A Stealth Cyber Attack Detection Strategy for DC Microgrids

Sahoo, Subham; Mishra, Sukumar ; Chih-Hsien Peng, Jimmy ; Dragicevic, Tomislav

Published in:
I E E E Transactions on Power Electronics

DOI (link to publication from Publisher):
10.1109/TPEL.2018.2879886

Publication date:
2019

Document Version
Accepted author manuscript, peer reviewed version

A Stealth Cyber Attack Detection Strategy for DC Microgrids

Subham Sahoo, *Member, IEEE*, Sukumar Mishra, *Senior Member, IEEE*, Jimmy Chih-Hsien Peng, *Member, IEEE* and Tomislav Dragičević, *Senior Member, IEEE*

***Abstract*—This paper proposes a cooperative mechanism for detecting potentially deceptive cyber attacks that attempt to disregard average voltage regulation & current sharing in cyber-physical DC microgrids. Considering a set of conventional cyber attacks, the detection becomes fairly easy for distributed observer based techniques. However, a well-planned set of balanced attacks, termed as the *stealth attack*, can bypass the conventional observer based detection theory as the control objectives are met without any physical error involved. In this paper, we discuss the formulation & associated scope of instability from stealth attacks to deceive distributed observers realizing the necessary & sufficient conditions to model such attacks. To address this issue, a novel cooperative vulnerability factor (CVF) framework for each agent is introduced, which accurately identifies the attacked agent(s) under various scenarios. To facilitate detection under worst cases, the CVFs from the secondary voltage control sublayer is strategically cross-coupled to the current sublayer, which ultimately disorients the control objectives in the presence of stealth attacks and provides a clear norm for triggering defense mechanisms. Finally, the performance of the proposed detection strategy is simulated in MATLAB/SIMULINK environment and experimentally validated for FDI & stealth attacks on sensors and communication links.**

***Index Terms*—DC microgrid, stealth attack, false data injection, distributed control.**

I. Introduction

DC microgrids are an effective means of integrating renewable energy sources, storage devices and modern electronic loads, capable of operating independently of the utility grid [1], [2]. Moreover, the operating nature of these units in the DC paradigm makes it a vivid option to enhance the efficiency [3]. For enhancing the scalability and robustness, distributed controllers are desirable in microgrids [4], [5] to avoid single point of failure as compared to the centralized communication, owing to their highly reliable operation during link failures. Moreover, distributed control philosophy is an economic option since it can be easily accommodated by transmitting lesser volume of data without entailing much traffic in contrast to the centralized communication [6]. In DC microgrids, cooperative secondary controllers have been deliberately used for various objectives such as average voltage regulation [7], proportional load sharing [8] and energy balancing [9].

To enhance the scope of reliability, system security plays an increasingly important role to maintain *unbiased* coordination among the sources since it directly affects the technological aspects based on penalties specifically allocated for poor performance metrics [10]. Few potential ways to violate security measures are cyber attacks, which typically include false data injection attacks (FDIAs) [11], denial of service (DoS) [12], replay attacks [13], and others. Such attacks are adept at disrupting the network stability as well as control structures. Several instances have been reported in the past, which became a critical concern for the control centers [14]. FDIAs alter the system state by injecting a false data into any of the compromised sensors/actuators. An example of implementation of such attacks is given in [11]. To analyze the impact of such attacks, further investigation is done in [15] to assess its impacts on the economic load dispatch that is realized in a cooperative manner. In this respect, the system under attack reaches a consensus stage which is not optimal. Broadly, detection and mitigation of conventional attacks is already well classified in the literature since such attacks disrupt the operation of observers which becomes a simple criteria for detection. However, it is reported that generalized FDIAs, commonly known as *stealth* attacks [16], can easily penetrate into networked systems without altering the system observability. These attacks can be specifically classified as *coordinated intelligent attacks* [17] which involves coordinated attack vectors in multiple nodes to nullify system dynamics. As a result, the system/agent operator would be unaware of any online attack vectors present in the system. Prior to this, the attacker could cause an unfair increase in the magnitude of attack vectors which may cause system shutdown depending upon the severity of the attack. Additionally, implementation of such attacks gets easier when the attacker has obtained *apriori* knowledge about the system using adequate system monitoring [18]. More instance of coordinated attacks on large power systems and its vulnerability assessment is provided in [19], [20]. In this regard, risk assessment alongwith control vulnerabilities is crucial since the modeling of coordinated attacks for microgrids can be easier owing to their small system size without significant security measures [21], [22].

In [23], the authors have identified aberrant operation of a microgrid when a false data is injected into the voltage controller of the substation. Apart from stability, it is also crucial to analyze if the proposed strategies can attain eco-

This research is supported by the Academic Research Fund Tier 1 from the Ministry of Education under the grant number R-263-000-C27-133.

S Sahoo and JCH Peng are with the Department of Electrical and Computer Engineering, National University of Singapore, Singapore, 119007 (e-mail: subhamsahoo50@gmail.com and jpeng@nus.edu.sg) *(Corresponding Author: Jimmy Chih-Hsien Peng)*

S Mishra is with the Department of Electrical Engineering, Indian Institute of Technology Delhi, New Delhi 110 016, India. (e-mail: sukumar@ee.iitd.ac.in)

T Dragičević is with the Aalborg University, Aalborg East 9220, Denmark (e-mail: tdr@et.aau.dk)

nomic vulnerabilities in a microgrid. In fact, this attribute is well addressed in [27] where the FDIAs are categorized by their utilization levels having monitored the stability of microgrids under different conditions. On the other hand, Beg *et. al.* in [24] have stressed on the identification the varying of candidate invariants to detect the presence of FDIAs. Moreover, it has been demonstrated that stealth attacks in DC microgrids can deceive the control system without creating any negative impact/disturbance. However, it is crucial to understand that such undetectable attacks, which are able to penetrate while maintaining discretion, can cause network instability in unforeseeable ways.

Since distributed observer based strategy [25] is more prone to cyber attacks for a well-spanned distributed graph as the injected false data propagates in the entire network, proper analysis has to be carried out towards the detection of the attacked agent in a microgrid to establish corrective action. False data propagation in DC microgrids may lead to loss of generality from an economic point of view, cause current sharing errors, which lead to circulating currents between each converter. Using distributed computation, the estimated states will converge to a nonzero steady value under FDIAs, which makes them simple to detect. In [28], the compromised agent with false data is detected using a cooperative based trust & confidence factors to realize mitigation of the propagation of false data in the cyber network. However, considering the worst case for such attacks, the abovementioned factors can also be manipulated by adding/subtracting a large constant value while the controller is attacked, which may lead to false values corresponding to the attacked node. Consequently, it will result in maloperation of the mitgation strategy, since it operates on non-attacked agent(s). In [26], Fawzi *et. al.* have determined a theoretical limit on the number of compromised sensors in a system beyond which it is impossible to characterize the detection of such attacks. Considering this view point, theoretical analysis for stealth attacks at multiple sensors/actuators in a cooperative network to create instability and the corresponding detection methodologies in DC microgrids has not gained significant attention yet. On the other hand, [29] have addressed this issue for an economic dispatch problem as it decreases the overall efficiency with an increase in the generation cost by dislocating towards a non-optimal point. However, it does not administer a mechanism for detection of the compromised agent during a stealth attack, which is crucial to cease its propagation into the network and may consequently lead to instability.

The idea behind stealth attack detection in this paper is identification of the merits of a well-spanned network in cooperative control mechanism. In particular, the difference between the secondary output of voltage sublayer, termed as cooperative vulnerability factor (CVF), converges to zero if the system is not under attack. Furthermore, the necessary and sufficient conditions for modeling of worst-case stealth attack involving multiple sensors/communication links are studied extensively. Moreover, the impact of FDI & stealth attacks on sensors and communication links is studied for intrusion in voltage and current information separately to preserve system security and energy efficiency simultaneously. Since the distributed control philosophy in DC microgrids is based on voltage observer which can easily translate any uncoordinated data injection with a residual output, the authors have identified the concept of balanced attacks as stealth attack modeling with further investigation on its detection. Based on these findings, the CVFs of each agent determined from the secondary voltage sublayer are strategically coupled into the local current sharing secondary control loop. For this reason, any subsequent disruption/attack necessarily disorients the control operation of the agents, thereby serving as an apparent detection criterion considering that the attacker may attempt to manipulate CVF locally. On the other hand, the agent(s) representing positive value of CVF is resolved as attacked which suggests that their respective measurements are *untrue*. This can be easily extended to trigger the likely defense mechanisms to prevent further instability.

To sum up, the research contributions of this paper are:

1) To ascertain the possibility of FDI and stealth attacks in DC microgrids, a new methodology based on a cooperative vulnerability factor (CVF) is proposed using the outputs from secondary sublayers used for global average voltage regulation in DC microgrids. Generalization of distributed observers is done to detect such attacks and how it can be circumvented for a multiple sensor/link based stealth attacks. For detection of the compromised/attacked agent, CVF of each agent is locally monitored for positive values across the network which represents the attacked agent(s). This technique is used as an apparent method of detecting attacks locally such that corrective actions can take place. To the best of authors' knowledge, CVF has never been proposed in the realm of cyber attack detection in microgrids.
2) A new cross-coupling methodology of CVF output of each agent from the secondary voltage sublayer is proposed to strategically disorient the control operation for the worst case of consecutive attacks when the attacker can attempt to reduce CVF into a negative value so as to deceive the abovementioned detection philosophy. Hence, the cross-coupling approach ensures accurate detection of the attacked agent(s) by prevention against further attacks into the proposed detection metric, i.e., CVF.

The rest of the paper is organized as follows. The system architecture of DC microgrids along with cyber layer preliminaries providing an overview of the secondary control strategy is illustrated in Section II. Section III depicts the problem formulation to demonstrate the behavior of cooperative control strategy under FDI and stealth attacks. Moreover, the necessary and sufficient conditions of modeling such attacks with multiple sensors/cyber link have been discussed in detail. Section IV provides a brief overview on the calculation of the cooperative vulnerability factor for each agent and its significance in the detection of such attacks. Simulations along with experimental validation are presented in Section V & VI respectively. Finally, Section VII concludes the paper.

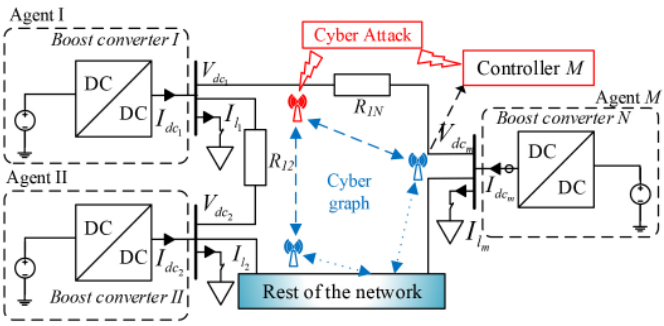

Fig. 1. Generic cyber-physical model of DC microgrid: Blue arrows represent the cyber layer and black lines represent the physical circuit.

II. Conventional Cooperative Realm in DC Microgrids

A. Cyber-physical Model

The autonomous DC microgrid considered in this paper is shown in Fig. 1. M DC sources connected via DC/DC converters of equal power rating are inter-connected through tie-lines, thereby constituting the physical layer of the microgrid. Each DC/DC converter operates to maintain the output voltage as per the reference values generated by the local primary and secondary controller. An undirected cyber graph of the communication network is considered in this paper, which sends and receives information from its neighbors. Further, loads are connected at the converter output of each unit. The simulated system parameters have been provided in Appendix.

Considering each source as an agent, the communication graph is represented as a digraph via edges and links via an adjacency matrix $\mathbf{A} = [a_{ij}] \epsilon R^{MXM}$, which suggests the communication weights to be

$$a_{ij} = \begin{cases} > 0, & \text{if } (x_i, x_j) \epsilon \mathbf{E} \\ 0, & \text{else} \end{cases} \tag{1}$$

where $\mathbf{E}$ is an edge connecting two nodes, x_i is the local node and x_j is the neighboring node. It is to be noted that the communication weights depict information exchange between two corresponding nodes only. Mathematically, it can be denoted by a matrix with incoming information, $\mathbf{Z}_{in} = \sum_{i \epsilon M} a_{ij}$. 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

$$l_{ij} = \begin{cases} \deg(m_i) & , i = j \\ -1 & , i \neq j \\ 0 & , \text{otherwise} \end{cases} \tag{2}$$

where $\deg(m_i)$ is the degree of i^{th} node and $\mathbf{L} = [l_{ij}] \epsilon R^{MxM}$.

Remark I: All the units will achieve consensus using $\mathbf{x}(k+1) - \mathbf{x}(k) = -\mu \mathbf{L}\mathbf{x}(k)$ for a well-spanned matrix L such that $\lim_{k \to \infty} x_i(k) = c$, $\forall\ i \epsilon M$, where c is a constant, μ is a positive value and M is the number of agents in the system.

B. Cooperative Control of Sublayers in DC Microgrids

The general philosophy of secondary cooperative realm in DC microgrids is to maintain the average voltage globally and share the currents proportionately using local as well as neighboring measurements such that the circulating currents can be reduced. These objectives are implemented using the secondary control sublayers in a cooperative manner using:

1) Sublayer I : Average Voltage Restoration: For global average voltage regulation in DC microgrids, an average voltage estimate $\bar{V}_{dc_i}(k)$ for i^{th} agent is obtained using a voltage observer, which is updated via a *dynamic consensus* algorithm [30] using the neighboring estimates $\bar{V}_{dc_j}(k)\ \forall\ j \epsilon\ N_i$, where N_i denotes the set of neighboring agents. Mathematically, it can be represented for i^{th} agent as

$$\begin{aligned} \bar{V}_{dc_i}(k+1) - \bar{V}_{dc_i}(k) &= V_{dc_i}(k+1-\tau_o^i) - V_{dc_i}(k-\tau_o^i) \\ &+ \underbrace{\sum_{j \epsilon N_i} a_{ij}(\bar{V}_{dc_j}(k-\tau_{in}^i-\tau_d^{ij}) - \bar{V}_{dc_i}(k-\tau_{in}^i))}_{\text{Cooperative input}} \end{aligned} \tag{3}$$

where $V_{dc_i}(k)$, N_i, τ_{in}^i and τ_o^i denote the measured voltage, set of neighboring agents, input and output delay [31] in i^{th} agent respectively. Moreover, τ_d^{ij} denote the communication delay between i^{th} & j^{th} agent, $\forall\ j\ \epsilon\ N_i$. Alternatively, (3) can be represented in the vector form as

$$\begin{aligned} \bar{\mathbf{V}}_{dc}(k+1) - \bar{\mathbf{V}}_{dc}(k) &= \mathbf{V}_{dc}(k+1-\tau_o) - \mathbf{V}_{dc}(k-\tau_o) \\ &+ \mathbf{A}\bar{\mathbf{V}}_{dc}(k-\tau_{in}-\tau_d) - \mathbf{Z}_{in}\bar{\mathbf{V}}_{dc}(k-\tau_{in}) \end{aligned} \tag{4}$$

$$\begin{aligned} \bar{\mathbf{V}}_{dc}(k+1) - \bar{\mathbf{V}}_{dc}(k) &= \mathbf{V}_{dc}(k+1-\tau_o) - \mathbf{V}_{dc}(k-\tau_o) \\ &- \mathbf{L}_1\bar{\mathbf{V}}_{dc}(k-\tau_{in}-\tau_d) - \mathbf{L}_2\bar{\mathbf{V}}_{dc}(k-\tau_{in}) \end{aligned} \tag{5}$$

such that $\mathbf{L} = \mathbf{L}_1 + \mathbf{L}_2$, where $\mathbf{L}_1 = \begin{bmatrix} 0 & l_{12} & \dots & l_{1M} \\ l_{21} & 0 & \dots & l_{2M} \\ \vdots & \vdots & \ddots & \vdots \\ l_{M1} & l_{M2} & \dots & 0 \end{bmatrix}$,

$\mathbf{L}_2 = \begin{bmatrix} l_{11} & 0 & \dots & 0 \\ 0 & l_{22} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & l_{MM} \end{bmatrix}$.

2) Sublayer II : Proportionate Current Sharing: Similarly, the normalized current regulation cooperative input for i^{th} agent using the neighboring output current measurements I_{dc_j}, $\forall\ j\ \epsilon\ N_i$ is given by

$$\begin{aligned} \bar{I}_{dc_i}(k) = \sum_{j \epsilon N_i} c_i a_{ij}(I_{dc_j}(k-\tau_o^j-\tau_d^{ij})/I_{dc_j}^{max} - \\ I_{dc_i}(k-\tau_o^i)/I_{dc_i}^{max}) \end{aligned} \tag{6}$$

where c_i, $I_{dc_i}(k)$, $I_{dc_i}^{max}$ and $I_{dc_j}^{max}$ denote the desired coupling gain, measured output current in i^{th} agent, maximum output current allowed for i^{th} agent and j^{th} agent respectively. To establish these objectives for an agent operating to regulate

output voltage, two voltage correction terms for i^{th} agent are calculated using

$$\Delta V_i^1(k) = K_P^{H_1} \underbrace{(V_{dc_{ref}} - \bar{V}_{dc_i}(k))}_{e_1^i(k)} + K_I^{H_1} \sum_{p=0}^{k} (V_{dc_{ref}} - \bar{V}_{dc_i}(p)) \quad (7)$$

$$\Delta V_i^2(k) = K_P^{H_2} \underbrace{(I_{dc_{ref}} - \bar{I}_{dc_i}(k - \tau_{in}^i))}_{e_2^i(k)} + K_I^{H_2} \sum_{p=\tau_{in}^i}^{k} (I_{dc_{ref}} - \bar{I}_{dc_i}(p - \tau_{in}^i)) \quad (8)$$

where $K_P^{H_1}, K_I^{H_1}, K_P^{H_2}, K_I^{H_2}$ are PI controller gains of H_1, H_2 in Fig. 4 and $V_{dc_{ref}}$, $I_{dc_{ref}}$ denote the global reference voltage and current quantities for all the agents respectively. The correction terms obtained in (7)-(8) are finally added to the global reference voltage $V_{dc_{ref}}$ setpoint to achieve local voltage reference $V_{dc_{ref}}^i$ for i^{th} agent using

$$V_{dc_{ref}}^i(k) = V_{dc_{ref}} + \Delta V_i^1(k) + \Delta V_i^2(k) \quad (9)$$

Remark II: Generally, the line impedances between each agent in a microgrid are significantly different, which usually introduces a poor current sharing profile using the primary droop concept without using communication [8]. However, by using (8), the voltage correction term $\Delta V_i^2(k)$ from the secondary controller compensates for the cable resistance as well as carries out proportionate sharing under different load conditions. As a result, the value of $\Delta V_i^2(k)$ is globally asymmetric in a microgrid with different tie-line resistances.

Remark III: Using the cooperative based consensus algorithm for a well connected cyber graph for a DC microgrid, the solutions in (3)-(6) shall converge to

$$\lim_{k\to\infty} \bar{V}_{dc_i}(k) = V_{dc_{ref}}, \ \lim_{k\to\infty} \bar{I}_{dc_i}(k) = 0 \ \forall i \ \epsilon M \quad (10)$$

It should be noted that $I_{dc_{ref}}$ in (8) has been kept zero for the load currents to be shared proportionately. However for false data-injection attacks in single sensor/communication link, (10) modifies to

$$\lim_{k\to\infty} \bar{V}_{dc_i}(k) = V_{dc_{ref}}^a, \ \lim_{k\to\infty} \bar{I}_{dc_i}(k) \neq 0 \ \forall i \ \epsilon \ M \quad (11)$$

where $V_{dc_{ref}}^a \neq V_{dc_{ref}}$. Assuming a pre-condition that the system always operates at a certain global reference voltage is known to each agent, (11) should be a sufficient criteria to justify that the system is attacked by an external entity. Many likely potential attacks on DC microgrids such as FDI & DoS [32], jamming [33] and distributed DoS [34] attacks have already been well studied in the literature. These attacks can be caused using several cyber-physical amendments such as jamming of cyber link, loss of measurements, data-packets flooding, compromised communication servers, sensors, etc. However, the authors in [32], [33] have already established that such attacks disrupt the cooperative synchronization law [30], which can be easily detected since (10) is violated. To provide with a detailed explanation, the abovementioned disturbances introduce an uncoordinated discontinuity in updating (5) which disrupts the consensus between agents, ultimately leading to (11).

Intuitively, the attacker conducting a stealth attack is able to penetrate into the control system without the system operator's knowledge. Such attacks can have adverse effect in the long run as the attacker has access to multiple nodes after penetrating into the system without system operator's knowledge and can create unintentional generation outage, which may eventually lead to system shutdown. Under these circumstances, detection of the attacked node(s) in a cooperative network is yet another aspect so as to prevent the system from further instability. The modeling of such attacks and its associated agenda of instability is discussed in detail in the following section.

III. Modeling of Stealth Attacks in Cooperative DC Microgrids

Considering the attacker injecting false data into multiple sensors/communication links to formulate a stealth attack, an analysis of how the convergence in (10) can be guaranteed is provided in this section. Furthermore, the necessary and sufficient conditions to formulate a stealth attack on multiple sensors in a cooperative network is given in detail.

For each agent, the local power balancing equation can be expressed in terms of

$$\chi_i(k) = I_{dc_i}(k) - I_{o_i}(k) \quad (12)$$

where $I_{o_i}(k)$ denote the total output current from i^{th} agent respectively. Using (12), the consensus algorithm in (3)-(6) under attacks can be rewritten as:

$$\begin{cases} \bar{V}_{dc_i}(k+1) = \bar{V}_{dc_i}(k) - \sum_{j\epsilon M} l_{ij} \bar{V}_{dc_j}(k - \tau_{in}^i - \tau_d^{ij}) \\ \qquad +\sigma\chi_i(k) + u_{V_i}^a(k) \\ I_{dc_i}(k+1) = I_{dc_i}(k) - \sum_{j\epsilon M} l_{ij} I_{dc_j}(k - \tau_o^j - \tau_d^{ij}) \\ \qquad +u_{I_i}^a(k) \\ \chi_i(k+1) = \chi_i(k) - \sum_{j\epsilon M} l_{ij}\chi_j(k) - \\ \qquad (I_{dc_i}(k+1) - I_{dc_i}(k)) \end{cases}$$

where $u_{V_i}^a(k)$ & $u_{I_i}^a(k)$ denote the attack vectors imposed into voltage & current secondary sublayer in i^{th} agent at k^{th} instant respectively. It should be noted that since $\chi_i(k)$ is not a physical measurement entity, the possibility of attack in $\chi_i(k)$ will be entirely due to $u_{I_i}^a(k)$. To provide with the basic understanding and investigating the effect of stealth attacks in multiple sensors/links in a cooperative network based DC microgrids (rated voltage of 315 V), a case study in Fig. 2 is done by injecting a balanced set of zero sum errors s & $-s$ into the voltage sensors in Agent I and III respectively during t = 1 s, where s is a constant attack element. After initiating the attack, it can be seen that $\bar{I}_{dc}(k)$ and $\bar{V}_{dc}(k)$ converge to their respective references as stated in (10) with the control objectives met satisfactorily without creating instability. Upon maintaining discretion for some time, the attacker attempts an unfair increase in the injected attack vectors by a large magnitude (highlighted as event A) at t = 2 s which results into a new operating reference $V_{dc_{ref}}^a$ in (11). A time-gap of 1 s between

the stealth attack and event A is intentionally considered in the case study to facilitate clear understanding. It should be noted that the attacker may introduce event A immediately at t = 1 s which necessitates a faster cyber attack detection strategy. As the agents' voltage ramp up to the highlighted overvoltage threshold, agents I & III are automatically tripped as a measure of overvoltage safety (highlighted as event B). Hence, if a vigilant attacker manages to penetrate, such attacks can lead to various unintentional scenarios without any trace for failure assessment. This case study necessitates the study of stealth attacks using multiple sensors/links along with an authentic detection mechanism. As a consequence, we obtain the necessary and sufficient conditions for the convergence of system under such attacks in (13).

Problem Statement: If there exist a constant R such that

$$\sum_{k=0}^{\infty} |u_V^a(k)| \leq R, \ \sum_{k=0}^{\infty} |u_I^a(k)| \leq R \ \forall \ i \ \epsilon \ M \tag{13}$$

then (13) in the presence of stealth attack shall converge as per (10) with $\lim_{k\to\infty} \chi_i(k) = 0$.

Proof: Representing (13) in the form of $x_i(k+1) = Ax_i(k) + Bu_i(k-\tau_{in}^i)$, we have

$$x_i(k+1) = Ax_i(k) + Bu_i(k-\tau_{in}^i) \tag{14}$$

$$= A^{k+1}x_i(0) + \sum_{p=\tau_{in}}^{k} A^{k-p}u_i(p-\tau_{in}^i) \tag{15}$$

As A is primarily composed of Laplacian matrices in (13), its eigenvalues lie around zero and unit plane [35]. Since $\lim_{k\to 0} \sum_{p=\tau_{in}}^{k} A^{k-p}u(p-\tau_{in})$ will converge to zero for a well-connected graph, as per (10), $\lim_{k\to 0} A^{k+1}x(0)$ should converge to $V_{dc_{ref}}d$, where $d = \left[1, ..., 1, 0, ..., 0, 0, ..., 0\right]^T \ \epsilon \ R^{3MX1}$ with M elements equal to 1 and $2M$ elements equal to 0. Hence, this proves the convergence of a stealth attacked system to the global reference set-points in (10). ■

Additionally, the abovementioned proof can be extrapolated to justify

$$\sum_{i \ \epsilon M} I_{dc_i}(k) = \sum_{i \ \epsilon \ M} I_{l_i}(k) \tag{16}$$

under a stealth attack where I_{l_i} is the local load at i^{th} agent. Due to (16), convergence of (12) is guaranteed. By the iterative rule, subtracting $I_{dc_i}(k+1)$ from $\chi_i(k+1)$, we get

$$\sum_{i \ \epsilon \ M} \chi_i(k+1) - \sum_{i \ \epsilon \ M} I_{dc_i}(k+1) = \sum_{i \ \epsilon \ M} \chi_i(k) - \sum_{i \ \epsilon \ M} I_{dc_i}(k) - \sum_{i \ \epsilon \ M} u_{I_i}^a(k) \tag{17}$$

$$= \sum_{i \ \epsilon \ M} \chi_i(k-1) - \sum_{i \ \epsilon \ M} I_{dc_i}(k-1) - \sum_{i \ \epsilon \ M} (u_{I_i}^a(k-1) + u_{I_i}^a(k)) \tag{18}$$

$$= \sum_{i \ \epsilon \ M} \chi_i(0) - \sum_{i \ \epsilon \ M} I_{dc_i}(0) - \sum_{p=0}^{k} \sum_{i \ \epsilon \ M} u_{I_i}^a(p) \tag{19}$$

Substituting for $I_{dc_i}(k+1)$ from (13) in (19) and taking limitation on both sides considering (12) as $k \to \infty, \forall i \ \epsilon \ M$, we get

$$\sum_{p=0}^{k} \sum_{i \ \epsilon \ M} u_{I_i}^a(p) = 0 \tag{20}$$

A similar analysis can be carried out to determine the effect of $u_V^a(k)$ in the convergence of the algorithm to get

$$\sum_{p=0}^{k} \sum_{i \ \epsilon \ M} u_{V_i}^a(p) = 0 \tag{21}$$

using $\chi_i(k+1)$ & $\bar{V}_{dc_i}(k+1)$ in (17).

Remark IV: Following the concept of cooperative synchronization [30], the average voltage estimate in (5) tends to achieve consensus for all its elements for a spanning cyber graph such that $\mathbf{L}\bar{\mathbf{V}}_{dc}(k) = 0$ during steady-state to reach a steady-state value of $V_{dc_{ref}}\mathbf{1}$. Alternatively, a similar representation can be given using $e_1^i(k)$ in (7) such that $\mathbf{L}\mathbf{E}_1(k) = 0$ reaches a steady state solution of zero, where $\mathbf{E}_1(k)$ denotes the vector notation of $e_1^i(k)$. Using (21) as an attack vector for the abovementioned consensus theory, it can be concluded that the steady solution isn't affected for $\mathbf{E}_1(k)$ owing to the

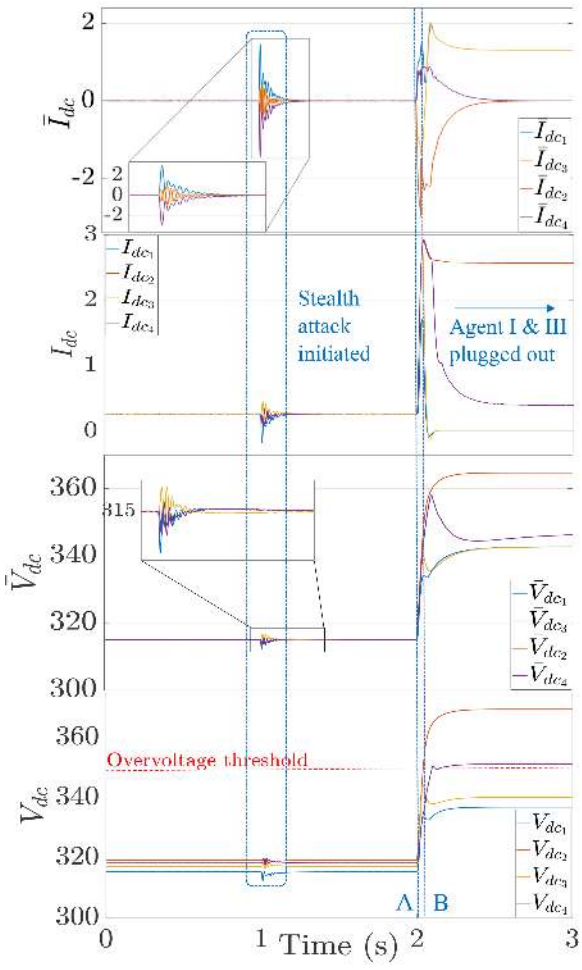

Fig. 2. Case study I: Instability caused by injecting an attack consisting of balanced set of zero sum error into the voltage sensors in DC microgrid consisting of M = 4 agents.

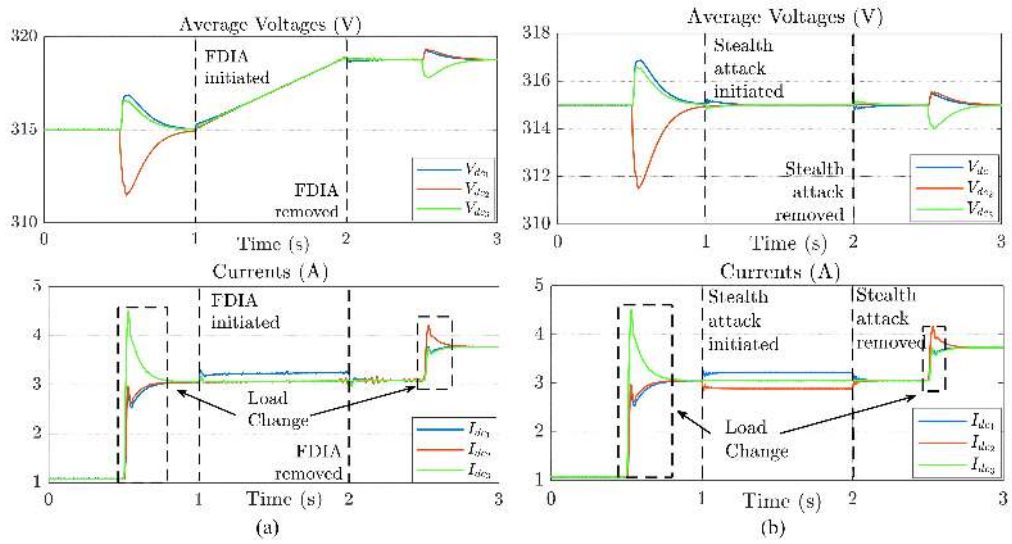

Fig. 3. Performance of DC microgrid consisting of M = 3 agents for (a) FDI attack on current sensor of agent I and (b) stealth attack on current sensors of agent I & II : Deteriorates current sharing profile.

consensus properties of a Laplacian graph [30]. Hence, it can be concluded that the final state convergence as per (10) is not affected even under stealth attacks since it gets nullified by the sum of false data injection in multiple sensors/links for a cooperative network as established in (20) & (21).

IV. Proposed Stealth Attack Detection Strategy

This section discusses about the detection of the attacked nodes in a cooperative network based DC microgrid. As opposed to the centralized systems where the global information is present at a single node, it is a complicated task to apprehend the attacked node in cooperative systems as intrusion in any agent affects the entire system for a strongly connected graph. To address the issue, this paper utilizes the concept of control output synchronization to detect the attacked node in a cooperative network where the input signals with attack vectors are deemed to achieve consensus. Following the convergence of the inputs, it is shown how the difference in their respective PI controller outputs achieves consensus for the same global reference voltage.

Remark V: Since output current from an agent, as shown in Fig. 1, is based on the voltage levels between two different points, a stealth intrusion in the agents' current values for operation at a particular load leads to change in voltage levels across the network thereby disproving (10). In simple terms, it can be stated that the agent can recognize such attacks as it would result in the current sharing error. Such error may in turn cause undesirable effects such as overloading of individual converters or reduced energy efficiency. This has been justified by a case study in Fig. 3 for FDI and stealth attack on current sensors in a DC microgrid shown in Fig. 1 of M = 3 agents. In Fig. 3(a), a false data of -0.5 A is injected into the current sensor in Agent I at t = 1 s which immediately results into improper sharing thereby reducing energy efficiency. Similarly, in Fig. 3(b), a stealth attack is attempted at t = 1 s by injecting a balanced set of zero sum attacks of $\pm$ 0.5 A into the current sensors in agent I & II simultaneously which deteriorates the current sharing profile. However, the average voltage is still maintained in Fig. 3(b) in contrast to the case for FDI attack. With the basic assumption that each agent operator bears knowledge that the system is equipped with proportionate current sharing controller, the sharing error shown in Fig. 3(a) & (b) should be a sufficient criteria to identify attacks on current sensors such that corrective action can take place. Hence, it becomes an easier task to determine such attacks in a cooperative network. However, stealth attacks on voltage sensors in case of multiple sensors/communication links can be inconspicuous to identify. In other words, the agent voltages are maneuvered in such a way that the control operation in (10) still holds true even in the presence of such attacks.

Using Remark V, the control input for voltage regulation is particularly used to present a strong case for stealth attack in this paper. Hence, the control input for average voltage regulation [36] at i^{th} agent is given by

$$u_i(k) = \sum_{j \epsilon N_i} \underbrace{a_{ij}(\bar{V}_{dc_j}(k) - \bar{V}_{dc_i}(k))}_{u_{ij}(k)} + b_i e_1^i(k) \qquad (22)$$

For various attacks in i^{th} controller, the attacked control input can be modeled as

$$\text{Sensor attack:} \quad u_i^f(k) = u_i(k - \tau_{in}^i) + \kappa u_i^a(k) \qquad (23)$$

$$\text{Cyber link attack:} \quad u_{ij}^f(k) = u_{ij}(k - \tau_d^{ij} - \tau_{in}^i) + \kappa u_i^a(k) \qquad (24)$$

where κ = 1 denote the presence of attack vector or 0, otherwise and $u_i^a(k)$ denotes the attack vector in i^{th} agent. By local investigation of $u_i^f(k)$ in each agent, non-zero synchronization error can be detected with residual output, however, it's not a sufficient criteria for detection of the attacked node(s) in a cooperative network since comparison of each residue requires global information which contradicts our case. To verify this case, the effort of the controller to synchronize the output for a given reference voltage is strategically used to indicate the

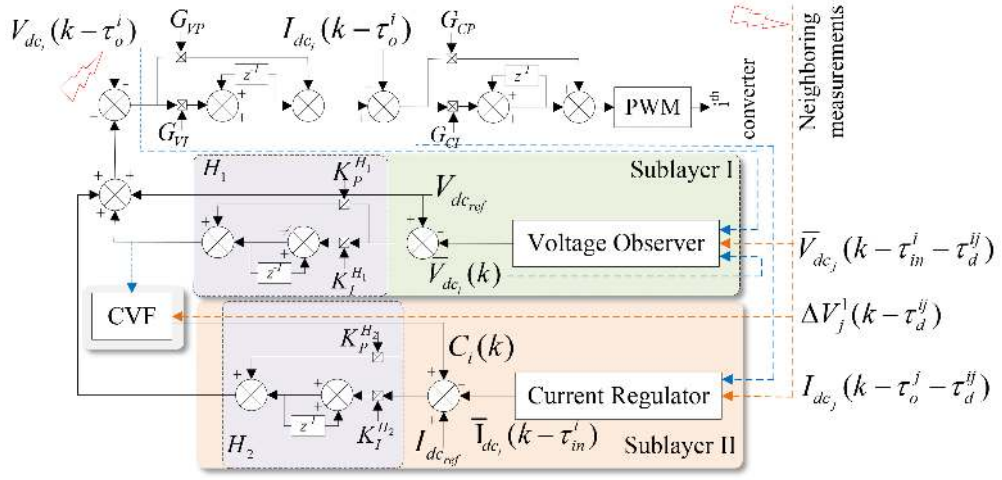

Fig. 4. Proposed controller for i^{th} agent to detect attack on sensors and communication links in DC microgrids.

occurrence of attack. It can be ensured using (3) & (7) in sublayer I to give

$$\xi_i(k) = u_i^f(k) - u_i(k-1) \tag{25}$$

for an attack within $[k-1, k]$ instant which changes due to the momentary increase/decrease in (25) as input for the attacked agents & its neighbors at the instant of attack vector injection in multiple sensors/cyber links in a microgrid. As a result, the change in PI output in sublayer I can be written as

$$\delta\Delta V_i^1(k) = K_P^{H_1}\xi_i(k) + K_I^{H_1}u_i^f(k) \tag{26}$$

where $\delta\Delta V_i^1(k) = \Delta V_i^1(k) - \Delta V_i^1(k-1)$. Using the change in outputs obtained in (26), a cooperative vulnerability factor (CVF) $C_i(k)$ is calculated using the PI controller outputs for each agent, which has been used in this paper to determine the attacked nodes accurately. Mathematically, it can be represented as

$$C_i(k) = h_i\,\underbrace{[\sum_{j\epsilon N_i} a_{ij}(\Delta V_j^1(k-\tau_d^{ij}) - \Delta V_i^1(k))]}_{o_1^i(k)} \underbrace{[\sum_{j\epsilon N_i} a_{ij}(\Delta V_j^1(k-\tau_d^{ij}) + \Delta V_i^1(k))]}_{o_2^i(k)} \tag{27}$$

for i^{th} agent, where h_i is a positive constant. Moreover, using (7) & Remark IV, we get

$$\Delta\mathbf{V}_1(k+1) - \Delta\mathbf{V}_1(k) = (K_I^{H_1} + K_P^{H_1})\mathbf{E}_1(k+1) - K_P^{H_1}\mathbf{E}_1(k) \tag{28}$$

where $\Delta\mathbf{V}_1(k)$ denotes the vector notation of $\Delta V_1^i(k)$ in (7). Since sublayer I operates as a secondary controller to achieve asymptotic convergence, $K_I^{H_1} << K_P^{H_1}$ such that the time constant of the secondary layer PI controller $(K_P^{H_1}/K_I^{H_1})$ is at least 20 times higher than the outer voltage controller in Fig. 4 to provide smooth response [37], (28) can be rewritten using Remark I as

$$\Delta\mathbf{V}_1(k+1) - \Delta\mathbf{V}_1(k) = \mathbf{E}_1(k+1) - \mathbf{E}_1(k) = -\frac{1}{K_P^{H_1}}\mathbf{L}\mathbf{E}_1(k) = 0 \tag{29}$$

Using (29) and Remark IV, it can be concluded that cooperative synchronization law [30] holds true in the absence of attacks. However in the presence of attacks, (29) synchronizes to a non-zero value which varies on the magnitude of injected attack vector. The above action can be justified by observing each secondary sublayer output in Fig. 5 for a stealth attack on multiple voltage sensors on agent II & III in a DC microgrid of different line resistances. It can be seen that the voltage correction terms from average voltage sublayer in Fig. 5(a) change symmetrically as compared to current sharing sublayer in Fig. 5(b) following a stealth attack at t = 1 s. This attribute can be explained using Remark II. Considering the system operating at steady-state, a step change of balanced zero sum attack $u_i^a(k)$ is injected into two agents during $(k-1)^{th}$ instant, (26) can be represented as

$$\Delta V_i^1(k) = K_P^{H_1}u_i^a(k) + \sum_{p=\tau_{in}^i}^{k} K_I^{H_1}(u_i(p-\tau_{in}^i)) + \underbrace{\sum_{p=(k-1)}^{k} K_I^{H_1}(u_i^a(p))}_{\Gamma_i(p)} \tag{30}$$

Eliminating the first two terms in RHS of (30) using Remark IV & substituting (30) in (27), it can be concluded that $o_1^i(k)$ and $o_2^i(k)$ will always lead to positive/negative values due to $\Gamma_i(k)$ for a balanced sum zero attack only on the attacked nodes. As a result, $C_i(k)$ of the attacked nodes will always reflect a positive value. This provides a sufficient criteria for the detection of the attacked nodes in case of multiple sensor/link based stealth attack in DC microgrids. Concluding the above discussion, the cooperative vulnerability factor algorithm for each agent will result into

$$C_i(k) = \begin{cases} 0 & \text{, if } \kappa = 0 \\ > 0 & \text{, else} \end{cases} \tag{31}$$

However, under worst cases, $C_i(k)$ can also be manipulated by the attacker using subtraction to make it negative, which

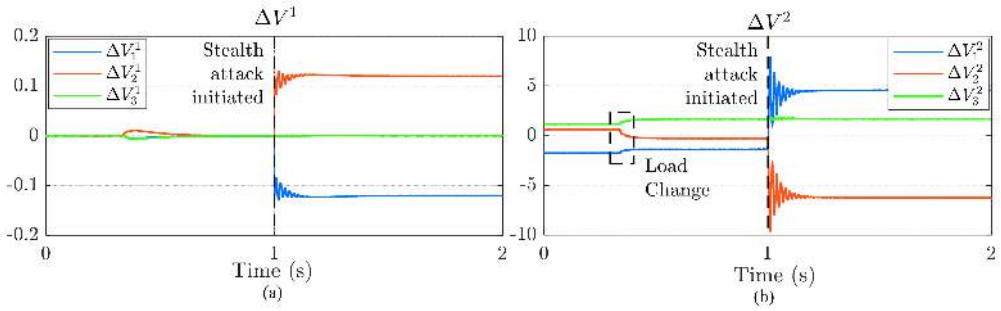

Fig. 5. Case study II: Performance of (a) average voltage regulation and (b) current sharing for a strong case of stealth attack on voltage sensors of agent II & III.

displeases our attack detection criteria. To handle these discrepancies, $C_i(k)$ is tactically added to $e_2^i(k)$ in (8), which can now be rewritten as

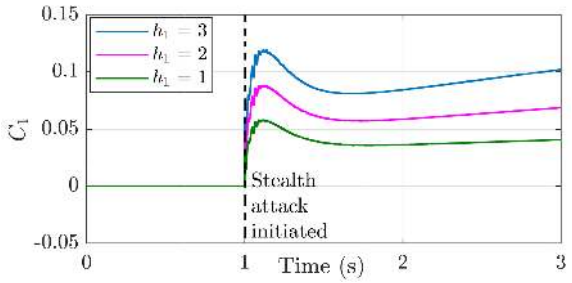

Fig. 6. Variation of C_1 for different values of the design parameter h_1.

$$\Delta V_i^2(k) = K_P^{H_2} \underbrace{(I_{dc_{ref}} + C_i(k) - \bar{I}_{dc_i}(k - \tau_{in}^i))}_{\bar{e}_2^i(k)} + K_I^{H_2} \sum_{p=\tau_{in}^i}^{k} (I_{dc_{ref}} + C_i(k) - \bar{I}_{dc_i}(p - \tau_{in}^i)) \quad (32)$$

such that the control operation will be disoriented locally, thereby allowing the agents to reliably detect the attacks. Since $I_{dc_{ref}}$ = 0, the cross-coupling of the CVF suggested in (32) will supplement to accurate detection and facilitates protection against attacks on CVF since $C_i(k)$ now forms the forward path between both secondary control sublayers. By doing so, further attacks on $C_i(k)$ will disorient the objectives laid down for the outer voltage controller in sublayer I since it disregards (10). The CVF output $C_i(k)$ when cross-coupled into sublayer II introduces a ramp signal into its input. The ramp up/down of $C_i(k)$ can be explained using the addition of the term $\Gamma_i(k)$ in (30), which ramps up/down indefinitely for $k \to \infty$ unless the positive/negative attack vector is removed from i^{th} agent. Hence, the ramp up/down of $C_i(k)$ in the positive region qualifies as a sufficient criteria for the corresponding node to be declared as *attacked* in the cooperative realm for DC microgrids.

Moreover in Fig. 6, it can be seen that the slope of $C_1(k)$ increases with increase in h_1 for a particular stealth attack in two sensors. As the ramping up/down of $C_i(k)$ is already established above, the steady state error $e_{ss}^i(k)$ for the ramp input $C_i(k) = \sum_{p=0}^{k} h_i p$ in the error term $\bar{e}_2^i(k)$ in (32), when introduced into the PI controller in sublayer II with the unity feedback output $y_i(k)$ can be calculated using

$$e_{ss}^i(k+1) - e_{ss}^i(k) = [y_i(k+1) - y_i(k)] - [C_i(k+1) - C_i(k)] \quad (33)$$

$$e_{ss}^i(k+1) - e_{ss}^i(k) = K_P^{H_2} e_{ss}^i(k+1) - K_P^{H_2} e_{ss}^i(k) + K_I^{H_2} e_{ss}^i(k+1) - [C_i(k+1) - C_i(k)] \quad (34)$$

$$e_{ss}^i(k+1) - e_{ss}^i(k) = K_P^{H_2} e_{ss}^i(k+1) - K_P^{H_2} e_{ss}^i(k) + K_I^{H_2} e_{ss}^i(k+1) - h_i \quad (35)$$

$$e_{ss}^i(k+1)[1 - K_P^{H_2} - K_I^{H_2}] = e_{ss}^i(k)[1 - K_P^{H_2}] - h_i \quad (36)$$

Since the abovementioned analysis is based on steady state conditions, $e_{ss}^i(k+1) \approxeq e_{ss}^i(k)$. Using this approximation in (36), we get

$$e_{ss}^i(k) = \frac{h_i}{K_I^{H_2}} \quad (37)$$

Hence, (37) implies that for higher values of h_i with constant $K_i^{H_2}$, the system may quickly lead into unstable zone owing to high steady state error considering bounded stability whereas for lower values of h_i, it is difficult to determine the attacked node under worse scenarios of stealth attack due to slow ramping. Since the main focus of the paper is to detect the attacked unit accurately alongside prevention of further coordinated attacks, it is a seemingly fair approach to include the cross-coupling strategy such that the defense mechanism can take place immediately without disrupting stability for lower values of h_i.

V. Simulation Results

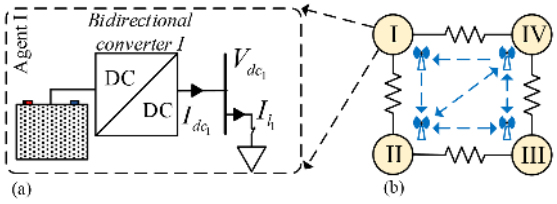

Fig. 7. Considered system: (a) Agent model and (b) Cyber-physical DC microgrid with four sources.

The proposed attack detection strategy is tested on a cyber-physical DC microgrid as shown in Fig. 7(b) with $V_{dc_{ref}}$ = 315

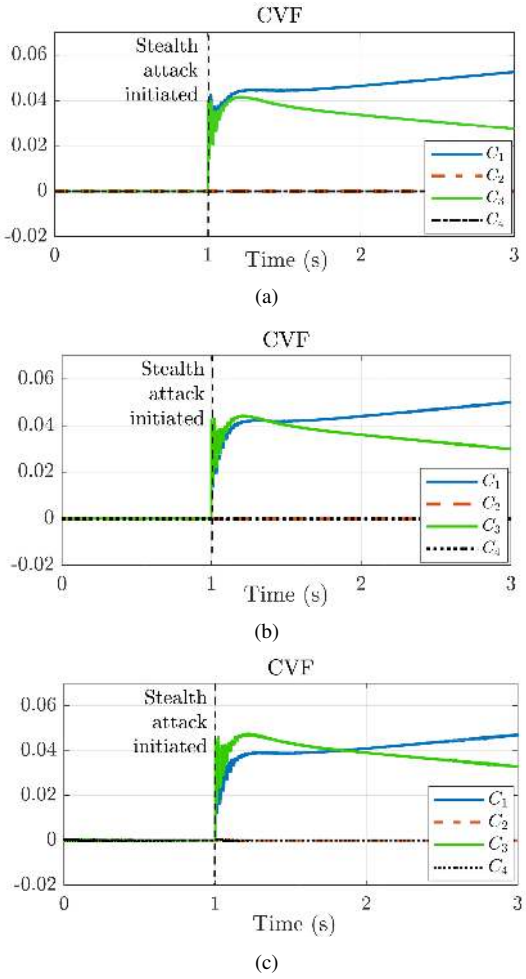

Fig. 8. Proposed detection strategy for case study I in Fig. 2: (a) without input, output & communication delay, (b) with delay(maximum value in the network): $\tau_{in}\Delta t$ = 1 ms, $\tau_o\Delta t$ = 3.5 ms, $\tau_d\Delta t$ = 45 ms, (c) with delay(maximum value in the network): $\tau_{in}\Delta t$ = 1 ms, $\tau_o\Delta t$ = 3.5 ms, $\tau_d\Delta t$ = 80 ms, where Δt is the sampling time.

V consisting of four agents of equal capacities interconnected to each other via resistive lines. It should be noted that each agent consists of a battery accompanied via DC/DC bidirectional converters respectively as shown in Fig. 7(a). To test the performance of the proposed attack detection strategy for cooperative DC microgrid, it has been tested against several disturbances such as FDIA, stealth attack in multiple sensors, which usually goes undetected by distributed observers, communication links to detect the affected node such that necessary action can be taken to maintain security. The system & control parameters are provided in Appendix. It should be noted that each event in the abovementioned scenarios are separated by a certain time-gap to provide clear understanding.

A. Behavior of Proposed Stealth Detection Strategy for Case Study I

For case study I in Fig. 2, the behavior of the proposed strategy without considering input, output & communication delay is shown in Fig. 8(a). As the stealth attack is initiated at t = 1 s in agent I & III, the values of C_1 & C_3 rises up into the positive region suggesting those agents to be the attacked units. Further, the performance of the proposed strategy in response to case study I is tested with input, output(within the agent) & communication(between two agents) delays in Fig. 8(b) & (c). It should be noted that input & output delays are constant whereas communication delays are time-varying [31]. As the distributed control law for DC microgrids provides rugged response to delays due to the dynamic averaging concept within an upper bound on the communication delay for a given well-spanned network [36], the philosophy of the proposed detection strategy under delays will be unaltered if the cooperative synchronization law in Remark IV holds true for the underlying control layer. As compared to Fig. 8(a), it can be seen that the CVF of the attacked agents initially rise with different peak magnitudes under delays of $\tau_{in}\Delta t$ = 1 ms, $\tau_o\Delta t$ = 3.5 ms, $\tau_d\Delta t$ = 45 ms & 80 ms(Δt is the sampling time) in Fig. 8(b) & (c) respectively, which can be attributed to varying delay in achieving consensus due to delayed measurements & inputs. It is worth notifying that the results in Fig. 8(b)-(c) have been investigated for maximum value of delay in the network to test the robustness of the proposed strategy. Since the CVF values of the affected agent goes instantly into the positive region in Fig. 8(a)-(c), it can be concluded that the proposed strategy entails faster detection of stealth attacks even under delays.

B. Scenario I

In scenario I, the voltage sensor in agent I is attacked with u_1^a = - 7 V at t = 1 s. As a result, due to the presence of distributed voltage observer designed for each agent in (5), the average voltage estimate in Fig. 9 immediately dips to 313 V for each agent. Assuming that the reference voltage of operation is known to every agent, the error in average voltage estimate should serve as a sufficient criteria to detect the presence of FDIA in the system. However, the identification of the attacked agent still remains a question. This paper has dealt with this issue by observing $C_i(k)$ in (27), which always converges to zero in the absence of attacks. In this case, it can be seen that the average voltage estimates do achieve consensus however, they synchronize to a different value $V_{dc_{ref}}^a$. When the PI output of voltage sublayer change symmetrically as shown in Fig. 5(a), $o_1(k)$ in (27) becomes comparatively apparent for the attacked node(s). Consequently, C_1, as shown in Fig. 9, rises upto 0.05 as per the proposed strategy which suggests that either sensors/links in agent I are maltreated with an attack. Prior to detection of the attacked node, a corrective measure is taken at t = 1.5 s where the outgoing links from agent I are deactivated. With link deactivation, it can be seen that the average voltage estimate restores back to 315 V. Another advantage with the proposed strategy is that it acts as a worthy index to denote if the injected false data is still active with the agent. When the injected false data is removed by the attacker at t = 2 s, C_1 immediately goes to zero. Since the system is secure, the deactivated link is restored back.

C. Scenario II

In scenario II, the outgoing cyber links from agent III is attacked with a set of attack vectors of $\pm$ 3 V at t = 1 s

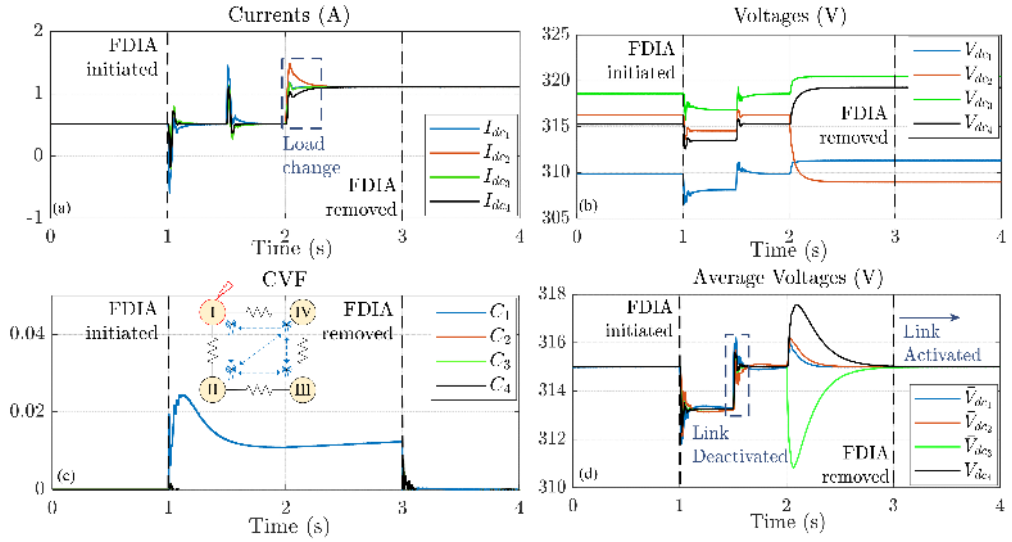

Fig. 9. Scenario I(a) Currents, (b) Voltages, (c) CVF, (d) Average voltages: False data injection attack on voltage sensor at t = 1 s in agent I. As seen, the average voltage dips on initiating FDIA. It is shown that the CVF of agent I instantly shoots into the positive region to detect the affected agent.

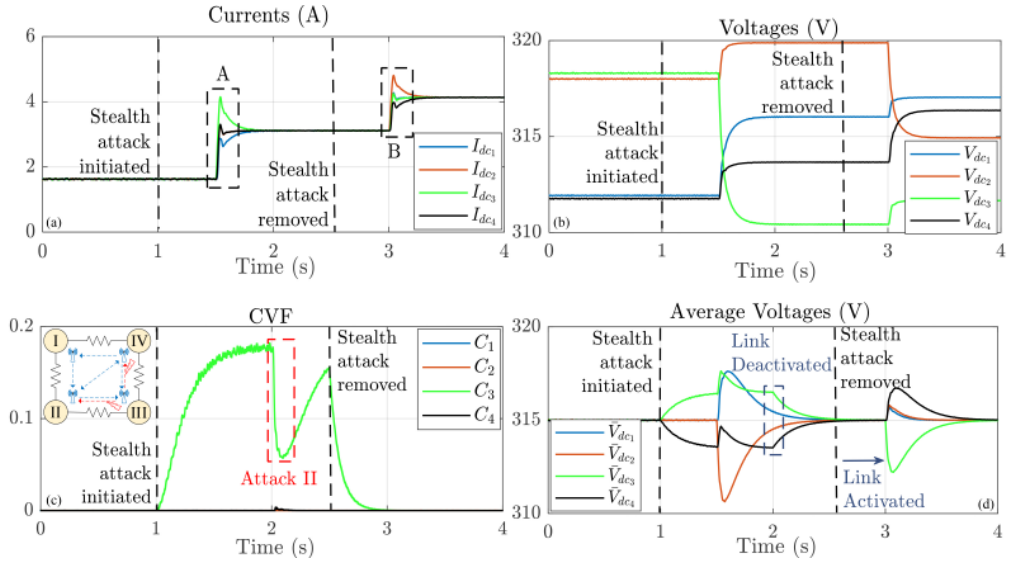

Fig. 10. Scenario II(a) Currents, (b) Voltages, (c) CVF, (d) Average voltages: Stealth attack on two outgoing cyber links at t = 1 s from agent III. It is shown that the average voltage estimates diverge symmetrically on initiating the attack. The proposed strategy accurately detects the *attacked* agent.

such that the cumulative effect seen in a cooperative network is zero. Prior to initiating the attack, it is difficult to denote the attacked node from the average voltage estimate as both estimates diverge symmetrically. Considering this problem using a distributed observer based approach, norm of these errors would mistranslate into two attacked nodes, i.e., agent III & IV. This issue is well addressed using the proposed approach since C_3 as shown in Fig. 10 shoots up to 0.18 thereby suggesting that agent III is attacked. As a protective measure of security, the outgoing links from agent III are deactivated which brings the average voltage estimate into synchronism by tracking the desired reference value of 315 V. For load changes highlighted as *A* & *B*, the system performs satisfactorily. To test the robustness of the proposed approach under worse case scenarios, another consecutive attack at t = 2 s is preempted by the attacker to manipulate C_3 by reducing it to a negative value. However, due to cross-coupling of $C_i(k)$ into sublayer II in (32), it prevents further exploitation as it can't disorient the nested control output for a particular operating point.

D. Scenario III

In scenario III, a balanced attack of $\pm$ 10 V in sensors of agent I & IV respectively at t = 1 s is practiced in Fig. 11 to test the fidelity of the proposed approach. As C_1 & C_4 shoots up in the positive region, agent I & IV are plugged out of the system at t = 1.5 s. Based on *Assumption 2* in [28], the network connectivity is affected due to plugging out of $M/2$ agents which leads to change in system dynamics. On clearing out of the attack at t = 3 s indicated by C_1 & C_4 dropping to zero, the converters are plugged back in around

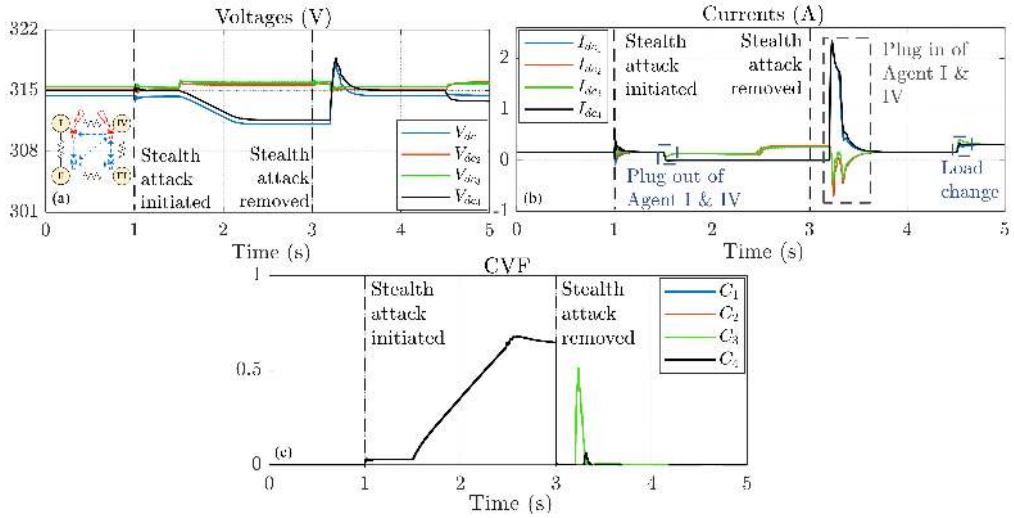

Fig. 11. Scenario III(a) Currents, (b) Voltages, (c) CVF: Stealth attack on voltage sensors of agent I & IV at t = 1 s. Upon initiating the attack, the average voltages and current sharing remain intact. As seen, the proposed strategy identifies the *attacked* agents instantly with the CVF for agent I & IV in the positive region.

t = 3.2 s resulting into restoration of the average voltage estimates to 315 V.

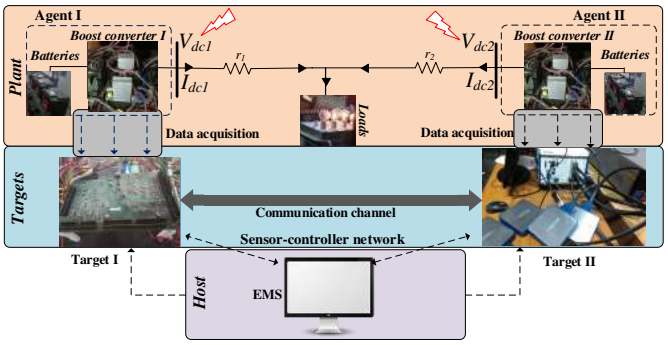

Fig. 12. Experimental setup of DC microgrid comprising 2 agents.

VI. Experimental Results

The proposed strategy has been experimentally validated in a DC microgrid comprising 2 agents as shown in Fig. 12. Two lead acid battery banks, where each bank consist of 3 batteries in series for an overall input voltage of 36 V, are connected to the loads via DC/DC boost converters of equal capacities and tie-lines operate to achieve average voltage regulation & share the load current proportionately among themselves. The analog measurements received from Hall effect transducers, LA 25-P and LV 20-P from each agent is acquired via two local controllers equipped with Xilinx board as highlighted in Fig. 12. Agent I is controlled using a National Instruments sbRIO 9683 chassis (Target I) with embedded data acquisition card sbRIO 9606. On the other hand, source II is controlled using a NI PXIe-8840 (Target II) with data acquired using NI PXIe 7853R series boxes and the control algorithms are implemented in LabVIEW which provides a GUI to produce respective gating signals for both the converters. The sensor attacks on the voltage sensors were modeled using (23). The experimental testbed parameters have been provided in Appendix.

A. Scenario I

In Fig. 13(a), when a false data of $u_1^{a,1}$ = 3 V is injected into the voltage sensor in agent I during event A, it leads to an increase in the voltage observer output. Consequently, the voltage of agent II also increases from 48.1 V to 51.6 V. This results into increase of C_1 from 0 to 0.2 V which ensures the attack vector in agent I. After a certain instant, when the link from agent I is deactivated which halts the propagation of false data during event B, agent II voltage returns back to 48.1 V. However, the injected false data is still effective which is evident from C_1 in Fig. 13(a). Under the worse case, the attacker may try to manipulate C_1 into the negative region such that the disabled link is restored. In event C, another attack vector $u_1^{a,2}$ = -1.2 V is injected into C_1, which doesn't affect its detection philosophy as it is strategically oriented into the control system of each agent using the cross-coupling methodology.

B. Scenario II

Similarly in Fig. 13(b), a stealth attack is modeled by injecting a balanced set of zero sum vectors $u_i^f = \pm$ 3 V into voltage sensors of both the agents prior to event A. Following the transient, both the voltages return back to their respective set-points before attacks. However, C_1 & C_2 increase from 0 to 0.2 V which suggests that both agents are *attacked*. To prevent further damage, a corrective action by disabling the cyber links during event B in Fig. 13(b) results into local operation for each agent.

VII. Conclusion

This paper proposes a general cyber attack detection framework for cyber-physical DC microgrids. The vulnerability of the conventional cooperative techniques in DC microgrids under false data injection is investigated in detail. In addition to that, the modeling of stealth attacks, which manage to

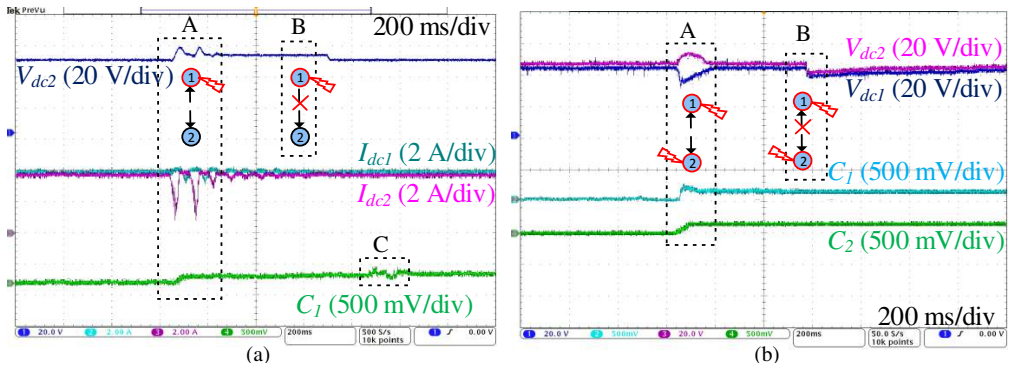

Fig. 13. Experimental validation of (a) FDIA, and (b) stealth attack on voltage sensor(s) in a DC microgrid with M = 2 agents. The experimental results validate the proposed findings.

deceive distributed observers is carried out using necessary and sufficient conditions. To address this issue, a cooperative vulnerability factor algorithm is presented which operates on the PI output of the voltage observer to track changes for each agent so as to provide an accurate identification strategy of the attacked agent(s). To add fidelity, it is cross-coupled with the secondary current sublayer such that it operates under worst scenarios of attacks. Its robustness is evaluated using both simulation and experimental results for both false data injection and stealth attacks on multiple sensors/links.

APPENDIX

Simulation Parameters

The considered system consists of four sources rated equally for 3 kW. It is to be noted that the line parameter R_{ij} is connected from i^{th} agent to j^{th} agent. Moreover, the controller gains are consistent for each agent.

Plant: R_{12} = 1.3 Ω, R_{13} = 1.8 Ω, R_{23} = 1.2 Ω, R_{43} = 1.5 Ω
Converter: L_i= 3 mH, C_{dc_i}= 250 μF, $i_{b_1}^{max} = i_{b_2}^{max}$ = 9.5 A
Controller: $V_{dc_{ref}}$= 315 V, $I_{dc_{ref}}$ = 0, $K_P^{H_1}$ = 3, $K_I^{H_1}$ = 0.01, $K_P^{H_2}$ = 4.5, $K_I^{H_1}$ = 0.32, G_{VP} = 2.8, G_{VI} = 12.8, G_{CP} = 0.56, G_{CI} = 21.8, h =1, c = 0.4

Experimental Testbed Parameters

The considered system consists of two sources with the converters rated equally for 350 W. It should be noted that the controller gains are consistent for each agent.

Plant: r_1 = 0.25 Ω, r_2 = 0.325 Ω, x_2 = 30 μH, L_i= 3 mH, C_{dc_i}= 100 μF
Controller: $V_{dc_{ref}}$= 48 V, $I_{dc_{ref}}$ = 0, $K_P^{H_1}$ = 240.6, $K_I^{H_1}$ = 1.6, $K_P^{H_2}$ = 4.5, $K_I^{H_1}$ = 0.08, G_{VP} = 0.07, G_{VI} = 4, G_{CP} = 0.02, G_{CI} = 19.4, h = 1, c = 0.4

REFERENCES

[1] R H Lasseter, "Smart distribution: Coupled microgrids" in *Proceedings of the IEEE*, vol. 99, no. 6, pp. 1074–1082, 2011.

[2] T Dragicevic, X Lu, JC Vasquez, JM Guerrero, "DC microgrids - Part I: A review of control strategies and stabilization techniques", *IEEE Trans. Power Elect.*, vol. 31, no. 7, pp. 4876-4891, 2016.

[3] L. Meng, T. Dragicevic, JM Guerrero and JC Vasquez, "Dynamic consensus algorithm based distributed global efficiency optimization of a droop controlled DC microgrid", *Energy Conference (ENERGYCON), 2014 IEEE Intl.*, pp. 1276-1283, 2014.

[4] M. Yazdanian and A. Mehrizi-Sani, "Distributed Control Techniques in Microgrids," *IEEE Trans. Smart Grid*, vol. 5, no. 6, pp. 2901–2909, 2014.

[5] S. Sahoo and S. Mishra, "An Adaptive Event-Triggered Communication Based Distributed Secondary Control for DC Microgrids", *IEEE Trans. Smart Grid*, 2017, DOI: 10.1109/TSG.2017.2717936

[6] T Dragicevic, X Lu, JC Vasquez, JM Guerrero, "DC microgrids - Part II: A review of power architectures, applications, and standardization issues", *IEEE Trans. Power Elect.*, vol. 31, no. 5, pp. 3528-3549, 2016.

[7] V. Nasirian, S. Moayedi, A Davoudi and F. L. Lewis, "Distributed Cooperative Control of DC Microgrids," *IEEE Trans. Power Elect.*, vol. 30, no. 4, pp. 2288–2303, 2015.

[8] S Anand, BG Fernandes, and JM Guerrero, "Distributed control to ensure proportional load sharing and improve voltage regulation in low-voltage DC microgrids." *IEEE Trans. Power Elect.*, vol. 28, no. 4, pp. 1900-1913, 2013.

[9] T Morstyn, H Branislav and GV Agelidis, "Cooperative multi-agent control of heterogeneous storage devices distributed in a dc microgrid", *IEEE Trans. Power Systems*, vol. 31, no. 4, pp. 2974–2986, 2016.

[10] C. K. Veitch, J. M. Henry, B. T. Richardson, and D. H. Hart, "Microgrid cyber security reference architecture," *Sandia Nat. Lab.(Hierarch. SNLNM), Albuquerque, NM, USA, Tech. Rep. SAND2013-5472*, 2013.

[11] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inf. Syst. Security*, vol. 14, no. 1, p. 13, 2011.

[12] G. Liang, J Zhao, F Luo, SR Weller and ZY Dhong, "A Review of False Data Injection Attacks Against Modern Power Systems", *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1630–1638, 2017.

[13] 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, 2013.

[14] Y Yan, *et al.*, "A survey on cyber security for smart grid communications", *IEEE Comm. Surveys and Tutorials*, vol. 14, no. 4, pp. 998-1010, 2010.

[15] P Li, *et al.*, "A Robust Distributed Economic Dispatch Strategy of Virtual Power Plant Under Cyber-Attacks", *IEEE Trans. Ind. Inform.*, 2018, DOI: 10.1109/TII.2017.2788868

[16] J Zhao, L Mili, and M Wang, "A Generalized False Data Injection Attacks Against Power System Nonlinear State Estimator and Countermeasures", *IEEE Trans. Power Sys.*, 2018, DOI: 10.1109/TPWRS.2018.2794468

[17] S Sridhar, M Govindarasu, and CC Liu, "Risk analysis of coordinated cyber attacks on power grid", *Control optimization methods for electric smart grids*, pp. 275–294, Springer, 2012.

[18] J Salmeron, K Wood, R Baldick,"Analysis of electric grid security under terrorist threat", *IEEE Trans Power Syst.*, vol. 19, no. 2, pp. 905–912, 2004.

[19] Z Li, M Shahidehpour, A Alabdulwahab, and A Abusorrah, "Bilevel Model for Analyzing Coordinated Cyber-Physical Attacks on Power Systems", *IEEE Trans. Smart Grid*, vol. 7, no. 5, pp. 2260–2272, 2016.

[20] Y Chakhchoukh, and H Ishii, "Coordinated Cyber-Attacks on the

Measurement Function in Hybrid State Estimation", *IEEE Trans. Power Sys.*,vo. 30, no. 5, pp. 2487–2497, 2018.
[21] SD Manshadi, and ME Khodayar,"Resilient Operation of Multiple Energy Carrier Microgrids", *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2283–2292, 2015.
[22] MM Rana, L Li, and SW Su,"Cyber Attack Protection and Control of Microgrids", *IEEE Journ. Automat.*, vol. 5, no. 2, 602–609, 2018.
[23] J. Hao, E. Kang, J. Sun, Z. Wang, Z. Meng, X. Li, and Z. Ming, "An adaptive markov strategy for defending smart grid false data injection from malicious attackers," *IEEE Trans. Smart Grid*, vol. 9. no. 4, pp. 2398–2408, 2018.
[24] O. Beg, T. Johnson, and A. Davoudi, "Detection of false-data injection attacks in cyber-physical dc microgrids," *IEEE Trans. Ind. Inform.*, vol. 13, no. 5, pp. 2693–2703, 2017.
[25] D Ding, *et al.*, "Observer-based event-triggering consensus control for multiagent systems with lossy sensors and cyber-attacks", *IEEE Trans. Cyber.*, vol. 47, no. 8, pp. 1936-1947, 2017.
[26] H. Fawzi, P. Tabuada, and S. Diggavi, "Secure estimation and control for cyber-physical systems under adversarial attacks," *IEEE Trans. Autom. Control*, vol. 59, no. 6, pp. 1454–1467, June 2014.
[27] H Zhang, *et al*, "Distributed Load Sharing under False Data Injection Attack in Inverter-Based Microgrid", *IEEE Trans. Ind. Electron.*, 2018, DOI: 10.1109/TIE.2018.2793241
[28] S. Abhinav, H Modares, FL Lewis, F Ferrese and A Davoudi, "Synchrony in Networked Microgrids under Attacks", *IEEE Trans. Smart Grid*, 2017, DOI: 10.1109/TSG.2017.2721382
[29] C. Zhao, J. He, P. Cheng, and J. Chen, "Analysis of consensus-based distributed economic dispatch under stealthy attacks," *IEEE Trans. Ind. Electron.*, vol. 64, no. 6, pp. 5107–5117, 2017.
[30] M Zhu, and S Martinez, "Discrete-time dynamic average consensus", *Automatica*, vol. 46, no. 2, pp. 322–329, 2010.
[31] X Xu, and G Feng, "Consensus of Discrete-Time Linear Multiagent Systems With Communication, Input and Output Delays", *IEEE Trans. Autom. Control*, vol. 63, no. 2, pp. 492–497, 2018.
[32] O Beg, LV Nguyen, T Johnson, and A Davoudi, "Signal Temporal Logic-based Attack Detection in DC Microgrids", *IEEE Trans. Smart Grid*, 2018, DOI: 10.1109/TSG.2018.2832544
[33] P Danzi, C Stefanovic, L Meng, JM Guerrero, and P Popovski, "On the Impact of Wireless Jamming on the Distributed Secondary Microgrid Control",*arXiv preprint*: 1609. 07368, 2016.
[34] X Zhong, L Yu, R Brooks, and GK Venayagamoorthy, "Cyber Security in Smart DC Microgrid Operations", *2015 IEEE Intl. Conf. DC Microgrids (ICDCM)*, pp. 1–6, 2015.
[35] RA Brualdi, and JR Herbert, "Combinatorial matrix theory", vol. 39, *Cambridge: Cambridge University Press*, 1991.
[36] S Sahoo and S Mishra,"A Distributed Finite-Time Secondary Average Voltage Regulation and Current Sharing Controller for DC Microgrids", *IEEE Trans. Smart Grid*, 2017, DOI: 10.1109/TSG.2017.2737938
[37] S Mishra, S Sahoo and A Dugar,"Hybrid MVMO based controller for energy management in a grid connected DC microgrid", *Power, Communication and Information Technology Conference (PCITC), 2015 IEEE*, pp. 114-119, 2015.

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. He is currently working as a Research Fellow in the Department of Electrical and Computer Engineering in National University of Singapore.

His current research interests include microgrids, cyber security, coordinated control and stability of cyber-physical systems.

Sukumar Mishra (M'97-SM'04) is a Professor at Indian Institute of Technology, New Delhi and has been part of IIT Delhi for the past 15 years. He has published over 200 research articles (including papers in international journals, conferences and book chapters).

Prof. Mishra has won many accolades throughout his academic tenure of 25 years. He has been a recipient of INSA medal for young scientist (2002), INAE young engineer award (2009), INAE silver jubilee young engineer award (2012) and has recently won the Samanta Chandra Shekhar Award (2016). He has been granted fellowship from many prestigious technical societies like IET (UK), NASI (India), INAE (India), IETE (India) and IE (India) and is also recognized as the INAE Industry Academic Distinguish Professor. Currently, Prof. Mishra is holding the position of Vice Chair of Intelligent System Subcommittee of Power and Energy society (PES) of IEEE. Apart from all research and academic collaborations, Prof. Mishra is very actively involved in industrial collaborations. Prof. Mishra is currently acting as INAE Chair professor and has previously delegated as the NTPC and Power Grid Chair professor. He is also serving as an Independent Director of the Cross Border Power Transmission Company Ltd. and the River Engineering Pvt. Ltd.

Prof. Mishra's research expertise lies in the field of Power Systems, Power Quality Studies, Renewable Energy and Smart Grid. Prof. Mishra is currently serving as an Editor for the IEEE Transactions on Smart Grid and an Associate Editor for the IET Generation, Transmission & Distribution journal

Jimmy Chih-Hsien Peng (M'04) is currently an Assistant Professor of Electrical and Computer Engineering at the National University of Singapore, Singapore. Previously, he was a faculty 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, Massachusetts. He later became a Visiting Assistant Professor at MIT in 2014.

He currently serves as the secretary for IEEE Power and Energy Society Working Group on High-Performance Computing for Power Grid Analysis and Operation. He is also a committee member for Singapore Standard SS 535. His research interests include power system stability, cyber security, microgrids, and high-performance computing.

Tomislav Dragičević (S'09-M'13-SM'17) received the M.Sc. and the industrial Ph.D. degrees in Electrical Engineering from the Faculty of Electrical Engineering, Zagreb, Croatia, in 2009 and 2013, respectively. From 2013 until 2016 he has been a Postdoctoral research associate at Aalborg University, Denmark. From March 2016 he is an Associate Professor at Aalborg University, Denmark. He made a guest professor stay at Nottingham University, UK during spring/summer of 2018.

His principal field of interest is overall system design of autonomous and grid connected DC and AC microgrids, and application of advanced modeling and control concepts to power electronic systems. He has authored and co-authored more than 140 technical papers (more than 55 of them are published in international journals, mostly IEEE Transactions) in his domain of interest and 8 book chapters and a book in the field. He serves as an Associate Editor in the IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS and in the Journal of Power Electronics. Dr. Dragičević is a recipient of a Končar prize for the best industrial PhD thesis in Croatia, and a Robert Mayer Energy Conservation award.