Distributed Screening of Hijacking Attacks in DC Microgrids

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

Published in:
I E E E Transactions on Power Electronics

DOI (link to publication from Publisher):
10.1109/TPEL.2019.2957071

Publication date:
2020

Document Version
Accepted author manuscript, peer reviewed version

Citation for published version (APA):
Sahoo, S., Chih-Hsien Peng, J., Mishra, S., & Dragicevic, T. (2020). Distributed Screening of Hijacking Attacks in DC Microgrids. *I E E E Transactions on Power Electronics*, *35*(7), 7574-7582. Article 8918297. https://doi.org/10.1109/TPEL.2019.2957071

Distributed Screening of Hijacking Attacks in DC Microgrids

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

***Abstract*—It is well known that distributed control can improve the resiliency of DC microgrids against multiple link failures as compared to centralized control. However, the control layer is still vulnerable to cyber attacks. Unlike widely studied false data injection attacks (FDIAs), which involve adding false signals on top of existing ones in the controller or communication links, hijacking attacks completely replace the existing signals. As a result, the compromised agent(s) diverge from steady state owing to imbalance in the iterative rule of consensus algorithm. To detect hijacking attacks, a novel distributed screening (DS) methodology is proposed. In addition to that, a fault detection (FD) metric is provided to assist the proposed attack detection strategy in differentiating between hijacking attacks and sensor faults. This reduces the complexity of decision making in the attack mitigation approach. Further, interoperability of the proposed detection metrics allows simultaneous detection of sensor faults and hijacking attacks. The performance of the proposed detection metrics is evaluated under simulation and experimental conditions to conclude that it successfully detects the attacked agent(s) as well as sensor fault(s).**

***Index Terms*—DC microgrid, cyber attack detection, distributed control.**

I. Introduction

DISTRIBUTED control of DC microgrids offers a reliable, flexible and economic alternative to centralized approach [1]. It provides resiliency from single-point-of-failure and operating flexibility with plug-and-play capability [2]. This philosophy has been extensively adopted for many purposes, such as energy balancing and current sharing solely using local and neighboring measurements [3]-[4]. Albeit its operational advantages, integration of communication and automation technologies increase the vulnerability of microgrids to cyber attacks [5]. These vulnerabilities allow potential adversaries to create unfavorable scenarios, which may lead to uneconomic operation, instability or system shutdown. This is a thriving concern for microgrid system operators, as the recent advancements in control and monitoring systems are exposed to such vulnerabilities [6]-[7].

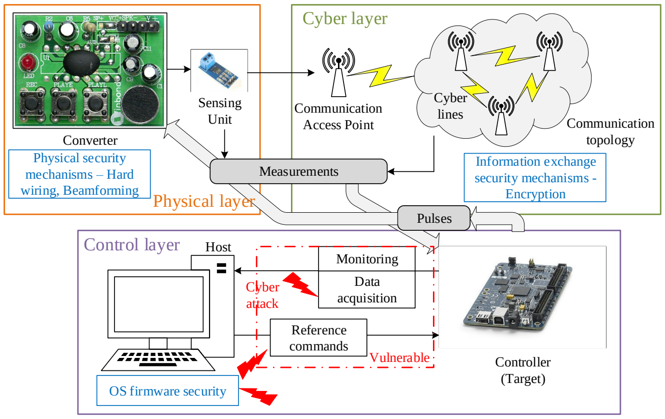


Fig. 1. Key vulnerable sections in industrial cyber-physical microgrids with security mechanisms - Control layer could be highly vulnerable to cyber intrusions via malware, if the regular host security updates go missing.

Many prevention mechanisms, such as, cryptography, authentication and access control processes have been designed to avoid facing any interruptions. Particularly for information exchange in the cyber layer, many encryption based security mechanisms are devised for the cyber layer. Further in the physical layer, the sensors are usually hard wired to ensure security. However, these efforts are still limited with regard to platform and communication security [8]-[9]. As shown in Fig. 1, the biggest security concern in industrial microgrids is often faced in the control layer instead of the cyber-physical layer [10]. As per many cybersecurity experts, malware intrusion into the host (as shown in Fig. 1) can be classified as a broad class of attack to compromise the system [11]. They can easily jeopardize operation of mission-critical autonomous systems such as, naval ships and submarines by malware propagating websites or tainted files. These elements often bypass the host security mechanism due to missing uninstalled updates in the host. Recently, a denial-of-service bug was found in the in-flight entertainment, which affected the critical flight systems [12]. According to the 2011 annual report of the Repository for Industrial Security Incidents (RISI), around 35% of industrial control system (ICS) security incidents were instigated through remote access of the host [13]. Hence, this necessitates the need to protect microgrids from hijacking attacks from a control design perspective.

From the control perspective, cyber attacks in microgrids are studied for covert [14], replay attacks [15], and attacks on energy management systems [16]. Further, the impact of the most prominent cyber attack in microgrids, i.e. the false data injection attack (FDIA) is extensively studied in [21]-

This research is supported by the National Research Foundation (NRF) Singapore under the grant number R-263-000-D42-281.

S Sahoo and T Dragičević are with the Department of Energy Technology, Aalborg University, Aalborg East, 9220, Denmark (e-mail: sssa@et.aau.dk and tdr@et.aau.dk)

J Peng is with the Department of Electrical and Computer Engineering, National University of Singapore, Singapore, 119007 (e-mail: 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-110016 (e-mail: sukumar@ee.iitd.ac.in)

[22]. Such attacks, when formulated in a sophisticated way to hide their presence from state observers, are termed as *stealth* attacks [23]. They are capable of disrupting the network stability and control structures deceitfully. A distinguishing feature of FDIAs is that they only add a false value on top of existing measurement signals. With regards to distributed control theory, asymptotic convergence to reach consensus is still possible, even though the final value may be incorrect. On the other hand, a separate class of intrusion approach, namely a hijacking attack, interrupts the update process of the consensus algorithm by completely replacing the existing signal with an exogenous input [24]. The impact of such attacks, alternatively referred to as random attacks, have been extensively studied in [25]-[26], where it was shown that they can deter the optimal performance of the microgrid. Since it replaces the time-stamped measurement with a constant input, the linear consensus algorithm fails to update its reference state with respect to its neighboring agents, ultimately resulting in inevitable power imbalance. Moreover, it is difficult to detect the attacked agent under such conditions since a disruption in consensus theory causes all the agents to misbehave simultaneously. Hence, detection of hijacking attacks in DC microgrids becomes more challenging than FDIAs.

Interestingly, some papers have addressed this problem also when agents have simply crashed or have sensor faults [27]-[28]. Hence, prior focus should be provided on accurate detection of hijacking attacks alongwith differentiation between cyber attack and sensor faults, especially when the misbehaving agents have malicious intent rather than simply being subjected to faults. Any sensor fault, which is usually caused by an interruption in the sensor-controller network, can disrupt the operation of agent(s) in DC microgrids, thereby reducing their reliability and operational efficiency. Such faults can be easily recovered by using state observers [30]. However, sensor faults also cause an interruption in the update of consensus law, thereby leading to maloperating events. As a result, a key indicator needs to be designed to differentiate between hijacking attacks and sensor faults in distributed control based DC microgrids.

To address this issue, this paper proposes a distributed screening (DS) based metric for each agent. This metric is calculated using local and neighboring input current references of DC/DC converters, which remain in consensus for a particular global voltage reference under no attack. However, during an attack, distributed screening metric of attacked agent does not obey consensus theory, which becomes the basis of determining the attacked agent. Further, its performance is assisted by a sensor failure detection (FD) metric which has been designed to detect sensor faults. As a result, the proposed framework avoids confusion, and allows interoperability of all the proposed detection criterias. Finally, the performance of proposed detection metric is assessed when agents are subjected to single/multiple attacks under plug in-and-out of agents, communication delay and sensor faults under simulation and experimental conditions to validate its robustness in distributed DC microgrids. These security mechanisms can be a key asset in real applications in autonomous systems such as, electric ships and aircrafts, telecommunication centres and renewable energy based systems.

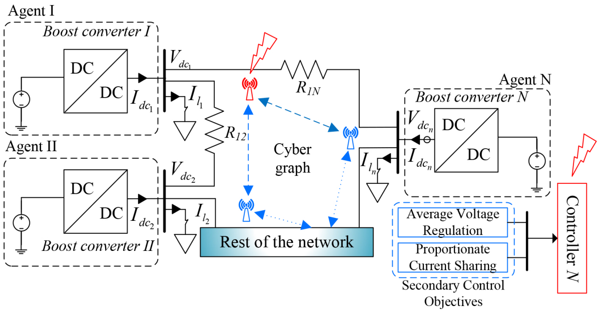


Fig. 2. Generic cyber-physical model of a DC microgrid with N agents operating to achieve average voltage regulation and proportionate current sharing: Blue arrows represent the cyber layer while black lines represent the physical circuit.

II. Conventional Distributed Control Strategy in DC Microgrids

A. Cyber-Physical Preliminaries

An autonomous DC microgrid considered in this work is shown in Fig. 2. N DC sources connected via DC/DC converters of equal power rating are interconnected to each other via tie-lines forming the physical layer of the microgrid. The DC/DC converters are operated in voltage controlled mode. Droop control philosophy ensures current sharing by imposing voltage offset error. To compensate for this offset and for line impedance mismatch, secondary controllers are deployed [4]. As shown in Fig. 2, the measurements from neighbors are transmitted between each other, and are used in achieving *consensus* to regulate average voltage and current sharing in the microgrid. In the cyber layer, an undirected graph is considered, where vertices denote the points of connections of physical sources (DC/DC converters). Each agent is represented by a node and a communication digraph by edges using an adjacency matrix $\mathbf{A} = [a_{ij}] \ \epsilon \ R^{N \times N}$. The communication weights are given by:

$$a_{ij} = \begin{cases} > 0, & \text{if } (\psi_i, \psi_j) \ \epsilon \ \mathbf{E} \\ 0, & \text{else} \end{cases}$$

where $\mathbf{E}$ is an edge connecting two nodes, with ψ_i and ψ_j being the local and neighboring node respectively. Each vertex sends and receives x_j = $[\bar{V}_{dc_j}, I_{dc_j}^{pu}]$ from its neighboring vertices to achieve the secondary control objectives highlighted in Fig. 2, where $\bar{V}_{dc_j}$ and $I_{dc_j}^{pu}$ denote the average voltage estimate and per unit output current of the neighboring agents. On the other hand, x_i = $[\bar{V}_{dc_i}, I_{dc_i}^{pu}]$ denote the local measurements in i^{th} agent. Using the cyber graph, the local input can be written as:

$$u_i = \sum_{i \in M_i} a_{ij}(x_j - x_i) \tag{1}$$

where u_i = $[u_i^V, u_i^I]$ corresponds to the elements in x_i respectively and M_i denotes the set of neighbors of i^{th} agent. 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:

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

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

To establish the highlighted objectives in Fig. 2 for DC/DC converters operating to maintain the output voltage, two voltage correction terms for i^{th} agent are calculated using:

$$\Delta V_{1_i} = H_1(s)\underbrace{(V_{dc_{ref}} - u_i^V)}_{e_i^V} \tag{3}$$

$$\Delta V_{2_i} = H_2(s)\underbrace{(I_{dc_{ref}} - u_i^I)}_{e_i^I} \tag{4}$$

where $H_1(s) = K_P^{H_1} + \frac{K_I^{H_1}}{s}$, $H_2(s) = K_P^{H_2} + \frac{K_I^{H_2}}{s}$ are PI controllers and $V_{dc_{ref}}$ and $I_{dc_{ref}}$ are the global reference voltage and current quantities of all the agents, respectively. It should be noted that $I_{dc_{ref}} = 0$ for proportionate current sharing between the agents.

Remark I: *As per the synchronization law [31], all the agents participating in distributed control will achieve consensus using* $\dot{\mathbf{x}} = -\mathbf{L}\mathbf{x}$ *for a well-spanned symmetric Laplacian matrix* $\mathbf{L}$ *such that* $\lim_{t\to\infty} x_i(t) = c$, $\forall i \epsilon N$, *where c =* [$V_{dc_{ref}}$, $I_{dc_{ref}}$]*.*

The voltage correction terms obtained in (3)-(4) are finally added to the global reference voltage $V_{dc_{ref}}$ setpoint to achieve local voltage references for i^{th} agent using:

$$V_{dc_{ref}}^i = V_{dc_{ref}} + \Delta V_{1_i} + \Delta V_{2_i}. \tag{5}$$

Using (5) as the local voltage reference for i^{th} agent, the secondary objectives highlighted in Fig. 2 is achieved. According to the distributed consensus algorithm for a well connected cyber graph in a DC microgrid, the system objectives for DC microgrids using (1)-(5) shall converge to:

$$\lim_{t\to\infty} \bar{V}_{dc_i}(t) = V_{dc_{ref}},\ \lim_{t\to\infty} u_i^I(t) = 0 \quad \forall i \ \epsilon \ N \tag{6}$$

where

$$\bar{V}_{dc_i}(t) = V_{dc_i}(t) + \int_{j\epsilon M_i} u_i^V(t) \tag{7}$$

with V_{dc_i} denoting the output voltage of i^{th} agent.

B. Modeling of Hijacking Attacks

Upon hijacking the communicated current measurement(s) in the controller, the communicated current signals received at i^{th} agent is modified to:

$$I_{dc_j}^a(t) = (1-\alpha)I_{dc_j}(t) + \alpha x_j^a \tag{8}$$

where $I_{dc_j}^a$ and x_j^a denote the final value of current measurement from the neighboring agent and a constant attack element, respectively. Moreover, α is a binary variable to represent the presence of any attack elements, with α = 1 implying that the system is attacked or 0, otherwise. As a result, the consensus theory misbehaves thereby restricting $I_{dc_j}^a(t)$ to update with further iterations. This instills arbitrary steady-state current values for each agent, which do not obey the consensus theory. On the other hand, FDIAs in the output currents of neighboring agents can be modeled as:

$$I_{dc_j}^a(t) = I_{dc_j}(t) + \alpha x_j^a. \tag{9}$$

Therefore, as opposed to (8), it is clear that (9) allow updates of the transmitted signal since the attacked signal is still dependent on a time-varying variable $I_{dc_j}(t)$. As a result, it leads to asymptotic convergence, albeit the value may be wrong.

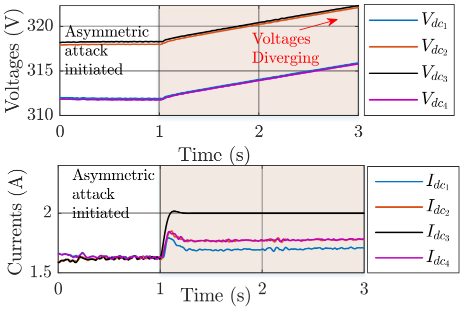


Fig. 3. Performance of cooperative agents in DC microgrid in the presence of asymmetric hijacking attack – The system objectives in (6) are violated leading to steady divergence of voltages.

The system behavior under hijacking attack is shown in Fig. 3 for a cyber-physical DC microgrid comprising of N= 4 agents, where agent III is attacked using (8) at t = 1 s. This attack leads to steady increase of voltages, which will ultimately lead to activation of protective system and a blackout of the whole microgrid. The protection measures for each converter will operate as soon as the following holds true:

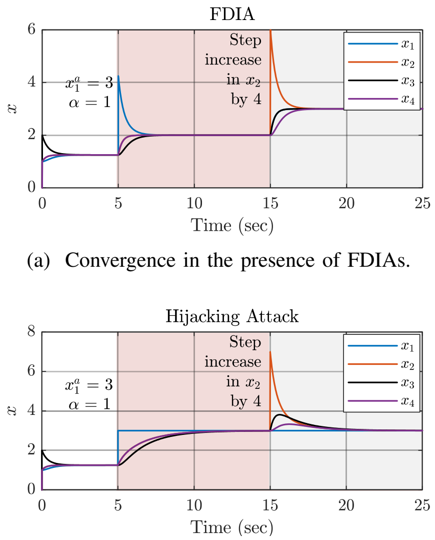
$$V_{dc_{min_i}} < V_{dc_i} < V_{dc_{max_i}} \tag{10}$$

$$I_{dc_{min_i}} < I_{dc_i} < I_{dc_{max_i}} \tag{11}$$

where $I_{dc_{min_i}}$, $I_{dc_{max_i}}$, $V_{dc_{min_i}}$ and $V_{dc_{max_i}}$ denote the minimum and maximum threshold for output current, minimum and maximum threshold for voltages of i^{th} agent. Eq. (8) can be termed as an asymmetric hijacking attack, since the data intrusion only into communicated measurements creates an asymmetrical drift of the states with respect to the Laplacian graph [31], such that $\dot{\mathbf{x}}^a + \mathbf{L}\mathbf{x}^a \neq 0$.

C. Differentiation with FDIAs

From an operational point of view, a FDI attack can be defined as an attack which adds an exogeneous input to the consensus update in (9) with every iteration. As a result, the consensus in the following iterations for (1) may update to a feasible value, if the states are operating within the bounds. For example, a FDI attack of x_1^a = 3 at t = 5 s in Fig. 4(a) causes every agent to converge to a feasible but biased value of 2. Further when an actual signal x_2 is increased by 4 at t = 15 s, the rest of the states iterate to a new value maintaining consensus theory. On the other hand, hijacking attacks for the same system impair the update rule



(a) Convergence in the presence of FDIAs.

(b) Convergence in the presence of hijacking attacks.

Fig. 4. Comparative performance evaluation of (1) under FDIAs and hijacking attacks - Hijacking attacks interrupt the iterative consensus theory; thereby resulting in an arbitrary performance.

in (1), thereby making it behave arbitatrily. This is carried out by replacing the measured signal with a constant attack signal, which then serves as a reference for other agents. Consequently, the attacked agent(s) operate incorrectly leading to an arbitrary solution. For example, an hijacking attack of x_1^a = 3 is launched at t = 5 s in Fig. 4(b), which causes the remaining states to slowly converge to the attacked value. Further for a step increase in x_2 by a value of 4 carried out at t = 15 s, the remaining units still converge to x_1^a = 3; thereby losing the iterative property. In microgrids, this could lead to several problems such as undervoltage, since such attacks prohibit dynamics of external disturbances. It should be clearly noted that the abovementioned attacks can be launched on x_i = $[\bar{V}_{dc_i}, I_{dc_i}^{pu}]$ in (1).

Remark II: *Under asymmetric hijacking attacks, the system resorts into a different operating condition as opposed to (6), which is given by:*

$$\lim_{t\to\infty} \bar{V}_{dc_i}(t) = V_{dc_{ref}}^a, \ \lim_{t\to\infty} u_i^I(t) \neq 0 \ \ \forall i \ \epsilon \ N \tag{12}$$

where $V_{dc_{ref}}^a \neq V_{dc_{ref}}$.

On the other hand, a local sensor attack in i^{th} agent is modeled using

$$I_{dc_i}^a(t) = (1-\alpha)I_{dc_i}(t) + \alpha x_i^a \tag{13}$$

in conjunction with (8) will lead to a symmetric hijacking attack on i^{th} agent.

Considering $\dot{\mathbf{x}}^a$ = $\mathbf{L}\mathbf{x}^a$, the set of eigenvalues Λ_s and Λ_a to denote the system and attack dynamics respectively, are given by:

$$\begin{cases} \Lambda_s = \{\lambda_s^1, \lambda_s^2, ..., \lambda_s^N\} \\ \Lambda_a = \{\lambda_a^1, \lambda_a^2, ..., \lambda_a^N\}. \end{cases} \tag{14}$$

Accounting marginally stable dynamics as per (6) with the eigenvalues centred at the origin, a synchronization matrix $S_m(t)$ can be defined using:

$$S_m(t) = \sum_{j=1}^{N} \sigma_{1j} x_j^a(t) \tag{15}$$

where σ_{1j} represent the element of left eigenvector corresponding to the zero eigenvalues of the Laplacian matrix $\mathbf{L}$. Further, $\sigma_i > 0$, if $i \in R$ or $\sigma_i = 0$, otherwise.

Remark III: *If $S_m(t) = 0$, symmetric hijacking attack elements are injected, which does not cause instability and obey (6).*

Using Remark III, it is sufficient to establish that $S_m(t) > 0$ will only hold true for asymmetric hijacking attacks. Another forthcoming point is since the system objectives in (6) are met, the system operator has no information of the presence of online attack elements. As the adversary wants to cause shutdown of the microgrid, these online attack elements could be increased invariably to cause activation of the protection system leading to system shutdown. Hence, detection strategies to counter both symmetric and asymmetric hijacking attacks in DC microgrids need to be developed to ensure system stability and security.

III. Proposed Detection Metrics for Hijacking Attacks and Sensor Faults

A. Distributed Screening Detection Metric for Hijacking Attacks

Using the modeled attacks in (8) and (13), the dynamic representation of the cyber attack in i^{th} agent is given by:

$$\chi_i(t) = C_i \frac{dV_{dc_i}}{dt} = [1 - D_i(t)]I_{in_i}(t) - I_{dc_i}^a(t) \tag{16}$$

where I_{in_i} and D_i denote the input current of DC/DC converter and normalized duty ratio in i^{th} agent, respectively. Denoting (16) in vector form and substituting in (7), we get:

$$\dot{\bar{\mathbf{V}}}_{dc} + \mathbf{L}\bar{\mathbf{V}}_{dc} = \mathbf{C}^{-1}(\mathbf{N}\mathbf{I}_{in} - \mathbf{I}_{dc}^a) \tag{17}$$

where $\mathbf{N}$ = $1 - \mathbf{D}$, $\mathbf{I}_{in}$, $\mathbf{D}$ and $\mathbf{I}_{dc}$ denote the diagonal matrices of I_{in_i}, D_i and I_{dc_i} for N agents, respectively. Multiplying (17) with $\mathbf{L}^T$ on the left hand side, we obtain:

$$\mathbf{L}^T(\dot{\bar{\mathbf{V}}}_{dc} + \mathbf{L}\bar{\mathbf{V}}_{dc}) = \mathbf{L}^T\mathbf{C}^{-1}\mathbf{N}\mathbf{I}_{in} - \mathbf{L}^T\mathbf{C}^{-1}\mathbf{I}_{dc}^a. \tag{18}$$

Using Remark III, (18) will be zero under symmetric attacks and non-zero under asymmetric attacks. Hence for asymmetric hijacking attacks, the secondary sublayer II output ramps up, leading to disorientation of steady-state solutions, as shown in Fig. 3. Since the attacked current measurement in case of asymmetric hijacking attack introduces a steady-state error in (4), the ramped up control output will lead to ramping up of output voltages at each bus. With steady increase in the voltages and a constant attacked current signal, output currents of the non-attacked agents will also increase for voltage dependent loads. Since the attacked current element in (8) is constant with every iteration, the attacked agent can be easily detected by following the disparity of zero gradient of output current. As per the above-mentioned detection criteria, it can be concluded that agent III is attacked in Fig. 3.

However, this detection strategy does not accord for symmetric hijacking attacks since asymptotic convergence between every agent is reached. Under steady-state conditions for (5) accounting a formidable tracking performance by the voltage controller, we get:

$$\mathbf{L}^T\Delta\mathbf{V}_1 + \mathbf{L}^T\Delta\mathbf{V}_2 + \mathbf{V}_{dc_{ref}} = \mathbf{L}^T\mathbf{V}_{dc}. \tag{19}$$

Since the system objectives are met for a symmetric attack, $\mathbf{L}^T\Delta\mathbf{V}_1 = 0$ holds true [22]. Using this equality and differentiating (19) with respect to time, we get:

$$\mathbf{L}^T\mathbf{H}_2\dot{\mathbf{e}}_a^I - \mathbf{L}^T\dot{\mathbf{V}}_{dc} = 0 \tag{20}$$

where $\mathbf{e}_a^I$ denote the vector representation of e_i^I in (4) including the attack element $\mathbf{x}^a$. For symmetric attacks, $\mathbf{L}^T\mathbf{C}^{-1}\mathbf{I}_{dc}^a = 0$. Using this equality after substituting (18) in (20), we get:

$$\mathbf{L}^T\mathbf{H}_2\dot{\mathbf{e}}_a^I - \mathbf{L}^T\mathbf{C}^{-1}\mathbf{N}\mathbf{I}_{in} = 0. \tag{21}$$

Remark IV: *Since the injected attack elements are constant in hijacking attacks, differentiation of the attacked quantities in (13) will translate into an asymmetric matrix in the first term of (21). As a result, this property will be reflected in the second term of (21), which becomes the basis of detection for hijacking attacks.*

Considering an apt tracking performance in the current controller as shown in Fig. 5, a distributed screening factor DS_i for i^{th} agent, as shown in Fig. 5, to detect hijacking attacks using Remark IV is proposed as follows:

$$\begin{aligned} DS_i(t) \quad = \quad & c_i[\sum_{j\epsilon M_i} I_{in_{ref}}^j(t) - I_{in_{ref}}^i(t)] \\ & [\sum_{j\epsilon M_i} I_{in_{ref}}^j(t) + I_{in_{ref}}^i(t)] \end{aligned} \tag{22}$$

where $I_{in_{ref}}^i$ is the normalized reference input current obtained from the outer voltage loop in i^{th} agent. Moreover, c_i is a positive scaling factor, which is used to increase/decrease the value of DS_i. As the cooperative synchronization theory by secondary sublayer II does not hold true under the presence of hijacking attacks, it can be deduced that DS_i obtained in (22) will always lead to a positive value greater than ρ_{DS_i} to notify presence of any undesired attack element in i^{th} agent. It is worth notifying that a small detection threshold of ρ_{DS_i} is used to avoid the false detection to bypass the unwanted noise in sensor measurements. To bypass the transients, a dwell time of 0.5 s is used to affirm detection using steady-state positive values. A larger value of ρ_{DS_i} affects the accuracy of detection and vice-versa. Upon detection, the attack element can be removed from the attacked agent(s) using a suppression mechanism, as reported in [32].

On the other hand, the proposed detection approach is also vulnerable to false indication of cyber attacks during sensor faults. Any sensor fault could also result in disorientation of objectives in (6), misleading to positive values of DS in multiple agents. To prevent this, an evaluation theory to detect sensor faults has been proposed in the next subsection to assist (22) in differentiating between hijacking attacks and sensor fault.

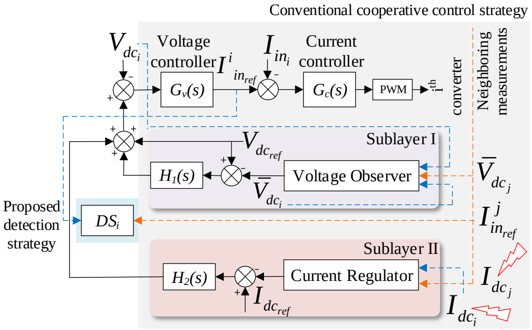


Fig. 5. Proposed distributed screening based detection controller for i^{th} agent in DC microgrids.

B. Fault Detection Metric for Sensor Faults

Typically, sensor faults in DC microgrids could arise due to physical interruption in: 1) the sensor-controller network owing to loose connections, and 2) disconnection of the regulated DC power supply into sensing circuit or a fault in the acquisition channel. This can be easily resolved by using state observers to estimate the measurement using other active sensors [29]. As the proposed detection scheme is designed to identify misbehaving agents in multi-agent based DC microgrids, it could lead to false detection of hijacking attacks during sensor faults, which exhibit a similar response. To avoid complexity in decision-making in implementing separate countermeasures for cyber attacks and sensor fault, fault detection FD^i metrics are proposed to detect the sensor faults in i^{th} agent. Since each agent consist of two sensors $\{V_{dc_i}, I_{dc_i}\}$, the corresponding fault detection metrics can be denoted by $\{FD_V^i, FD_I^i\}$. The impact on the controller response due to faults on both sensors has been desribed below:

1) Current Sensor Fault: A current sensor fault directly affects the current regulation secondary sublayer in (4). As soon as the fault occurs in a given agent, the corresponding current measurement reports zero values to the local controller as well as the communication links. Referring to (4), this symmetric change is cancelled out with respect to the Laplacian graph theory. Considering a column matrix with faulted current measurement in N^{th} agent $\mathbf{I}'_{dc}$ = $[I_{dc_1}$,I_{dc_2}, ..., $0]^T$, we extend the error quantity in (4) under steady-state conditions to:

$$\mathbf{L}^T[I_{dc_{ref}}\mathbf{1} - \mathbf{L}\mathbf{I}'_{dc}] = 0 \tag{23}$$

where $\mathbf{1}$ is an identity matrix. Hence, (23) concludes that the steady-state error created by the sensor fault is nullified owing to the symmetric information exchange in the multi-agent DC microgrid. As a result, the remaining agents share the demand to regulate average voltage estimates to $V_{dc_{ref}}$ with the current of the faulted agent being zero. Hence, the difference in the output currents between each agent can be utilized as a sufficient criteria to detect current sensor fault in i^{th} agent using:

$$FD_I^i = u_i^I = \begin{cases} > \rho_{FD^i}, & \text{if } \mathbf{I}_{dc} \neq \mathbf{I}'_{dc} \\ < \rho_{FD^i}, & \text{else} \end{cases} \tag{24}$$

where ρ_{FD^i} is a positive detection threshold used to avoid

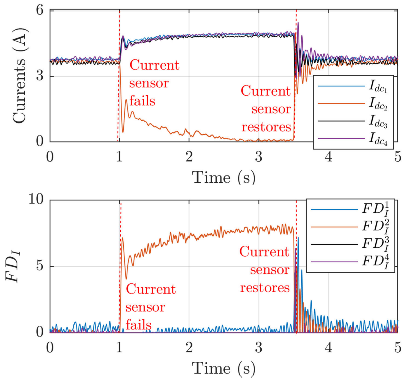


Fig. 6. Performance of the fault detection metric for current sensor faults in agent II – Positive FD_I^2 confirms current sensor fault in agent II.

false detection by bypassing the noise in current measurements. As shown in Fig. 6, when a current sensor of agent II fails at t = 1 s, FD_I^2 shoots to the positive region to confirm that current sensor has failed in agent II. Further, when the sensor is restored at t = 3.5 s, it can be seen that FD_I^2 returns back to zero. In other words, the microgrid operates with $N-1$ agents during current sensor fault, which imitates a similar dynamic attribute when a converter is plugged out. However, a distinguishing feature between both scenarios is that control and communication of the plugged out converter is lost as opposed to the case involving current sensor fault.

Remark V: *It is worth mentioning that the control input of the faulted agent in (22) should be disregarded when (24) is positive to avoid any conflicts for detection of hijacking attacks in other agents. It is intuitive that faulted sensors can't be further attacked, hence this corollary holds true.*

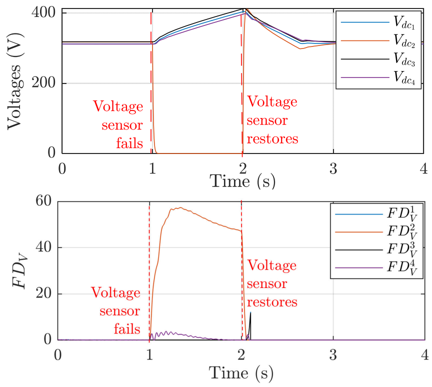


Fig. 7. Performance of the fault detection metric for voltage sensor faults in agent II – Positive FD_V^2 confirms voltage sensor fault in agent II.

2) Voltage Sensor Fault: Considering a column matrix with faulted voltage sensor in N^{th} agent $\mathbf{V}'_{dc}$ = $[V_{dc_1},V_{dc_2},....,0]^T$ and substituting in (17), the dynamics during a voltage sensor fault in each controller can be written as:

$$\mathbf{L}^T\dot{\mathbf{V}}'_{dc} = \mathbf{C}^{-1}(\mathbf{N}\mathbf{I}'_{in} - \mathbf{I}_{dc}) \tag{25}$$

where $\mathbf{I}'_{in}$ = $[I_{in_1},I_{in_2},....,I_{in_{max_N}}]^T$ with $I_{in_{max_N}}$ as the maximum input current of N^{th} agent. As soon as voltage sensor fails, the output of voltage controller shown in Fig. 5 will ramp up to reach the maximum input current. This explains the corresponding row entry for $\mathbf{I}'_{in}$ due to the faulted voltage sensor. Since a distributed voltage observer is employed, the currents from remaining agents also increase/decrease to maintain power balance. This results into a disproprotionate per-unit input current sharing. This asymmetry will be reflected in the second term of RHS of (25) and can be used as a sufficient criteria to confirm voltage sensor fault in i^{th} agent using:

$$FD_V^i = -u_i^I = \begin{cases} > \rho_{FD^i}, & \text{if } \mathbf{V}_{dc} \neq \mathbf{V}'_{dc} \\ < \rho_{FD^i}, & \text{else} \end{cases} \tag{26}$$

where FD_V^i is the failure detection metric for voltage sensor in i^{th} agent. A positive detection region has been consistently used in this paper for all the malfunctioning events in DC microgrids. Since the faulted voltage sensor of an agent induces its output current to rise to the maximum value as compared to the remaining agents, the control input u_i^I is multiplied by a factor of -1 to fetch positive values of fault detection. To test its performance, a voltage sensor fault is conducted in agent II in Fig. 7 at t = 1 s. As soon as the sensor fault occurs, the voltage reported in agent II immediately goes to zero. Using the fault detection theory in (26), it can be seen that FD_V^2 rises into the positive region. Similar to the current sensor fault scenario, the microgrid operates with $N-1$ agents during voltage sensor fault. Hence, the proposed detection criterias in (22), (24) and (26) impart precision and interoperability to detect hijacking attack and sensor faults separately. Moreover, they are simple to design which can be readily done using the existing resources in distributed control based DC microgrids. It is worth notifying that an evaluation theory to discriminate between DC line-to-line faults and cyber attacks is already studied in [33]. As a result, this provides a composite evaluation and detection model to differentiate various sorts of anomalies in the operation of DC microgrids.

IV. Simulation Results

The proposed detection theory is tested on cyber-physical DC microgrids with N= 4 agents, as shown in Fig. 2. Each agent comprises of a DC source and a DC/DC boost converter with equal power capacities. The output voltage of all buses are regulated by a global reference $V_{dc_{ref}}$ = 315 V. The robustness of the proposed distributed screening based detection theory has been tested for symmetric hijacking attacks, which goes undetected by the distributed voltage observer. Furthermore, it is tested under multiple scenarios such as plug and play of converter and communication delay to validate its performance. In addition, a case study is presented to show the performance of the failure detection metrics to differentiate between sensor fault and hijacking attack. It should be noted that each event in the abovementioned detection scenarios are separated by a certain time-gap to provide clear understanding. The simulation plant and control parameters are provided in Appendix.

Referring to Fig. 8, the reliability of the proposed detection strategy is examined when subjected to a maximum communication delay of 135 ms and 10% packet loss in the ring-based cyber network. Since delay affects the performance

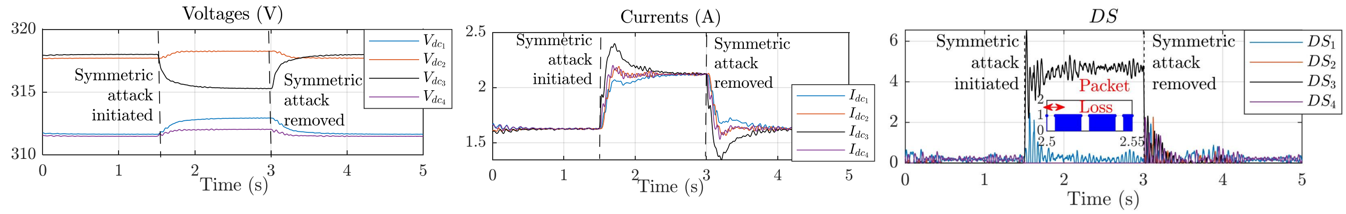


Fig. 8. Performance of cooperative agents in DC microgrids in the presence of maximum communication delay of 135 ms and 10% packet loss – Positive DS_3 indicates the presence of a symmetric attack in agent III.

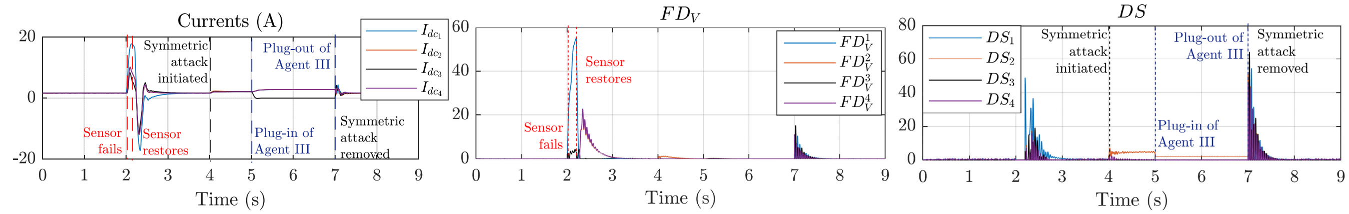


Fig. 9. Performance of cooperative agents in DC microgrids during voltage sensor fault and plug-and-play of agent III – Positive DS_3 for t = [4, 5] s indicates the presence of a symmetric attack in agent III. Positive FD_V^1 for t = [2, 2.15] s indicates a voltage sensor fault in agent I, thereby ensuring accurate detection of the malfunctioning events.

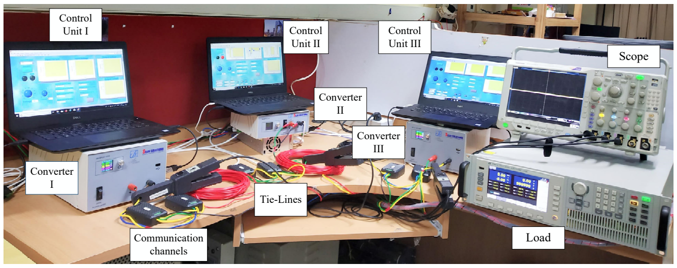


Fig. 10. Experimental setup comprising of three commercial DC/DC converters connected in parallel to form a ring DC network.

of the distributed controller, the system operation is always carried out within a borderline delay such that the convergence is guaranteed using consensus theory [3]. Within the said borderline delay range, the rate of convergence is directly proportional to the communication delay. To test this theory, a symmetric hijacking attack is carried out on agent III at t = 1.5 s in Fig. 8. It can be seen that even with a slower rate of convergence owing to the communication delay, a positive value for DS_3 confirms the presence of attack in agent III. Hence, it can be concluded that the performance of proposed detection scheme will remain unaffected by communication delay as long as the convergence is reached to obey the system objectives in (6).

In Fig. 9, the performance of the proposed detection scheme is evaluated during a converter outage and restoration and voltage sensor fault. When the voltage sensor in agent I fails at t = 2 s, FD_V^1 rises into the positive region thereby validating (26) and goes to zero upon restoration of the sensor at t = 2.15 s. It can be seen that DS following some initial transient does not indicate positive values during a sensor fault. Further when agent III is plugged out at t = 4 s, the remaining active agents share the load equally in terms of both input and output currents. However, when a symmetric attack of x_1^a = 2 A is injected into agent I, even though output currents are shared proportionately, DS_1 rises into the positive region thereby ensuring presence of attack elements in agent I. As already mentioned in Section III, the communication and control is lost for agent III, which restricts the calculation of DS_i only for active agents. This establishes that no conflict is encountered while detecting sensor fault and hijacking attacks using the proposed detection metrics in DC microgrids.

V. Experimental Results

The proposed detection strategy has been experimentally validated in a DC microgrid with N = 3 agents, as shown in Fig. 10. A single line diagram of the experimental setup is shown in Fig. 11. To demonstrate the simplicity in design of the proposed detection strategy, the experimental prototype is carried out with three commercial DC/DC boost converters [34] tied in parallel and form a physical ring-bus network comprising of a programmable load at one of the buses. The reference voltage for each converter can be varied in their respective control units, as shown in Fig. 10. Each analog measurement from each converter is communicated to their neighboring control units using USB accompanying the *Mod-*

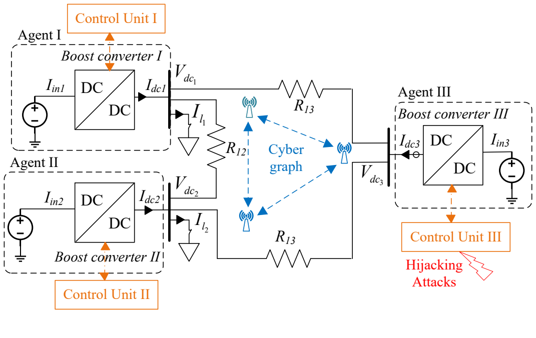
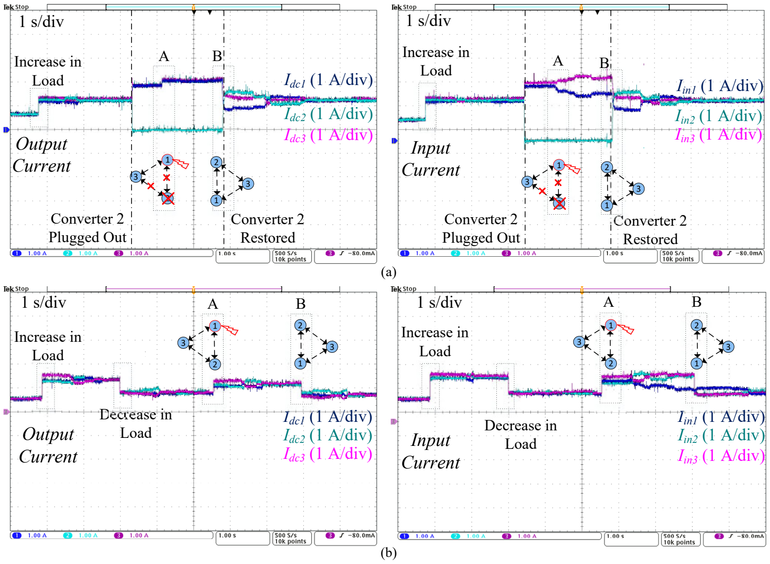


Fig. 11. Single-line diagram of Fig. 10.



(a)

(b)

Fig. 12. Experimental validation of the proposed DS based detection theory with input and output currents : (a) Symmetric hijacking attack on agent I during plug in-and-out of agent II, and (b) Symmetric hijacking attack on agent I under a maximum communication delay of 80 ms. Positive DS for the attacked agents [calculated using (22)] ensures the presence of attack element in the corresponding agents from A-B.

bus protocol to execute undirected distributed communication. Using the local and neighboring measurements, the secondary sublayer shown in Fig. 5 is modeled in the LabVIEW platform to vary the voltage references for each agent to meet the control objectives in (6) accordingly. It is worth notifying that since the commercial DC/DC converters did not have an acquisition channel, the experimental results have been shown in terms of measurable quantities, which provides a basic understanding of the proposed discordant theory. The value of DS can be calculated using (22) in waveforms of input currents with c = 1.2. In the following results, event A depicts the instant where the false data is injected to initiate the attack and event B depicts the instant where the attack is removed. The experimental testbed parameters are provided in Appendix.

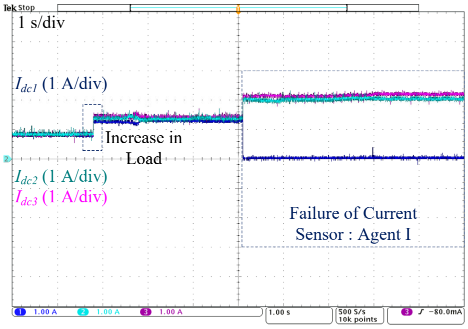


Fig. 13. Experimental validation of the proposed FD_I metric to detect current sensor fault in agent I : Positive FD_I^1 [calculated using (24)] ensures the current sensor fault in agent I.

In Fig. 12(a), the performance of the proposed detection scheme is evaluated during a converter outage and restoration. As soon as agent II is plugged out, the remaining active agents share the load equally for both input and output currents. However, when a symmetric hijacking attack of x_1^a = 0.4 A is injected into agent I, the input currents of active agents goes into disproportionate sharing despite the output currents are shared proportionately. Using (22), DS_2 goes positive to denote the presence of symmetric attack elements in agent I. This demonstrates that the proposed detection scheme performs normally even under plug in-and-out of agents in DC microgrids. Further in Fig. 12(b), when the output current sensor in agent I is attacked with I_{dc}^a = 0.6 A during event A under a maximum communication delay of 80 ms, the input currents also follow a similar response as in Fig. 12(a). It should be noted that the rise in DS_1 into the positive region takes some time, owing to the communication delay. Hence, it can be concluded that the attack detection philosophy performs normally under experimental conditions even in the presence of communication delay.

In Fig. 13, the performance of the fault detection metric for current sensor fault in agent I is examined. The fault is emulated experimentally by replacing the measurement from the acquisition channel with zero. As soon as the current sensor fails, it can be seen that FD_I^1 [calculated using (24)] rises to a positive value immediately, thereby validating the proposed fault detection theory.

VI. Conclusion

A novel distributed screening based detection strategy is proposed for both symmetric and asymmetric hijacking attacks. The system response for both hijacking attacks has been demonstrated with a detailed explanation and theoretical validation using the consensus theory in DC microgrids. Since sensor faults also cause a similar arbitrary response to that of hijacking attacks, an evaluation theory is proposed to assist the proposed detection strategy to differentiate between hijacking attack and sensor fault. This evaluation theory is quantified using a fault detection metric for both voltage and current sensors by conducting a detailed analysis. As a result, it facilitates interoperability of detection and mitigation of both events and avoid confusion. Another contribution is simplicity of the detection scheme. Finally, the proposed detection strategy has been validated experimentally under plug-and-play of converters and communication delay to show the robustness for any commercially available voltage controlled DC/DC converters. This study can be an asset in many real applications such as, telecommuniation centeres, electric ships and aircrafts, renewable energy based systems, etc.

Appendix

The simulated system consists of four sources rated equally for 5 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} = 1.8 Ω, R_{14} = 1.3 Ω, R_{23} = 2.3 Ω, R_{43} = 2.1, L_{se_i}= 3 mH, C_{dc_i}= 250 μF, $I_{dc_{max}}$ = 16 A, $I_{dc_{min}}$ = 0 A, $V_{dc_{min}}$ = 270 V, $V_{dc_{max}}$ = 385 V

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, $K_I^{H_2}$ = 0.32, G_{VP} = 2.8, G_{VI} = 12.8, G_{CP} = 0.56, G_{CI} = 21.8, V_{in} = 270 V, c = 3.24, ρ_{FD^i} = 1.5, ρ_{DS_i} = 0.75.

Further, the experimental setup consists of three sources with the converters rated equally for 1 kW. The controller gains are consistent for each agent.

Plant: R_{12} = 0.6 Ω, R_{13} = 0.8 Ω, R_{23} = 0.75 Ω, L_{se_i}= 2.5 mH, C_{dc_i}= 100 μF, $I_{dc_{max}}$ = 20 A, $I_{dc_{min}}$ = 0 A, $V_{dc_{min}}$ = 44 V, $V_{dc_{max}}$ = 52 V

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, c = 1.2, ρ_{FD^i} = 0.3, ρ_{DS_i} = 0.25.

References

[1] T Dragicevic, X Lu, JC Vasquez, and JM Guerrero,”DC Microgrids–Part I: A Review of Control Strategies and Stabilization Techniques”, *IEEE Tran. Power Electr.*, vol. 31, no. 7, pp. 4876-4891, 2016.

[2] S Sahoo and S. Mishra, ”A Distributed Finite-Time Secondary Average Voltage Regulation and Current Sharing Controller for DC Microgrids”, *IEEE Trans. on Smart Grid*, vol. 10, no. 1, pp. 282-292, 2017.

[3] S Sahoo, S Mishra, S Jha, B Singh, ”A Cooperative Adaptive Droop Based Energy Management & Optimal Voltage Regulation Scheme for DC Microgrids”, *IEEE Trans. on Ind. Electr.*, pp. 1-1, 2019.

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

[5] M. S. Rahman, M. A. Mahmud, A. M. T. Oo, and H. R. Pota, ”Multiagent approach for enhancing security of protection schemes in cyberphysical energy systems,” *IEEE Trans. Ind. Informat.*, vol. 13, no. 2, pp. 436-447, Apr. 2017.

[6] M. Cheminod, L. Durante, and A. Valenzano, ”Review of security issues in industrial networks,” *IEEE Trans. Ind. Informat.*, vol. 9, no. 1, pp. 277-293, 2013.

[7] 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.

[8] N. Liu, J. Chen, L. Zhu, J. Zhang, and Y. He, ”A key management scheme for secure communications of advanced metering infrastructure in smart grid,” *IEEE Trans. Ind. Electron.*, vol. 60, no. 10, pp. 4746-4756, Oct. 2013.

[9] W. Zeng and M. Y. Chow, ”Optimal tradeoff between performance and security in networked control systems based on coevolutionary algorithms,” *IEEE Trans. Ind. Electron.*, vol. 59, no. 7, pp. 3016-3025, Jul. 2012.

[10] JJ Jacard, S Nepal, ”A survey of emerging threats in cybersecurity”, *Journ. of Comp. and Syst. Sciences*, vol. 80, pp. 973-993, 2014.

[11] DHS S&T, *Roadmap for cybersecurity research*, Jan. 2009.

[12] Theregister.co.uk, ”Buffer overflow flaw in British Airways in-flight entertainment systems will affect other airlines, but why try it in the air?” [Online], Available: https://www.theregister.co.uk/2019/03/08/thales_topseries_vuln/

[13] Annual report 2011, The Repository for Industrial Security Incidents (RISI), Online: http://www.securityincidents.net/index.php/products/indepth/risi_annual_report/

[14] A. O. de S, L. F. R. d. C. Carmo, and R. C. S. Machado, ”Covert attacks in cyber-physical control systems,” *IEEE Trans. Ind. Inform.*, vol. 13, no. 4, pp. 1641-1651, 2017.

[15] H Keshtkar, et al, ”Proposing an improved optimal LQR controller for frequency regulation of a smart microgrid in case of cyber intrusions,” *2014 IEEE 27th Canadian Conf. on Electr. and Comp. Engg. (CCECE)*, pp. 1-6, 2014.

[16] W. Zeng, Y. Zhang, and M. Y. Chow, ”Resilient distributed energy management subject to unexpected misbehaving generation units,” *IEEE Trans. Ind. Informat.*, vol. 13, no. 1, pp. 208-216, 2015.

[17] 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.

[18] M Rekik, et al, ”A Cyber-Physical Threat Analysis for Microgrids,” *2018 15th Intl. Multi-Conference on Systems, Signals & Devices (SSD)*, 2018.

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

[20] MM Rana, L Li, and SW Su, ”Cyber attack protection and control in microgrids using channel code and semidefinite programming,” *Power and Energy Society General Meeting (PESGM)*, 2016. 6731–6741, 2017.

[21] 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.

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

[23] G Dan, and H Sandberg, ”Stealth attacks and protection schemes for state estimators in power systems” *2010 IEEE International Conf. on Smart Grid Comm.* pp. 214-219, 2010.

[24] G. D. Torre and T. Yucelen, ”Adaptive architectures for resilient control of networked multiagent systems in the presence of misbehaving agents,” *Int. J. Control*, vol. 91, no. 3, pp. 495-507, 2018.

[25] 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.

[26] 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.

[27] H. Park and S. Hutchinson, ”Robust rendezvous for multi-robot system with random node failures: an optimization approach,” *Autonomous Robots*, pp. 1-12, 2018.

[28] A Mitra, et al, ”Resilient distributed state estimation with mobile agents: overcoming Byzantine adversaries, communication losses, and intermittent measurements,” *Autonomous Robots*, vol. 43, no. 3, pp. 743-768, 2019.

[29] HM Khalid, JCH Peng, ”A Bayesian Algorithm to Enhance the Resilience of WAMS Applications Against Cyber Attacks”, *IEEE Trans. Smart Grid*, vol. 7, no. 4, pp. 2026-2037, 2016.

[30] CP Tan, and C Edwards, ”Sliding mode observers for robust detection and reconstruction of actuator and sensor faults,” *Intl. Journ. Robust and Nonlin Control*, vol. 13, no. 5, pp. 443-463, 2003.

[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] F. C. Schweppe and D. B. Rom, ”Power system static-state estimation, part III,” *IEEE Trans. Power App. Syst.*, vol. PAS-89, no. 1, pp. 130-135, Jan. 1970.

[33] S Sahoo, JCH Peng, A Devakumar, S Mishra, T Dragicevic, ”On Detection of False Data in Cooperative DC Microgrids?A Discordant Element Approach”, *IEEE Trans. Ind. Electron.*, 2019.

[34] Silov Solutions Pvt. Ltd., 2018. [Online] Available: http://www.silovsolutions.com/