Multi-Layer Resilience Paradigm Against Cyber Attacks in DC Microgrids

Sahoo, Subham Swaroop; Dragicevic, Tomislav; Blaabjerg, Frede

Published in:
IEEE Transactions on Power Electronics

Link to article, DOI:
10.1109/TPEL.2020.3014258

Publication date:
2020

Document Version
Peer reviewed version

Citation (APA):
Sahoo, S. S., Dragicevic, T., & Blaabjerg, F. (2020). Multi-Layer Resilience Paradigm Against Cyber Attacks in DC Microgrids. *IEEE Transactions on Power Electronics*, *36*(3), 2522 - 2532.
https://doi.org/10.1109/TPEL.2020.3014258

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TPEL.2020.3014258, IEEE Transactions on Power Electronics

Multi-Layer Resilience Paradigm Against Cyber Attacks in DC Microgrids

Subham Sahoo, *Member, IEEE*, Tomislav Dragičević, *Senior Member, IEEE* and Frede Blaabjerg, *Fellow, IEEE*

***Abstract*—Recent advancements in DC microgrids are largely based on distributed control strategies to enhance their reliability. However, due to numerous vulnerabilities in the communication layer, they are susceptible to cyber attacks. Hijacked cyber link(s) could affect the microgrid system reliability and operation in many ways. Therefore, the accuracy in detection of the compromised link(s) becomes very critical due to the dynamic relationship between the cyber-physical entities in DC microgrids. One of the most prominent attacks on cyber layer is referred to as the man-in-the-middle (MITM) attack. This type of attack involves infiltrating the information between two communication nodes by a third-party. This paper proposes a multi-layer resilient controller to detect and mitigate MITM attacks immediately for ensuring the security of DC microgrids. Firstly, the modeling of MITM attacks based on (a) cooperative response, and (b) degree of coordination of attack element(s) is discussed in detail. Further, a diverging factor (DF) based detection law is proposed to locate the compromised cyber link(s) and to identify the malicious signals in voltage and current counterparts. A multi-layer based event-driven strategy is then used to remove these signals by introducing multiple mitigation layers. Based on the authentication signal for each neighboring agent `True` or `False`, the data flow between the multi-layer cyber network takes place to guarantee resilience against MITM attacks. Lastly, the proposed resilient mechanism in the presence of MITM attack is theoretically verified and validated using simulations and experiments.**

***Index Terms*—DC microgrid, man-in-the-middle attacks, distributed control, cyber-physical systems, resilient controller.**

I. Introduction

THE rapid development of DC microgrids has undergone a paradigm shift from centralized to distributed, driven by advances in cooperative control strategies that yield improved scalability, reliability and resiliency to a single point of failure [1]-[2]. Apart from that, distributed control also offers performance assets, such as robustness to delay and multiple link failure, as well as smaller communication overheads [3]-[5]. The enhanced flexibility in coordination among sources in DC microgrids can largely be attributed to the robustness of the distributed cyber layer, where factors such as bandwidth and connectivity graph affect the dynamic performance of the system. However, distributed control still bears large cyber-security concern due to omnipresence of communication links [6]. As microgrids are key components of many mission critical applications such as military bases, hospitals and industrial plants [7], it is crucial to ensure their security against such adversial attacks [8]-[10].

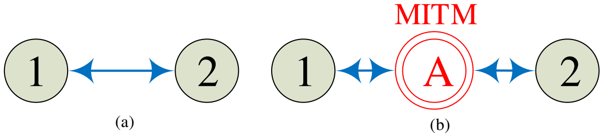

Fig. 1. Communication between agents 1 and 2 - (a) Uncompromised and, (b) with man-in-the-middle (MITM) attack (highlighted as A) to modify the content of information received and transmitted by both agents.

One of the key objectives to achieve consensus among sources in networked microgrids is to align on the control quantity of interest [11]. However, the information exchange among these sources can potentially be tampered with maligned data packets by a third-party agent intending to steer the microgrid towards inconsistent performance. Such attacks are commonly termed as the man-in-the-middle (MITM) attacks [12]-[13]. A simple example of this attack is shown in Fig. 1(b), where the attacker A becomes the proxy for communication between agents 1 and 2. As opposed to secure communication established between both nodes in Fig. 1(a), the attacker can either intercept only the incoming information or malign both incoming and outgoing information between the nodes. In [14], automation models of the cyber-physical layer subject to MITM attacks in the sensor and/or communication channels have been proposed to provide detailed insights on interactions between physical agents. However, verification of the security module is still not identified in [14] to detect and prevent the damage caused by cyber attacks. Moreover, accuracy in selectively detecting the compromised cyber link in distributed control systems remains another critical aspect, which needs to be carefully examined before any mitigating action. Hence, while accuracy in detection and mitigation of MITM attacks in a timely manner in distributed DC microgrids is a topic of extreme practical interest, how to effectively realize it is still an open research question. Additionally in power electronics based systems, the mitigating action needs to be fast, otherwise the network can become unstable or even lead to shutdown.

Few attack mitigation techniques in microgrids have been recently proposed. In [15], O. Beg et. al. have proposed an attack impact quantification technique and suppressed

This work was supported by THE VELUX FOUNDATIONS under the VILLUM Investigator Grant – REPEPS (Award Ref. No.: 00016591).

S. Sahoo and F. Blaabjerg are with the Department of Energy Technology, Aalborg University, Aalborg East, 9220, Denmark (e-mail: sssa@et.aau.dk and fbl@et.aau.dk) *(Corresponding Author: Subham Sahoo)*

T. Dragičević is with the Center of Electric Power and Energy, Technical University of Denmark, 2800 Kgs. Lyngby, Denmark (e-mail: tomdr@elektro.dtu.dk)

This paper has supplementary downloadable materials available at http://ieeexplore.ieee.org, provided by the authors. This includes one multimedia mp4 format movie clip, which shows the performance of the proposed multi-layer resilient controller against cyber attacks with a description file for further elaboration.

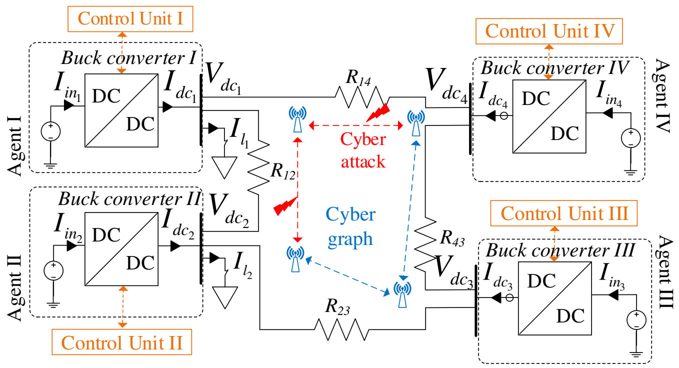

Fig. 2. Generic cyber-physical model of DC microgrid with N = 4 agents: Blue arrows represent the cyber layer and black lines represent the physical circuit. The red bolts indicate the attacked cyber link(s) with a man-in-the-middle (MITM) attack.

the impact of attack element using a deterministic number. Another well-defined mitigation approach is to employ an observer for each unit to operate with the estimated states using the pre-attack points upon detection of attack [16]. Even though these approaches are quite efficient, they have model-intensive requirements and their performance is thus highly prone to model uncertainities. Further, an upper bound based mitigation condition is also proposed in [17] based on the total number of compromised units, termed as F-total, or the local compromised agents in the neighborhood of each unit, termed as F-local. Although it counteracts against the attacks on sensors and communication links, it might affect the cyber graph connectivity by unneccesarily abandoning neighbor's information during a load change even when there is no attack. As a result, this necessitates a new self-healing mitigation strategy, which can offer system recovery without losing the cyber network connectivity vis-a-vis uncompromised system performance.

To address these issues, this paper proposes for the first time a multi-layer based event-driven control strategy for DC microgrids, which is resilient against MITM attacks. The presence of attack elements in attacked cyber link is identified using a diverging factor DF_i^j based detection law. Positive values of this detection metric suggests the presence of attack element in the cyber link directed from $j^{th} \rightarrow i^{th}$ agent. As soon as the proposed detection metric rises beyond a very small threshold, an *event* is generated to activate the attack mitigation layer. Prior to generation of these *events*, authentication signatures (`True`/`False`) are also created to signal the credibility of the information received from cyber links. As long as these events are activated in the attacked cyber link, an event-triggered signal is constructed using *trusted* control input error signals (with authentication signal labeled as `True`) in the outbound agent. This formulates the first layer of resilience against MITM attacks. However, it may also happen that all the control input error signals in the neighboring agent are compromised in a given outbound agent, which would then overcome the first layer of resilience. This serves as a motivation to formulate more defense layers in the form of a multi-layer resilience paradigm, which only transmits *trusted* control input error signals from inbound agents or neighbors/associates of inbound agents to construct the event-triggered signal.

The signal reconstruction is done by using the proposed detection criterion as a triggering mechanism to operate within pre-specified thresholds. By doing so, it is ensured that the system continues to operate normally during both steady-state and transient conditions. Finally, different avenues of system operation are simulated and later validated under experimental conditions to establish that the system could operate with $N-1$ event-driven resilient signals under worse case attack scenarios.

The rest of the paper is organized as follows. Section II depicts a brief overview of the cyber-physical architecture of DC microgrids along with a basic overhaul of distributed secondary control objectives and definition alongwith different variants of MITM attacks. Moreover, the impact of disabled cyber link on distributed control convergence is studied to clearly formulate the problem statement. Next, a comprehensive resilience framework alongwith signal reconstruction via triggering criterion for MITM attacks is provided in Section III. Simulations along with experimental validation are presented in Section IV and V, respectively. Finally, Section VI provides the concluding remarks and future scope of work.

II. Preliminaries of MITM Attacks in Cooperative DC Microgrids

A. Preliminaries of Conventional Cooperative Control in DC Microgrids

An exemplary autonomous DC microgrid considered in this work is shown in Fig. 2. N = 4 DC sources connected via DC/DC buck converters of equal power rating are interconnected to each other via tie-lines, thereby forming the physical layer of the microgrid. Each converter is operated in voltage controlled mode. Cooperative secondary controllers are employed to improve the coordination between the sources and their performance [18]. These controllers are enabled by a distributed communication layer, which shares information only between the neighboring units. Each unit, represented as an *agent* in the cyber layer, sends and receives $x_j = \{\bar{V}_{dc_j}, I^{pu}_{dc_j}\}$ from the neighboring agent(s) to achieve secondary control objectives namely, average voltage regulation and proportionate current sharing. Here, $\bar{V}_{dc_j}$ and $I^{pu}_{dc_j}$ denote the average voltage estimate and per unit output current of the neighboring agents.

Each agent in Fig. 2 represented via a node, and a communication digraph via edges constitute an adjacency matrix $\mathbf{A} = [a_{ij}] \in R^{N\times N}$, where the communication weights are given by: $a_{ij} = 1$, if $(\psi_i, \psi_j) \in \mathbf{E}$, where $\mathbf{E} \subset N \times N$ is a set of all edges connecting two nodes, with ψ_i and ψ_j being the local and neighboring node, respectively. Otherwise, $a_{ij} = 0$. $M_i = \{j|(\psi_i, \psi_j) \in \mathbf{E}\}$ denotes the set of all neighbors of i^{th} agent. Further, the in-degree matrix $\mathbf{Z}_{in}$ = diag$\{z_{in}\}$ is a diagonal matrix with its elements given by $z_{in} = \sum_{i\in M_i} a_{ij}$. Further, the Laplacian matrix $\mathbf{L}$ is defined as $\mathbf{L} = \mathbf{Z}_{in} - \mathbf{A}$.

Using the preliminaries of the communication graph, the local control input of the cooperative secondary controller can be written as:

$$u_i(t) = \xi \sum_{j \epsilon M_i} \underbrace{a_{ij}(x_j(t) - x_i(t))}_{e_{ij}(t)} \tag{1}$$

where $u_i = \{u_i^V, u_i^I\}$, $e_{ij} = \{e_{ij}^V, e_{ij}^I\}$ respectively as per the elements in x, ξ is the convergence variable.

Remark I: *As per the cooperative synchronization law [19], all the agents participating in distributed control will achieve consensus using* $\dot{\mathbf{x}} = -\mathbf{L}\mathbf{x}$ *with* $\mathbf{L}$ *having at least one spanning tree such that* $\lim_{t\to\infty} x_i(t) = c$, $\forall\ i \in N$, *where* c *is the steady-state reference and* N *is the number of agents.*

Using (1), the control inputs to achieve average voltage regulation and proportionate current sharing can be obtained respectively by using the following voltage correction terms for the i^{th} agent:

$$\Delta V_{1_i} = H_1(s)(V_{dc_{ref}} - \bar{V}_{dc_i}) \tag{2}$$

$$\Delta V_{2_i} = -H_2(s)u_i^I \tag{3}$$

where $\bar{V}_{dc_i} = V_{dc_i} + \int_0^\tau \sum_{i\in M_i}(e_{ij}^V d\tau)$ with V_{dc_i} denoting the measured output voltage of i^{th} agent. Further, $H_1(s)$ and $H_2(s)$ are PI controllers. Moreover, $V_{dc_{ref}}$ is the global reference voltage for all the agents. The correction terms obtained in (2)-(3) are finally added to the global reference voltage to achieve local voltage references for i^{th} agent using:

$$V_{dc_{ref}}^i = V_{dc_{ref}} + \Delta V_{1_i} + \Delta V_{2_i}. \tag{4}$$

Using (4) as the local voltage reference for i^{th} agent, the abovementioned secondary control objectives are met.

Using the distributed consensus algorithm for a sparse cyber network (with at least one spanning tree) in a DC microgrid, the system objectives for DC microgrids using (1)-(4) shall converge to:

$$\left.\begin{array}{l} \lim\limits_{t\to\infty} \bar{V}_{dc_i}(t) = V_{dc_{ref}} \\ \lim\limits_{t\to\infty} u_i^I(t) = 0 \end{array}\right\} \quad \forall i \ \in \ N \tag{5}$$

B. Modeling of MITM Attacks in DC Microgrids

As shown in Fig. 2, cyber attackers may inject false data into the communication links etc. to disrupt the system objectives in (5). These attacks can be conducted using various ways of intrusion into the cyber links categorizing them into aspects, such as degree of coordination and the dynamic response of the system.

1) Degree of Coordination:

- `Degree 1` Attack: These attacks can be identified as the least sophisticated MITM attacks. They disregard both the system objectives in (5). These attacks can be modeled using:

$$\dot{\mathbf{x}}(t) = -\mathbf{L}\mathbf{x}(t) + \mathbf{A}\mathbf{x}_{attack} \tag{6}$$

where $\mathbf{x}_{attack}$ denotes a column matrix of the attacked information for voltages and currents. Any non-zero value in $\mathbf{x}_{attack}$ denote the attack element. It should be noted that $\mathbf{x}_{attack}$ can be designed by the attacker as either a steady or a time-varying quantity. Using (6), it is sufficient to conclude that $\dot{\mathbf{x}}(t) \neq 0$ for `Degree 1` attacks since $\mathbf{A}\mathbf{x}_{attack} \neq 0$. This causes the secondary layer output in (2)-(3) to ramp up/down of voltages, ultimately leading to activation of the protection system. The protection measures of each converter will start operating as soon as the following condition holds true:

$$\mathbf{V}_{dc_{min}} < \mathbf{V}_{dc} < \mathbf{V}_{dc_{max}} \tag{7}$$

$$\mathbf{I}_{dc_{min}} < \mathbf{I}_{dc} < \mathbf{I}_{dc_{max}} \tag{8}$$

where $\mathbf{I}_{dc_{min}}$, $\mathbf{I}_{dc_{max}}$, $\mathbf{V}_{dc_{min}}$ and $\mathbf{V}_{dc_{max}}$ denote the vector representation of minimum and maximum threshold for output current, minimum and maximum threshold for output voltages.

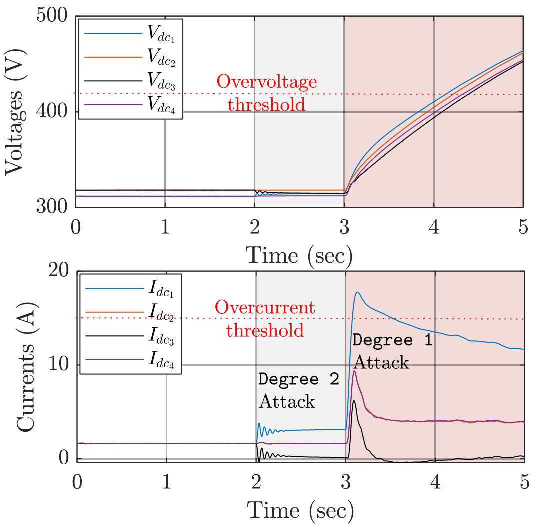

Fig. 3. `Degree 2` MITM attack on current measurements transmitted from unit II → III and II → I simultaneously at t = 2 sec – The system response is steady and stable with the attack element present only in the cyber link to the outbound agents sharing the currents disproportionately. `Degree 1` MITM attack on the same link at t = 4 s – the voltages ramp up quickly beyond the overvoltage threshold.

- `Degree 2` Attack: These attacks can be identified as the most sophisticated MITM attacks and can be modeled using:

$$\dot{\mathbf{x}}(t) = -\mathbf{L}\mathbf{x}(t) + \mathbf{W}\mathbf{x}_{attack} \tag{9}$$

Further, $\mathbf{W} = [w_{ij}]$ denotes the `Degree 2` cyber attack matrix with its elements given by:

$$|w_{ij}| = \begin{cases} 1, & \textbf{if } j \in M_i, j \neq i \\ 0, & \textbf{if } j = i \\ 0, & \textbf{else} \end{cases} \tag{10}$$

such that $\sum_{j\in M_i} w_{ij} = 0$. Using (10), `Degree 2` MITM attack introduces zero dynamics in $\mathbf{W}\mathbf{x}_{attack}$ in (9) ultimately leading to $\dot{\mathbf{x}} = 0$ with a sparse cyber network. To prove this, we consider the set of eigenvalues Λ_s and Λ_a to denote the system and attack dynamics respectively as:

$$\begin{cases} \Lambda_s = \{\lambda_s^1, \lambda_s^2, ..., \lambda_s^N\} \\ \Lambda_a = \{\lambda_a^1, \lambda_a^2, ..., \lambda_a^N\}. \end{cases} \tag{11}$$

Accounting marginally stable dynamics as per (5) with the eigenvalues centred at the origin, a synchronization matrix $S(t)$ can be defined using:

$$S(t) = \sum_{j=1}^{N} \sigma_{1j} x_j^a(t) \tag{12}$$

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

Remark II: *If $S(t)$ = 0,* Degree 2 *MITM attack will always lead to a feasible solution.*

Using Remark II, $S(t) > 0$ conversely holds true for Degree 1 MITM attacks. It is worth notifying that Degree 2 MITM attacks are different from stealth attacks [8]-[10] in a way that only one of the mentioned objectives in (6) hold true for the former. To demonstrate the level of coordination of MITM attacks, a case study is carried out for a DC microgrid (See Fig. 3) with N = 4 agents in Fig. 3, where a Degree 2 MITM attack is carried out on the outbound current measurements from agent 2 to 1 and 3 simultaneously at t = 2 s. As soon as Degree 2 attack is conducted, the attacked output currents of the outbound agents are being shared disproportionately by equal numbers. However, the average voltage of each converter is still being regulated to the global voltage reference, which satisfies (6) partially. On the other hand, when Degree 1 attack is launched at t = 4 s, the output currents increase invariably with the voltages ramping up. As the voltages reach close to the overvoltage threshold (highlighted in Fig. 3), they could potentially lead to the shutdown of the system. As a result, a convenient detection scheme needs to be designed for such attacks, which identifies the attacked cyber link with the highest accuracy.

2) Dynamic Response: rblueIt is worth notifying that $\texttt{attack}_{ij}$ is a binary state with the value 1 suggesting the presence of an attack in the cyber link directed from j^{th} to i^{th} agent or 0, otherwise. Based on the dynamic response of the system prior to the injection of cyber attack, the modeling of MITM attacks can be characterized into two categories:

- Faulty attack: A faulty MITM attack can be defined as an attack, which adds an exogeneous input to the consensus update in (6) with every iteration. As a result, the consensus in the following iterations for $\dot{\mathbf{x}} = -\mathbf{L}\mathbf{x}$ may update to a feasible value, if the participating states in $\mathbf{x}$ are operating within the bounds. This attack can be modeled using:

$$u_i^a(t) = u_i(t) + \texttt{attack}_{ij} x_{attack}^i \tag{13}$$

- Hijacking attack: An hijacking MITM attack is carried out by replacing the existing measurement with the attacked signal, which then serves as a reference for other agents. It basically impairs the update rule of the consensus theory, thereby making it behave arbitrarily. This attack can be modeled using:

$$u_i^a(t) = (1 - \texttt{attack}_{ij}) u_i(t) + \texttt{attack}_{ij} x_{attack}^i \tag{14}$$

More details on the dynamic attributes of faulty and hijacking attacks in DC microgrids can be referred from [9].

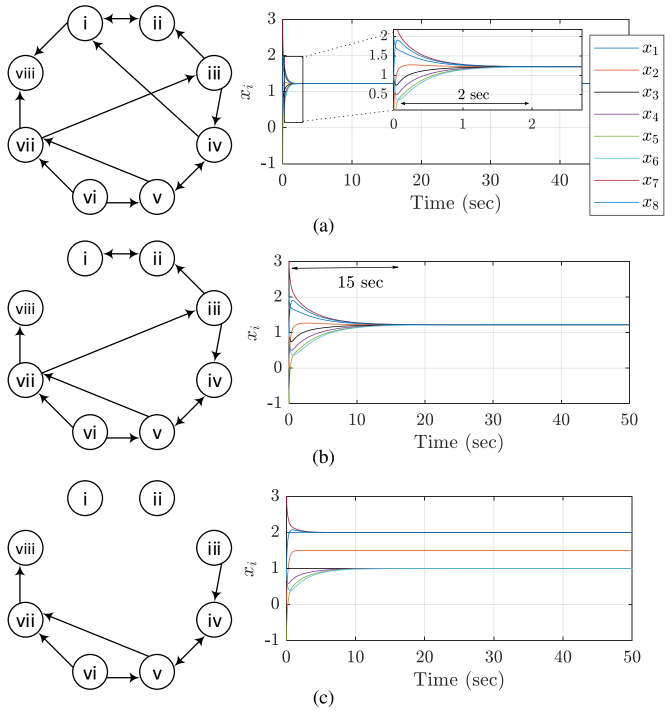

Fig. 4. Impact on convergence for (1) with (a) fully distributed network $\mathbb{G}$ - no attack leading to faster convergence within 2 sec, (b) partially distributed - disabled cyber link due to multiple MITM attacks leading to delayed convergence upto 15 sec, (c) divergent solutions for the worst case MITM attack.

C. Impact on Convergence due to MITM Attacks

Consider a set of N = 8 agents in Fig. 4(a) interconnected by a directed graph $\mathbb{G}$ to implement a distributed algorithm in (1). These agents tend to reach a steady-state solution, $\frac{1}{N}\sum_{i \in N} x_i(0) = \mathbf{1}^T \frac{\mathbf{X}(0)}{N}$, as long as the cyber graph has at least one spanning tree. However, the rate of convergence varies as per the connectivity of cyber graph. This can clearly be seen in Fig. 4(a), where the system states in (1) converge to the average value in 2 sec for a given value of ξ. The steady-state value can alternatively be termed as an agreement subspace $\mathbb{A}$, where the set of all agents have the same value, i.e. $x_i = x_j$ for all i and j. Hence, the convergence of consensus over cyber graphs (without a spanning tree converging to a steady-state value of y) can be assessed by using:

$$\text{dist}(y, \mathbb{A}) = \inf_{x \in \mathbb{A}} ||y - x||_2 \tag{15}$$

where dist(q, s) is a distance operator which calculates the distance between both the indices q and s. Hence, if dist$(y, \mathbb{A})$ = 0, steady-state convergence is reached.

However, the distributed algorithm is prone to data manipulation via MITM attacks modeled using (6), (9), (13) and (14). An elementary step to minimize the risk of such occurences is to isolate the compromised link from the normal operation [20]-[21]. With MITM attacks on multiple cyber links, it can be seen in Fig. 4(b), that it impedes the rate of convergence to 15 sec. Further, when more cyber links were disabled in Fig. 4(c) due to sophisticated MITM attacks, it could easily lead to multiple steady-state solutions (where, dist(y, $\mathbb{A}$) $\neq$

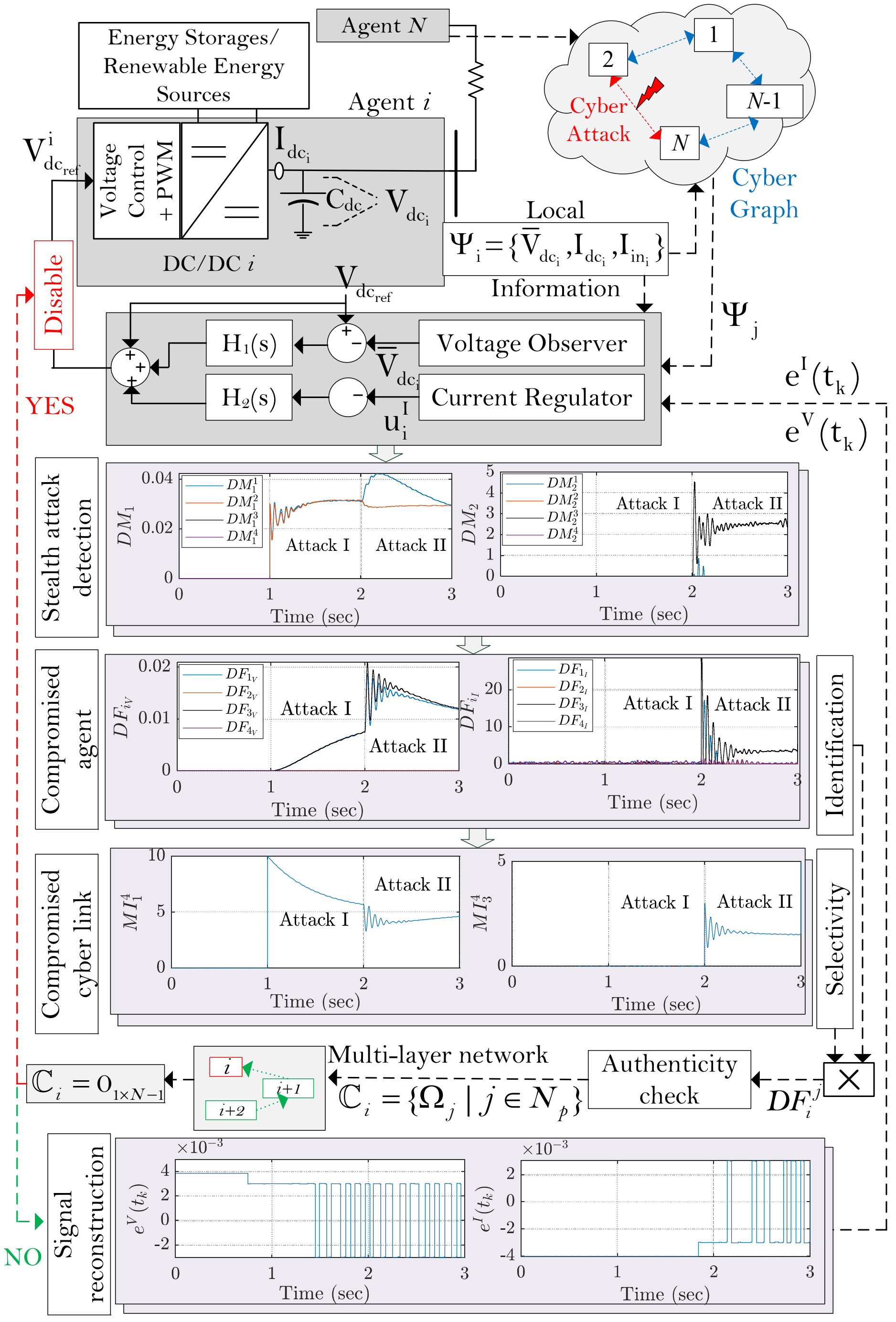

Fig. 5. Proposed multi-layer event-driven resilient control strategy to mitigate defined variants of MITM attacks in DC microgrids.

0), thereby preventing the system to regard the objectives in (5). As a consequence, this case study necessitates immediate detection and mitigation of MITM attacks using the actual cyber graph, such that aforementioned risks can be prevented easily.

III. Proposed Multi-Layer Resilient Control Strategy

In this section, the detection philosophy alongwith the proposed multi-layer countermeasure to remove the attack element(s) is discussed in detail. Moreover, attack-resilient operation of DC microgrid during both steady-state and transient conditions in the presence of MITM attacks will be explained thoroughly.

A. *Detection of compromised agent(s)*

This paper firstly identifies the maximum impact (MI) of the cyber attack on the agents separately for voltage and current control inputs in (1) by using:

$$MI_i^j = \max(\chi_{ij}), \ \forall j \in M_i \tag{16}$$

TABLE I
DETECTION CRITERIA FOR STEALTH ATTACKS [8]-[10]

Stealth attack	Detection criteria for i^{th} agent	Terminology
Voltage [8]	${h_i}^1[\sum_{j\epsilon M_i} a_{ij}(\Delta V_{1_j} - \Delta V_{1_i})]$ $[\sum_{j\epsilon M_i} a_{ij}(\Delta V_{1_j} + \Delta V_{1_i})] \geq \Upsilon_1$	DM_1^i
Current [9]-[10]	$f_i[\sum_{j\epsilon M_i} a_{ij}(I^j_{in_{ref}} - I^i_{in_{ref}})]$ [2] $[\sum_{j\epsilon M_i} a_{ij}(I^j_{in_{ref}} + I^i_{in_{ref}})] \geq \Upsilon_2$	DM_2^i

[1] h_i is a positive quantity used for i^{th} agent.
[2] f_i, $I^i_{in_{ref}}$ denote a positive quantity and the input current reference for i^{th} agent.

TABLE II
TRIGGERING CRITERIA FOR MITM ATTACKS

MITM attack	Triggering criteria for i^{th} agent	Triggering function
x_V^a	$\mathbf{u}^V\mathbf{L}\Delta\mathbf{V}_1^a > \Upsilon_1$ [1]	Ξ_1
x_I^a	$\mathbf{u}^I\mathbf{L}\Delta\mathbf{I}^a_{in_{ref}} > \Upsilon_2$ [2]	Ξ_2

[1] $\Delta\mathbf{V}_1^a$ denote vector representation of ΔV_{1_i} with attack elements.
[2] $\mathbf{I}^a_{in_{ref}}$ denote vector representation of $I^i_{in_{ref}}$ with attack elements.

where $\chi_{ij} = |e_{ij}(t)|$. It is worth notifying that (16) is only tested for i^{th} agent(s), if any of the corresponding elements in the set $DM^i = \{DM_1^i, DM_2^i\}$ goes positive. The performance of the stealth attack detection metrics in Table I to MITM attacks has already been shown in Fig. 5. This implies that as soon as any of the proposed detection metrics in Table I goes positive for i^{th} agent, all the incoming transmitted measurements from its neighbors are examined via (16) to determine the attacked cyber link. It is quite intuitive from (6) and (9) that $|e_{ij}|$ will be maximum for the compromised link as the attack element is added directly to the off-diagonal positive elements in the Laplacian matrix. Using this hypothesis, a positive diverging factor (DF) for i^{th} agent:

$$DF_i = u_i DM^i \tag{17}$$

confirms the presence of an attack element in the respective unit in any of the incoming measurement(s) from the cyber layer.

B. Detection of compromised cyber link(s)

To determine the compromised cyber link(s) originating from j^{th} to i^{th} agent, the following criteria is used:

$$||DF_i^j|| = ||MI_i^j.DF_i|| = \begin{cases} > \Upsilon, \textbf{if } \texttt{attack}_{ij} = 1 \\ < \Upsilon, \textbf{else} \end{cases} \tag{18}$$

It is worth notifying that the detection thresholds in Υ are very small values, which are designed to disregard measurement noise and ensure accurate detection.

Remark III: *Using (18), it can be formalized that the set of detection criterion $DF_i^j = \{DF_{i_V}^j, DF_{i_I}^j\}$ for MITM attacks in Table II can be defined as events, when their values rise above the detection threshold $\Upsilon = \{\Upsilon_1, \Upsilon_2\}$, respectively.*

It can be seen in Fig. 5 where the positive values of DF_{1_V} and DF_{3_V} at t = 1 sec in attack detection monitors suggest that the incoming voltage measurements into agent I and III are attacked. This discrepancy has been resolved in the next step where the positive maximum values of MI_1^4 confirm the presence of `Degree 1` MITM attack element in the cyber link [IV → I]. Following this, a `Degree 1` MITM attack is conducted on the current measurements at t = 2 sec. However using the proposed philosophy, the presence of attack element can be confirmed in cyber link [IV → III] using the positive values of DF_{3_I} and χ_{34_I}. Upon multiplying the values of the detection metrics DF_i and MI_i^j, we obtain positive values for DF_1^4 and DF_3^4 using (18) to confirm the presence of MITM attack elements in the cyber links [IV → I] and [IV → III], respectively.

Upon detection, an authentication signal Ω_i is generated for the particular counterpart (voltage/current) in i^{th} agent to alarm the presence of attack element in i^{th} agent. It should be noted that the nature of authentication signal is binary, such that:

$$\Omega_i^j = \begin{cases} 0(\texttt{F}), & \textbf{if } ||DF_i^j|| > \Upsilon \\ 1(\texttt{T}), & \textbf{else} \end{cases} \tag{19}$$

To simplify the representation of authentication for any signal, $\circ^{\texttt{T}}$ and $\circ^{\texttt{F}}$ will be used to symbolize `True` and `False` for communicated measurements, respectively using (19).

C. Mitigation

As long as these event(s) hold true, the control variables used in designing DF_i are forced to follow the trajectories of non-compromised neighboring signals (with Ω_i^j labeled as `True`). To put this idea into action, this paper uses a multi-layer paradigm to retrieve trustworthy information from agents with authentication signals labeled as `T`. In simple terms, a multi-layer resilience paradigm in cyber network allows to conduct the search of trustworthy agents by consulting the immediate neighbors and the neighbors of neighbors, as shown in Fig. 5. As a result, this search could lead to multiple stops (hops $H-1$, $H-2$ in Fig. 5) before a trustworthy agent is reached. Since MITM attack incurs non-zero error into the control input of the outbound agent, the idea is to force the compromised control error e_{ij} to zero using signal reconstruction of non-compromised error signals from the multi-layer paradigm. As highlighted in Fig. 5, if the set of authentication signals $\mathbb{C}_i$ for i^{th} agent is not a zero vector in the presence of attack elements, event-driven resilient signals are reconstructed to mitigate MITM attacks using:

$$e_{ij}^V(t_k) = \Xi_1(e_{jr}^{V^{\texttt{T}}}(t)) \tag{20}$$

$$e_{ij}^I(t_k) = \Xi_2(e_{jr}^{I^{\texttt{T}}}(t)) \tag{21}$$

where $\circ(t_k)$ (with k as the triggering instant) denote the event-triggered samples of the respective signals and r denoting the final *trustworthy* agent with authentication signal labeled as `T`. These event-driven signals are generated when the triggering criterion in Table II is activated during MITM attacks. Its performance has been shown in Fig. 5, which proves that the control input error will be bounded within a very small defined threshold Υ, despite the presence of attack.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TPEL.2020.3014258, IEEE Transactions on Power Electronics

It is worth notifying that $\Xi(\circ)$ in (20)-(21) is a triggering function, which holds the input signal $\circ$ until the next instant of triggering. However, if $\mathbb{C}_i$ is a null vector, this implies that all the remaining agents are compromised with attack elements and they should be prevented from being used in i^{th} agent. As a result, this leads to localized operation of i^{th} agent by disabling the secondary controller inputs (as highlighted in Fig. 5).

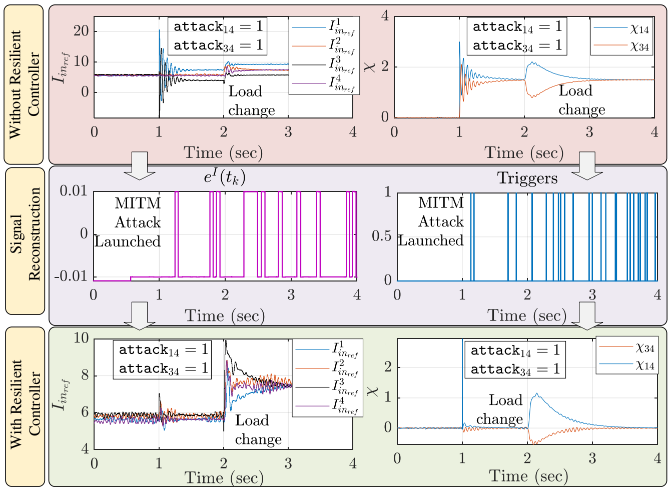

Fig. 6. Performance in the presence of a `Degree 2` MITM attack of the system shown in Fig. 2 at t = 1 sec – the proposed signal reconstruction concept provides resiliency immediately.

The resilient action is completed by susbstituting the event-driven resilient signals with the attacked signal based on the local authentication signal Ω_i^j using:

$$e^V_{ij}(t) = \Omega_i^j e^V_{ij}(t) + (1-\Omega_i^j) e^V_{ij}(t_k) \tag{22}$$
$$e^I_{ij}(t) = \Omega_i^j e^I_{ij}(t) + (1-\Omega_i^j) e^I_{ij}(t_k) \tag{23}$$

Finally, the signals obtained in (22) and (23) are substituted into (1) to realize mitigation of MITM attacks in DC microgrids. As soon as they are substituted, the authentication signals are again traversed back to `T` for the attacked agents. The proposed strategy not only mitigates the attacks but allows to operate normally under external disturbances such as load change, communication delay, etc. It should be further noted that the multi-layer resilience paradigm proposed in this paper can always be further hardened to follow advanced security measures, which specifically requires attention to mitigate the security challenges in the cyber layer. Since this paper aims to provide resilience only using the control layer perspective, the performance of the system in the presence of advanced cyber vulnerabilities can be extended as a future scope of work.

To simplify the operation of the proposed signal reconstruction concept, a case study is carried in Fig. 6 out for the considered microgrid (in Fig. 2) with N = 4 agents following a ring based cyber topology, where a `Degree 2` MITM attack is injected into the outgoing current measurements from agent IV at t = 1 sec. As soon as the attack is launched, it can be seen that without any resilient controller, the input currents are shared disproportionately leading to a positive value of χ_{14} and χ_{34}. However, in the presence of the proposed resilient controller, (23) is immediately activated prior to the detection of *events* in sublayer II of agent I and III in Fig. 6. Upon signal reconstruction of event-driven apriori, it can be seen in Fig. 6 that the error convergence is held between [-0.01, 0.01] owing to every triggering instants in Table II. This leads to proprotionate sharing of input currents even in the presence of attacks. Further, its performance aligns perfectly for external disturbances, such as load change at t = 2 sec, thereby obeying (5). For the purpose of brevity of this paper, the convergence analysis between time-triggered and event-driven signal can be referred from authors' previous work in [23]. This technique has been briefly discussed in [24] for cyber attacks on heterogeneous sources in DC microgrids where disproportionate current sharing can be ascribed to many factors such as cost, capacity and reliability. Further, a detailed explanation to extend this philosophy in AC microgrids has been provided in [25]-[26]. Additionally, the hop-count limitation in a multi-hop cyber network can be referred from [27].

IV. Simulation Results

The proposed event-driven resilient control strategy is tested on a cyber-physical DC microgrid, as shown in Fig. 2 with N= 4 agents. Each agent of equal power capacities (6 kW) comprising of a DC source and DC/DC buck converter, operate to maintain output voltage for a global reference $V_{dc_{ref}}$ = 315 V at their respective buses. Firstly, a sensitivity analysis to study the performance of the proposed strategy for different detection thresholds Υ is studied. Next, its performance is also tested in a variable noise environment for further design recommendations of the threshold. Finally, its performance validation for each vairant of MITM attacks under scenarios such as plugging out of converters, communication delay is carried out to verify the robustness of the event-driven signal reconstruction based attack mitigation strategy. The simulated system and control parameters are provided in Appendix.

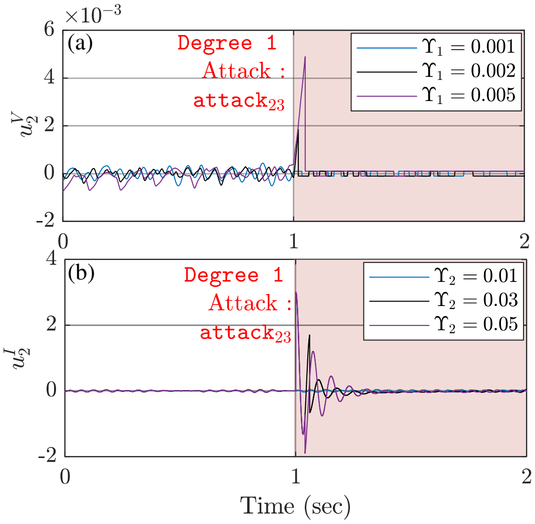

Fig. 7. Sensitivity analysis of the proposed event-driven attack resilient mechanism (refer to the system in Fig. 2) in the presence of `Degree 1` MITM: (a) voltage, and (b) current attack on agent II for different values of Υ_1 and Υ_2 respectively.

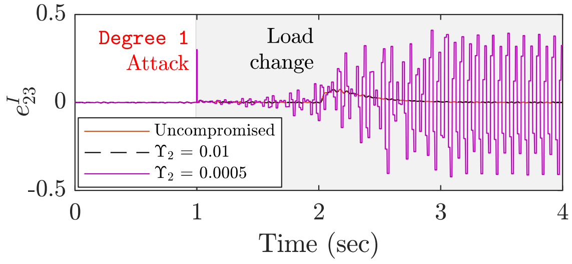

Fig. 8. Performance of the proposed event-driven resilient controller in a high noise environment for different values of Υ – Lower value of Υ_2 leading to oscillatory behavior.

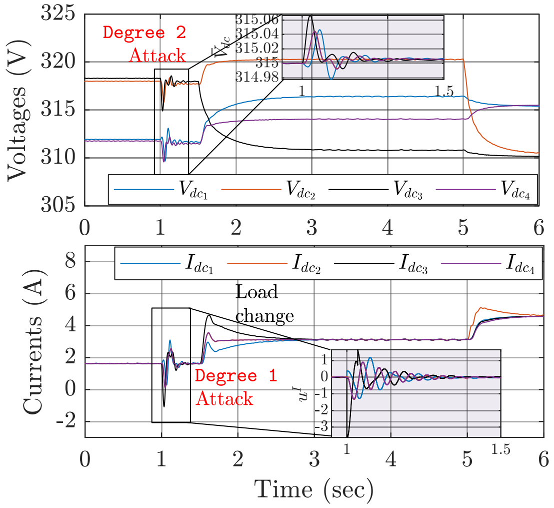

Fig. 9. Performance of the proposed event-driven attack resilient controller in the presence of Degree 1 and 2 MITM attack on current and voltage measurements transmitted to agent II (refer to the system in Fig. 2) at t = 1 sec under a maximum communication delay of 140 ms – the settling time increases due to delayed authentication updates from neighbors.

A sensitivity analysis is carried out to inspect the detection capabilities of the proposed strategy in Fig. 7 for different values of Υ. When a Degree 1 MITM attack is launched on voltage measurements at t = 1 sec, it can be seen that with increase in the value of Υ_1, the transient peak and the settling time to the optimal setpoint keeps increasing. A similar performance can be observed for a Degree 1 MITM attack on the current measurements for different values of Υ_2 in Fig. 7(b). Moreover, to provide resiliency against input and acquisition noise, Υ can be adjudged as small as possible, yet sufficiently larger than the measurement noise to avoid unenuecessary triggering. Hence, the design of Υ highly influences factors such as accuracy and dynamic response. Specifically in a variable noise environment, very small values can lead to stability issues. This has been demonstrated in Fig. 8 where the reconstructed error signals starts oscillating for a very small value of Υ in a variable signal noise environment. When a Degree 1 attack is launched at t = 1 s, it can be seen that the reconstructed error signal follows the uncompromised signal trajectory when $\Upsilon_2 = 0.01$. Whereas when $\Upsilon_2 = 0.0005$, the reconstructed signal gets easily influenced by the noise and encounters unintentional triggering, ultimately leading to an oscillating signal. To handle these issues, the variance of noise in the measurements for a given system can be used as a good indicator to decide the minimum value of Υ in advance. Moreover, an adaptive state-dependent threshold [26] can also be designed to enhance resiliency against noise instead of employing a constant threshold.

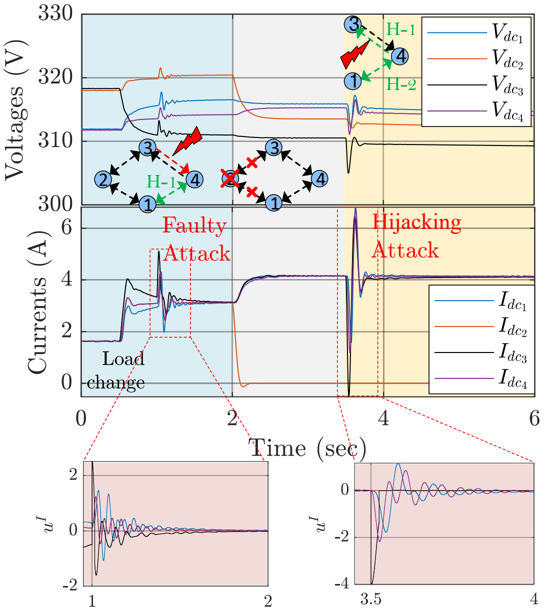

Fig. 10. Performance of the proposed event-driven attack resilient controller in the presence of faulty and hijacking attacks in multiple agents with agent II (refer to the system in Fig. 2) plugged out at t = 2 sec – resiliency is always achieved with the authentication signal for agent III immediately switched from Ω_2 to Ω_1 using a multi-layer paradigm.

In the next case study, the performance of the proposed resilient controller is tested for multiple MITM attacks under a maximum network communication delay of 140 ms, as shown in Fig. 9. At first, when a Degree 2 MITM attack x^V_{attack} of ± 15 V ([attack$_{23}$]&&[attack$_{21}$] = 1) is launched at t = 1 sec; the attacked signal causes an momentary increase with the transient being eliminated as the authentication signal $\Omega_1 = \mathtt{T}$ is reached after a delay of 140 ms to update the event-driven signal $e^V_{23}(t_k)$ using (23). As this hypothesis is well-studied previously, the settling time intuitatively increases to 0.3 sec for a value of $\Upsilon_2 = 0.02$. Further at the same time, a Degree 1 MITM attack x^I_{attack} of 3 A is launched on agent II (attack$_{21}$ = 1), which creates a momentary increase and settles down as the resilient update of $e^I_{21}(t_k)$ is received after a delay of 140 ms using $\Omega_1 = \mathtt{T}$. The robustness of the proposed controller can bedemonstrated via a load change at t = 1.5 & 5 sec, when the currents from each agent are proportionately shared. Hence, the proposed event-driven resilient scheme is not only limited to mitigating attacks for steady-state operation of converter(s) but, is also flexible to operate for dynamic conditions such as load change.

In the final case study, the performance of the proposed resilient controller is tested for instances when the authentication signal is switched from one agent to another. It can be seen in Fig. 10 that a faulty attack of x^I_{attack} = 4 A (attack$_{43}$ = 1) is conducted at t = 1 sec, which triggers the mitigation philosophy as $\mathbb{C}_3$ is not a null vector. This implies that all the agents are transmitting `True` measurements, except for the cyber link directed from IV → III. It is worth notifying that the selection of authentication signal from the set $\mathbb{C}_i$ is not governed by any priority labels. Using this hypothesis, agent I signals with authenticity labeled as $\Omega_1 = \texttt{T}$ is activated immediately for signal reconstruction of $e^I_{43}(t_k)$. Following up to monitor its performance to regard consensus during external disturbances, it can be seen in Fig. 10 that the objectives in (5) still hold true. However, when agent II is plugged out at t = 2 sec, the outgoing communication links are disabled which restricts the transmission of signals to any of its neighbors. When an hijacking attack of x^I_{attack} = 14 A ($\texttt{attack}_{34}$ = 1) is launched at t = 4 sec, agent III immediately switches to the multi-layer paradigm from agent IV (hop $H-1$) re-routing finally to agent I (hop $H-2$) for reconstruction of $e^I_{34}(t_k)$ such that the remaining active agents share the load current equally. Moreover, when both the attacks of magnitude x_{attack} = 4 and 14 A at t = 1 and 4 sec respectively, it can be seen that the sharing accuracy and consensus between agents is unlatered despite the magnitude of attack.

V. Experimental Results

The proposed detection strategy has been experimentally validated in a DC microgrid operating at a voltage reference $V_{dc_{ref}}$ of 50 V with N = 2 buck converters, as shown in Fig. 11. Both the converters are tied radially to a programmable load (voltage-dependent mode). Each converter is controlled by dSPACE MicroLabBox DS1202 (target), with control commands from the ControlDesk from the PC (host). Using the local and neighboring measurements, the proposed event-driven resilient strategy shown in Fig. 5 is modeled for every converter to mitigate the attacks and meet the control objectives in (5). The experimental testbed parameters are provided in Appendix.

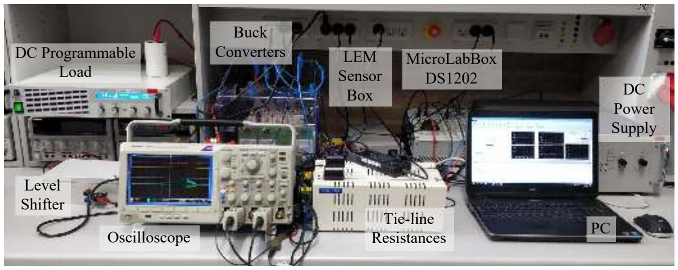

Fig. 11. Experimental setup of a cooperative DC microgrid comprising of N = 2 agents controlled by dSPACE MicroLabBox DS1202 supplying power to the programmable load.

In Fig. 13(a), when MITM attack on the current measurement is launched at the same time for both the cyber links, since the detection philosophy is dependent on transmitted sensor measurements, the authentication signals from both converters will traverse to `F`. As a result, the system immediately runs into local operation as described in Fig. 5 and Fig. 12. Finally, when the attack element in cyber link directed from I → II is removed, it can be seen that the system returns back to the normal operating condition following consensus theory using the proposed event-driven mitigation strategy.

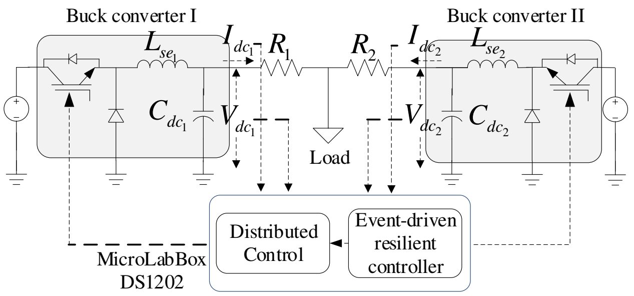

Fig. 12. Single line diagram of the experimental setup shown in Fig. 11.

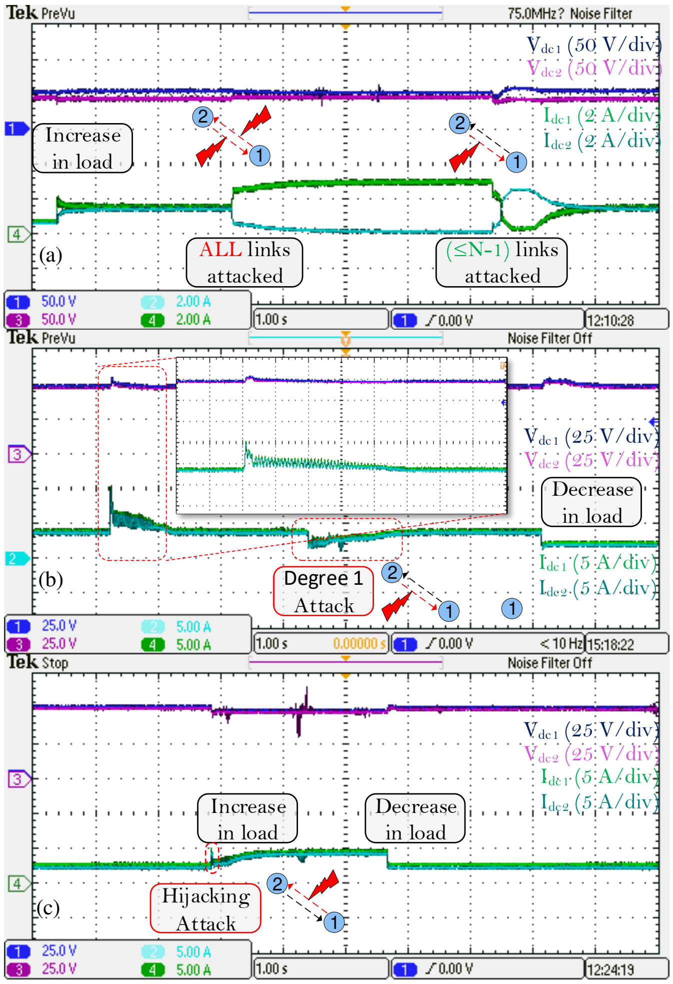

Fig. 13. Experimental validation of the proposed resilient controller for : (a) MITM attack on both cyber links, (b) `Degree 1` attack on link II → I, (c) hijacking MITM attack on link I → II.

Hence, this validates the effectiveness of the performance of proposed resilient controller to a maximum of ($\leq N-1$) scale attacks (at least one *trusted* agent will always be required to broadcast `True` signals). Further in Fig. 13(b), when a `Degree 1` MITM attack of x^I_{attack} = 4 A ($\texttt{attack}_{12}$ = 1) is first launched, the secondary control objective is disregarded, thereby activating the mitigation criteria to trigger e^I_{12} to zero. A zoomed picture is also highlighted to show that consensus is achieved between the states. The resilient action is further repeated as soon as a `Degree 1` MITM attack of x^I_{attack}

= -2 A ($\texttt{attack}_{12}$ = 1) is launched in Fig. 13(b). It is worth notifying that as soon as the attack is launched, the authentication signal from both agents is cross-verified as soon as the detection criteria suggests the presence of an attack. Since Ω_2 = $\texttt{T}$ in this case, the reconstructed resilient signal $e^I_{12}(t_k)$ is designed such that consensus holds true. Finally, in Fig. 13(c), an hijacking MITM attack of x^V_{attack} = -6 V is launched, the resilient controller immediately updates $e^V_{21}(t_k)$ using the *trustworthy* agent I. The action is so fast that it easily accomodates an increase in load immediately following the MITM attack. This establishes that the proposed resilient mechanism can be easily extended to many applications in power electronic systems.

VI. Conclusions and Future Scope of Work

This paper presents a multi-layer event-driven resilient control scheme to detect two sophisticated categories of man-in-the-middle (MITM) attacks on voltage and current measurements in cyber-physical DC microgrids. Since such attacks can impose risk on critical infrastructure, it is vital to remove these attacks in a timely manner in power electronic systems. Adopting a new philosophy by emphasizing cyber attacks as *events*, this paper detects the attacks using a diverging factor (DF) based detection law and transmit the authenticity of communicated measurements to the neighboring agents. As a result, the remaining agents re-orient their operation and assist the attacked cyber link to reconstruct an event-driven error signal using the *trustworthy* agents in a multi-layer paradigm. Since the basic philosophy of consensus theory complies with *identical* arrangements, this concept has been exploited to design the proposed controller. Extensive simulations under many instances are carried out to demonstrate that the proposed controller is robust to many physical disturbances and provides a good manifestation to trigger only during MITM attacks. Moreover, the $(N-1)$-scale resiliency is widely discussed and the hypotheses are validated in the experimental prototype. Future studies will be conducted on the proposed scheme to extend the scope of detection using an adaptive detection threshold for several anomalies. As IEEE 1547-2018 standards for interconnection have recommended communication between grid-connected PV inverters, it also raises the vulnerability of interoperable controller to cyber attacks. Apart from disabling coordination, these cyber attacks may also disregard maximum generation from PVs alongside affecting many grid-supportive functions such as, frequency regulation, reactive power support, virtual inertial response, etc. Using the proposed event-driven resilient scheme prior to a well-designed cyber attack detection criterion [7], such attacks can be easily mitigated from large distribution networks. This strategy will also be highly applicable for mission-critical application such as naval ships and electric aircrafts, where security is a prime concern.

Appendix

Simulation Parameters

The considered system consists of four sources rated equally for 6 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 Ω
Converter: L_{se_i}= 3 mH, C_{dc_i}= 250 μF, $I_{dc_{min}}$ = 0 A, $I_{dc_{max}}$ = 18 A, $V_{dc_{min}}$ = 270 V, $V_{dc_{max}}$ = 360 V.
Controller: $V_{dc_{ref}}$= 315 V, $I_{dc_{ref}}$ = 0, $K^{H_1}_P$ = 3, $K^{H_1}_I$ = 0.01, $K^{H_2}_P$ = 4.5, $K^{H_2}_I$ = 0.32, G_{VP} = 2.8, G_{VI} = 12.8, G_{CP} = 0.56, G_{CI} = 21.8, V_{in} = 270 V, ξ = 4, h = 1.4, f = 2.6, Υ_1 = 0.02, Υ_2 = 0.015.

Experimental Testbed Parameters

The considered system consists of two sources with the converters rated equally for 600 W. It should be noted that the controller gains are consistent for each converter.

Plant: L_{se_i}= 3 mH, C_{dc_i}= 100 μF, R_1 = 0.8 Ω, R_2 = 1.4 Ω
Controller: $V_{dc_{ref}}$= 50 V, $I_{dc_{ref}}$ = 0, $K^{H_1}_P$ = 1.92, $K^{H_1}_I$ = 15, $K^{H_2}_P$ = 4.5, $K^{H_2}_I$ = 0.08, g = 0.64, ξ = 1.8, h = 1.8, f = 2.4, Υ_1 = 0.025, Υ_2 = 0.035.

References

[1] T. Dragicevic, X. Lu, J. C. Vasquez, J. M. Guerrero, “DC microgrids–Part I: A review of control strategies and stabilization techniques”, *IEEE Trans. Power Electron.*, vol. 31, no. 7, pp. 4876-4891, 2016.

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

[3] S. Sahoo and S. Mishra, “A Distributed Finite-Time Secondary Average Voltage Regulation and Current Sharing Controller for DC Microgrids,” *IEEE Trans. Smart Grid*, vol. 10, no. 1, pp. 282-292, Jan 2019.

[4] S. Sahoo, S. Mishra, S. Jha, B. Singh, “A Cooperative Adaptive Droop Based Energy Management & Optimal Voltage Regulation Scheme for DC Microgrids,” *IEEE Trans. Ind. Electron.* vol. 67, no. 4, pp. 2894-2904, 2019.

[5] S. Sahoo and S. Mishra, “An Adaptive Event-Triggered Communication Based Distributed Secondary Control for DC Microgrids”, *IEEE Trans. on Smart Grid*, vol. 9, no. 6, pp. 6674-6683, Nov. 2018.

[6] 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.

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

[9] S. Sahoo, J. C. H. Peng, S. Mishra, and T. Dragicevic, “Distributed Screening of Hijacking Attacks in DC Microgrids,” *IEEE Trans. Power Electron.*, 2019.

[10] S. Sahoo, J. C. H. Peng, A. Devakumar, S. Mishra, and T. Dragicevic, “On Detection of False Data in Cooperative DC Microgrids–A Discordant Element Approach,” *IEEE Trans. Ind. Electron.*, 2019.

[11] S. Sundaram and C. N. Hadjicostis, “Distributed function calculation and consensus using linear iterative strategies,” *IEEE Journ. Select. Areas Commun.*, vol. 26, no. 4, pp. 650-660, May 2008.

[12] M. Conti, N. Dragoni, and V. Lesyk, “A survey of man in the middle attacks,” *IEEE Commun. Surveys Tut.*, vol. 18, no. 3, pp. 2027-2051, 2016.

[13] Y. Desmedt, “Man-in-the-middle attack,” *Encyclopedia of Cryptography and Security*, Springer, pp. 759, 2011.

[14] P. M. Lima, M. V. Alves, L. K. Carvalho and M. V. Vorheira, “Security Against Communication Network Attacks of Cyber-Physical Systems,” *Journ. Control, Autom. and Electr. Systems*, vol. 30, pp. 125-135, 2019.

[15] O. Beg, L. V. Nguyen, T. T. Johnson, and A. Davoudi, “Signal Temporal Logic-based Attack Detection in DC Microgrids,” *IEEE Trans. Smart Grid*, vol. 10, no. 4, pp. 3585-3595, 2019.

[16] K. Manandhar, X. Cao, F. Hu, and Y. Liu, “Detection of faults and attacks including false data injection attack in smart grid using Kalman filter,” *IEEE Trans. Control Netw. Syst.*, vol. 1, no. 4, pp. 370-379, Dec. 2014.

[17] F. Pasqualetti, A. Bicchi, and F. Bullo, "Consensus computation in unreliable networks: A system theoretic approach," *IEEE Trans. Automatic Contr.*, vol. 57, no. 1, pp. 90-104, 2012.

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

[19] M Zhu, and S Martinez, "Discrete-time dynamic average consensus," *Automatica*, vol. 46, no. 2, pp. 322-329, 2010.

[20] C. S. J. Nash-Williams, "Edge-disjoint spanning trees of finite graphs," *J. London Math. Soc.*, vol. 1, no. 1, pp. 445-450, 1961.

[21] S. M. Cioaba and W. Wong, "Edge-disjoint spanning trees and eigenvalues of regular graphs," *Linear Algebr. Appl.*, vol. 437, no. 2, pp. 630-647, 2012.

[22] F Pasqualetti, F Dorfler, and F Bullo, "Control-theoretic methods for cyberphysical security: Geometric principles for optimal cross-layer resilient control systems," *IEEE Control Systems*, vol. 35, no. 1, pp. 110-127, 2015.

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

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

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

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

[27] L. Wenxing, W. Muqing, Z. Min, L. Peizhe, and L. Tianze, "Hop count limitation analysis in wireless multi-hop networks," *Intl. Journ. Distr. Sensor Networks*, vol. 13, no. 1, 2017.

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

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

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 2016 until 2020, he was an Associate Professor at Aalborg University, Denmark. From 2020, he is a professor at the Technical University of Denmark.

He made a guest professor stay at Nottingham University, UK during spring/summer of 2018. His principal field of interest is design and control of microgrids, and application of advanced modeling and control concepts to power electronic systems. He has authored and co-authored more than 200 technical papers (more than 100 of them are published in international journals, mostly in IEEE), 8 book chapters and a book in the field.

He serves as Associate Editor in the IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, in IEEE TRANSACTIONS ON POWER ELECTRONICS, in IEEE Journal of Emerging and Selected Topics in Power Electronics and in IEEE Industrial Electronics Magazine. Dr. Dragičević is a recipient of the Končar prize for the best industrial PhD thesis in Croatia, and a Robert Mayer Energy Conservation award. He is a winner of Alexander van Humboldt fellowship for experienced researchers.

Frede Blaabjerg (S'86-M'88-SM'97-F'03) was with ABB-Scandia, Randers, Denmark, from 1987 to 1988. From 1988 to 1992, he got the PhD degree in Electrical Engineering at Aalborg University in 1995. He became an Assistant Professor in 1992, an Associate Professor in 1996, and a Full Professor of power electronics and drives in 1998. From 2017 he became a Villum Investigator. He is honoris causa at University Politehnica Timisoara (UPT), Romania and Tallinn Technical University (TTU) in Estonia.

His current research interests include power electronics and its applications such as in wind turbines, PV systems, reliability, harmonics and adjustable speed drives. He has published more than 600 journal papers in the fields of power electronics and its applications. He is the co-author of four monographs and editor of ten books in power electronics and its applications.

He has received 32 IEEE Prize Paper Awards, the IEEE PELS Distinguished Service Award in 2009, the EPE-PEMC Council Award in 2010, the IEEE William E. Newell Power Electronics Award 2014, the Villum Kann Rasmussen Research Award 2014, the Global Energy Prize in 2019 and the IEEE Edison Medal in 2020. He was the Editor-in-Chief of the IEEE TRANSACTIONS ON POWER ELECTRONICS from 2006 to 2012. He has been Distinguished Lecturer for the IEEE Power Electronics Society from 2005 to 2007 and for the IEEE Industry Applications Society from 2010 to 2011 as well as 2017 to 2018. In 2019-2020 he serves a President of IEEE Power Electronics Society. He is Vice-President of the Danish Academy of Technical Sciences too. He is nominated in 2014-2018 by Thomson Reuters to be between the most 250 cited researchers in Engineering in the world.