employment, New Zealand. He was nominated by the IEC National Committee of New Zealand to join the IEC Young Professionals Program in 2011.