Stealth Attacks in Microgrids: Modeling Principles and Detection

Devakumar, Annavaram; Sahoo, Subham; Mishra, Sukumar

Published in:
2021 9th IEEE International Conference on Power Systems (ICPS)

DOI (link to publication from Publisher):
10.1109/ICPS52420.2021.9670061

Creative Commons License
CC BY 4.0

Publication date:
2021

Document Version
Accepted author manuscript, peer reviewed version

Citation for published version (APA):
Devakumar, A., Sahoo, S., & Mishra, S. (2021). Stealth Attacks in Microgrids: Modeling Principles and Detection. In *2021 9th IEEE International Conference on Power Systems (ICPS)* IEEE (Institute of Electrical and Electronics Engineers). https://doi.org/10.1109/ICPS52420.2021.9670061

Stealth Attacks in Microgrids: Modeling Principles and Detection

Devakumar Annavaram
Department of Electrical Engineering
IIT Delhi
New Delhi, India
devakumarannavaram@gmail.com

Subham Sahoo
Department of Energy Technology
Aalborg University
Aalborg East, Denmark
sssa@energy.aau.dk

Sukumar Mishra
Department of Electrical Engineering
IIT Delhi
New Delhi, India
sukumariitdelhi@gmail.com

***Abstract*—This paper proposes a attack index to detect stealth attacks on current sensor information in a distributed controlled dc microgrids. Stealth attacks are considered the intelligent false data injection attack where it satisfies consensus algorithm objectives in the secondary control. This particular study is carried out on a secondary controller, which is highly prone to cyber-attacks due to involved communication. An attack index (AI) is calculated to detect the stealth attack on the current sensor information, which effectively identifies the stealth attack with existing low bandwidth communication. A stealth attack on current sensor information to the dc microgrid's secondary controller is simulated using Matlab/Simulink environment, and attack detection results are presented and verified with the experimental results.**

***Index Terms*—stealth attack, distributed control, attack detection, consensus.**

I. Introduction

Renewable energy sources are gaining popularity in reducing conventional fossil fuel-based generation's carbon footprint and promoting green energy like solar photovoltaic (SPV), wind, etc. Microgrids are small-scale energy units at the distribution network level where mostly renewable sources are utilized to form. As renewable energy sources, storage devices, and most of the electronic loads are dc in nature, integrating these units in dc microgrids is easier than ac system [1].

Secondary control schemes are employed in dc microgrids apart from primary control to achieve different objectives like proportional power-sharing and average voltage restoration. Centralized control architecture in the secondary controller is vulnerable to a single point of failure [2]. The risk of single-point failure in centralized schemes may be minimized using distributed control scheme. Authors in [3], proposed a distributed controller-based secondary controller for dc microgrid, which only utilizes neighbor's communication to exchange microgrid information. A dynamic average consensus algorithm is proposed in [4]- [5] to obtain the average voltage and currents of the dc microgrid, which are used as control inputs to generate the voltage correction terms.

The presence of a communication system in distributed control makes it more prone to cyber-attacks such as false data injection (FDI) attacks, denial of service (DoS), man in the middle (MITM) attacks, etc. Industrial control systems in the energy sector are considered critical infrastructures that need to be protected from cyber threats, which can cause possible power outages [6]. In [7], authors discussed FDI attacks and DoS attacks on dc microgrids and proposed a signal temporal logic (STL) based detection scheme to detect the presence of attacks. Stealth attacks are known to be intelligent FDI attacks that can deceive control systems without the system operator's notice. A stealth attack on voltage measurements in a dc microgrid with a detection algorithm based on cooperative vulnerability factor is presented in [8].

Further, FDI attacks on current sensor measurement are explored in [9], with discordant element approach-based detection metrics for effective FDI attack detection. Recently, authors in [10] proposed a nonlinear observer-based detection and mitigation method for FDI attacks on current sensor readings in a dc microgrid with constant power loads. A novel FDI attack called concurrent attack was introduced in [11], which aims for both local estimated voltages and communicated values simultaneously to disrupt the cooperative control of microgrid. Most of the attacks are either FDI attacks on current measurements or stealth attack on voltage sensor measurements from the existing literature. Still, the stealth attack on current sensor measurement is not yet investigated thoroughly. Also, all these methods are required to communicate some additional information with neighbor agents to detect an attack, consequently increasing the bandwidth of the communication channels. In [12], a localized attack detection scheme is proposed to detect FDI attacks in ac microgrid, which mainly eradicates the indistinguishability between FDI attacks and disturbances.

In this paper, stealth attack on current sensor measurement to the current regulator in the secondary controller is explored, and a localized attack detection metric is proposed for effective detection. The proposed detection method utilize only existing low bandwidth communication and measurements to calculate the attack index. MATLAB/Simulink environment is used to simulate the attack and to validate efficacy of the proposed detection scheme. The rest of the paper is organized as follows: Section II discussed dc microgrid, distributed control scheme, and graph theory. The stealth attack model and proposed attack index details are provided in Section III. Simulation results of

978-1-6654-2873-6/21/$31.00 © 2021 IEEE

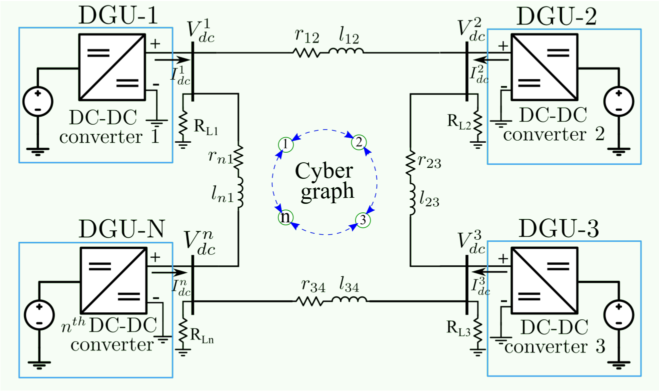

Fig. 1. Cyber-physical model of *N* DGU based distributed dc microgrid

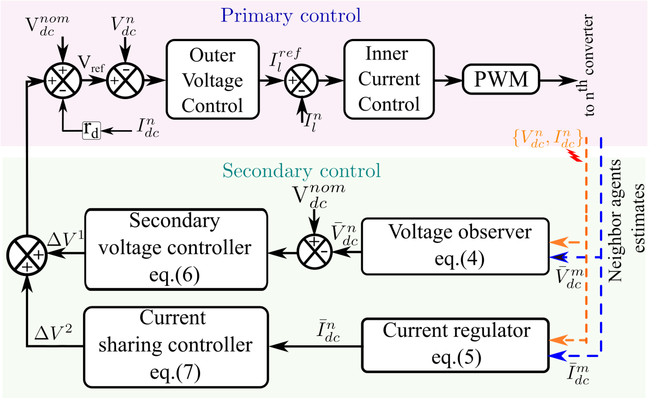

Fig. 2. Control structure for n^{th} DGU

the proposed attack detection method detailed in Section IV, and finally, Section V concludes the paper.

II. Distributed secondary control of dc microgrid

A. System Description

The cyber-physical model of the autonomous dc microgrid consisting of *N* distributed generation units (DGU) is shown in Fig. 1. The DGU consists of a dc source connected to the dc-dc converter is connected to the network through line resistance and inductance. Every DGU in the decentralized microgrid consists of a primary and a secondary controller to generate a setpoint voltage for the n^{th} converter. The primary control is used to achieve proportional power-sharing using droop characteristics, and it also includes the faster inner voltage and current loops. Due to droop characteristics, the terminal voltage of DGU is deviated from its nominal voltage and needs to restore to nominal voltage. A secondary controller is employed to restore the dc microgrid average voltage and subsequently achieve equal current sharing.

B. Preliminaries of Graph Theory

Consider a dc microgrid consisting of N DGUs as a set of nodes $N = 1, 2, \ldots\ldots.N$ connected through an undirected communication link or edge. If an edge presents between any two nodes 'n,m' then node m said to neighbor or adjacent to node n. An adjacency matrix $\mathbf{A} = [a_{nm}] \in R^{NXN}$ is defined as

$$a_{nm} = \begin{cases} > 0, & \text{if } (x_n, x_m) \in \mathbf{E} \\ 0, & else \end{cases} \tag{1}$$

Graph laplacian matrix for the considered cyber graph is $L = D - A$, where E is an edge set. The neighbor set of the n^{th} DGU is given by $N_n = \{m \in N | (m,n) \in E, m \neq n\}$. The eigenvalues of the laplacian matrix highly influences the dynamics of the consensus algorithm and the system.

C. Control Layers in dc microgrids

1) Primary control: The primary control in a DGU consists of inner current control and outer voltage loop with droop control integrated. The duty d output from the current control loop given to the pulse width modulation (PWM) generator and the input reference obtained from the outer voltage controller. The input reference to the voltage controller is acquired as follows

$$v_{ref} = V_{dc}^{nom} - I_{dc} r_d + \Delta V^1 + \Delta V^2 \tag{2}$$

where V_{dc}^{nom}, I_{dc}, r_d, ΔV^1 and ΔV^2 are nominal dc voltage of the microgrid, output dc current of DGU, virtual droop resistance, and voltage correction terms from the secondary control. The virtual droop resistance calculated using

$$r_d = \frac{\Delta v_{max}}{I_{dc}^{max}} \tag{3}$$

where Δv_{max} and I_{dc}^{max} are maximum allowed voltage deviation and maximum current rating of a DGU.

2) Distributed secondary control: The main objective of the secondary controller is to restore the deviated average voltage of the microgrid to its nominal dc voltage and to achieve proportional current sharing [5]. To restore the average voltage of the dc microgrid to nominal dc voltage, a voltage observer used to estimates the average voltage of n^{th} DGU using the dynamic average consensus algorithm. Voltage observer utilizes neighboring estimated voltage $\bar{V}_{dc}^m \; \forall \; m \in N_m$, where N_m denotes the set of neighboring DGUs. The average voltage estimated at n^{th} DGU is given by,

$$\bar{V}_{dc}^n(t) = V_{dc}^n(t) + \int \sum_{m \in N_n} a_{nm} \left(\bar{V}_{dc}^m(\tau) - \bar{V}_{dc}^n(\tau) \right) d\tau \tag{4}$$

where $\bar{V}_{dc}^m$, V_{dc}^n are estimated average voltage at n^{th} DGU and measured output voltage of n^{th} DGU. Similarly, a normalized average current estimated at n^{th} DGU using the neighbors normalized estimated average current $\bar{I}_{dc}^m \; \forall \; m \in N_m$, is given by,

$$\bar{I}_{dc}^n(t) = \int \sum_{m \in N_n} a_{nm} \left(\frac{\bar{I}_{dc}^m(\tau)}{I_{dc_m}^{max}} - \frac{\bar{I}_{dc}^n(\tau)}{I_{dc_n}^{max}} \right) d\tau \tag{5}$$

where $\bar{I}_{dc}^{n}$, $I_{dc_n}^{max}$ and $I_{dc_m}^{max}$ denote measured output current of n^{th} DGU, maximum current rating of n^{th} and m^{th} DGU, respectively. The estimated average values of voltage and current are compared with nominal dc voltage of microgrid and normalized output current of n^{th} DGU, respectively. Subsequently, these errors are processed through the secondary voltage controller and current sharing controller to calculate voltage correction terms ΔV^1 and ΔV^2 respectively.

$$\Delta V^1(t) = (K_{pvs} + \frac{K_{ivs}}{s})(V_{dc}^{nom} - \bar{V}_{dc}^{n}(t)) \tag{6}$$

$$\Delta V^2(t) = (K_{pcs} + \frac{K_{ics}}{s})(\bar{I}_{dc}^{n}(t) - I_{dc}^{n}(t)) \tag{7}$$

where K_{pvs}, K_{ivs}, K_{pcs}, and K_{ics} are proportional integral (PI) gains of secondary voltage controller and current sharing controller as in Fig. 2. Finally, the calculated voltage correction terms added to the primary control as depicted in Fig. 2, to create a setpoint voltage (2) for n^{th} DGU dc-dc converter.

III. Modeling Principles of Stealth Attack

A. Stealth Attack Modeling

The distributed control-based secondary controller successfully achieves convergence in estimated voltages and currents if the cyber graph consists of a spanning tree [4]. At the steady-state, for a spanning tree in the cyber graph, the estimated values in (4) and (5) shall converge to

$$\lim_{t\to\infty} \bar{V}_{dc_n}(t) = V_{dc}^{nom}, \ \lim_{t\to\infty} \bar{I}_{dc_n}(t) = I_{dc_n}, \tag{8}$$

Considering a false data injection attack (FDIA)s in a sensor or communication link, then (8) changes to

$$\lim_{t\to\infty} \bar{V}_{dc_n}(t) = V_{dc}^{a}, \ \lim_{t\to\infty} \bar{I}_{dc_n}(t) \neq I_{dc_n}, \tag{9}$$

For any FDIAs, estimated values are not converged and can easily detected since (8) is infringed. The attacker conducting a stealth attack on sensor information to the secondary controller shall satisfies (8). And such intelligent attacks can easily penetrate into the system controller without the system operator's knowledge. If such an attack is undetected, it can cause system-wide instability and subsequent outage of DGUs from the network. The necessary and sufficient conditions to establish an attack vector for the stealth attack found in [8].

For a different attack on voltage and current measurement in the n^{th} agent can be modeled as

$$\textbf{Sensor attack}: x_n^f(t) = x_n(t) + \alpha_n x_n^a(t) \tag{10}$$

$$\textbf{Communication link attack}: x_{nm}^f(t) = x_{nm}(t) + \alpha_n x_{nm}^a(t), \tag{11}$$

where $x_n = \{V_{dc}^n, I_{dc}^n\}$, $\alpha_n = 1$ in the presence of attack, otherwise $\alpha_n = 0$.

The following case study depicted in Fig. 3 of stealth attack created on current sensor measurement to the secondary control provides a brief understanding of attack effect. A four DGU based dc microgrid with an operating voltage of 315 V is considered. The stealth attack vector $x_n^a = [s; 0; -s; 0]$ is constructed to inject zero-sum errors into the current sensor measurement to the secondary controller of agents 1 and 3. At t = 1.5 sec, the load is increased, and the system states changed according to new increased load values, and estimated values are converging. At t = 2.5 sec, a stealth attack is initiated with the attack vector as mentioned earlier on DGU 1 and 3. After launching the attack on current sensor measurements, it is evident that estimated voltage and actual current values converge according to (8). At t = 3.5 sec, the attacker may attempt a destabilization attack to create instability in the system. The attacker may unfairly increase one of the attacked sensor measurement by a large magnitude; subsequently, the output voltages of DGU rapidly increase and hit the over voltage threshold limit of safety relays.

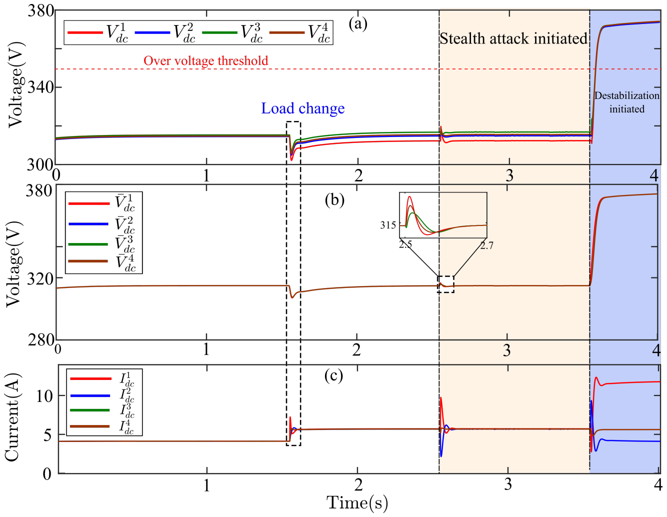

Fig. 3. Destabilization caused by stealth attack on current sensor measurement of DGU 1 & 3 in dc microgrid. (a) DGUs output voltages (b) Average voltages of DGUs (c) DGUs output current

B. Proposed Attack Detection Scheme

An localized attack index $b_n(t)$ is proposed to detect the stealth attack on current measurements before it propagates into the system and to take a corrective action accordingly minimize the adverse effects.The proposed detection method has the advantage of utilizing only existing low bandwidth communication and communicated parameters. The attack index is calculated in the secondary controller of n^{th} DGU using local measurement and local estimated average currents, and other shared estimated values. The calculated generalized attack index is given by,

$$b_n(t) = g\left[\sum_{m\in N_n}(\Delta x_m(t) - \Delta x_n(t))\right] + \left[\sum_{m\in N_n}(\Delta x_m(t) + \Delta x_n(t))\right], \tag{12}$$

where g is positive value, and

$$\Delta x_n = I_{dc}^n(t) - \bar{I}_{dc}^n(t), \tag{13}$$

$$\Delta x_m = I_{dc}^n(t) - \bar{I}_{dc}^m(t), \tag{14}$$

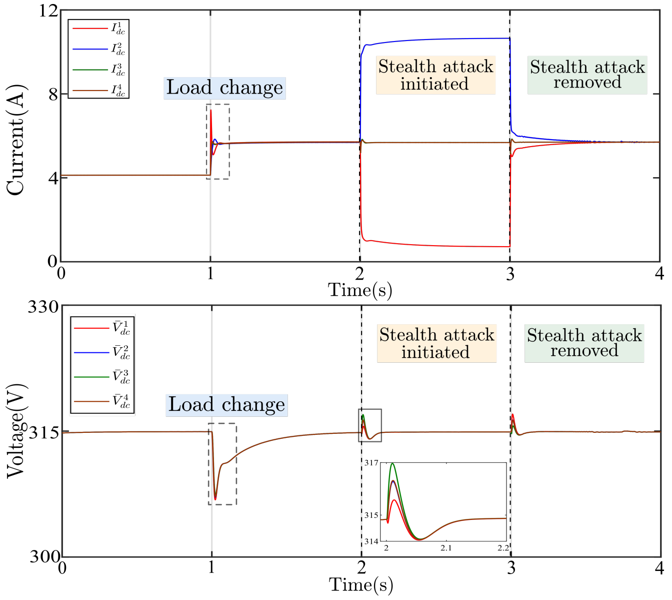

Fig. 4. Case 1: Stealth attack on current measurements of DGU 1 and 3 as per [8] (a) DGU output current (b) Average voltages of DGUs.

From the resulted attack index, $b_n(t)$ is either positive or negative for the attacked DGUs for some time over τ_a then the event declared as an attack; otherwise, the attack index $b_n(t)$ is zero.

IV. Results and Discussion

A four DGU based ring connected dc microgrid shown in Fig. 1 with an operating voltage 315 V is simulated in the MATLAB/Simulink environment to test the stealth attack on current sensor measurement and proposed detection method. A ring connection-based cyber-graph is employed to communicate the neighbor's average voltage and current measurement information with the n^{th} agent. Further, hardware results for the stealth attack on current measurements is presented.

A. Stealth Attack on Current Measurements of Secondary Controller

In case 1, the stealth attack on current sensor measurement presented in [8] is simulated and shown in the Fig. 4 . At t = 1 sec, the load on the system is increased, and the respective average voltage and output currents of all DGUs reach respective consensus values. At t = 2 sec, in DGU 1 and 3, a stealth attack on current measurement to the secondary control created with attack vector $I_{dc}^a = [5; 0; -5; 0]$ A and it is evident from the Fig. 4, the output currents of DGU has deviated from the consensus, but average voltage still converges to actual nominal voltage, thus violated (8). At t = 3 sec, the attack removed from current sensor information and the output currents of DGUs start converging to average current of microgrid. Whereas in case 2, a stealth attack only on current measurement to the secondary control current regulator is initiated at t = 2 sec, as shown in the Fig. 5, which satisfies (8) for successful consensus.

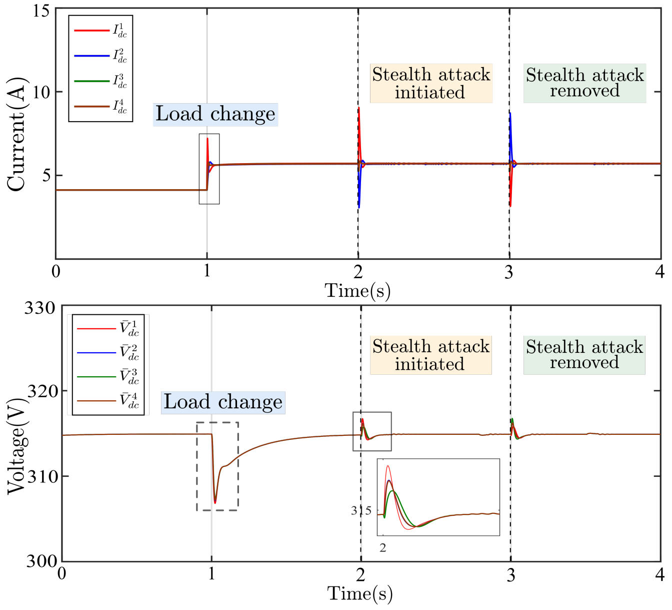

Fig. 5. Case 2: Stealth attack only on current measurements to the secondary control current regulator of DGU 1& 3. (a) DGUs output currents (b) Average voltages of DGUs.

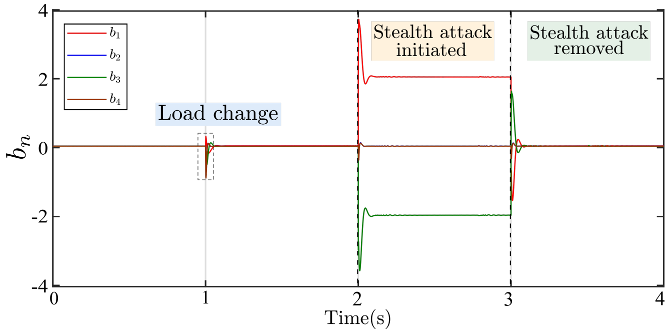

Fig. 6. Proposed attack index $b_n(t)$ to detect the stealth attack on current measurement.

This kind of attack is unnoticed and can quickly escape from the operator's observation and consequently launches destabilization attacks to create system-wide outages. The zoomed portion in Fig. 5 shows the convergence of all DGUs average voltage to 315 V after initiating the attack, which is the nominal voltage of dc microgrid. The performance of the proposed detection method for the stealth attack on a current sensor with attack index $b_n(t)$ is given in Fig. 6. At t = 2 sec, for the stealth attack on current measurement, the attack index $b_n(t)$ of DGU 1 and DGU 3 deviates from the zero for more than τ_a and the remaining DGU $b_n(t)$ is zero. At t = 3 sec, the attack on current sensor information is removed. Soon after this, the attack index $b_n(t)$ of all DGUs becomes zero, which indicates no attack. After detection of the attack, necessary corrective action is taken by the DGU operator to avoid the system-wide failure.

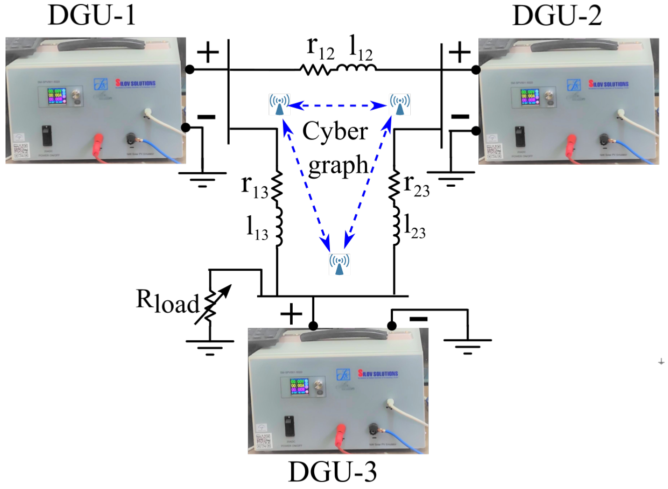

Fig. 7. Single line diagram of dc microgrid experimental setup comprises of three DGUs.

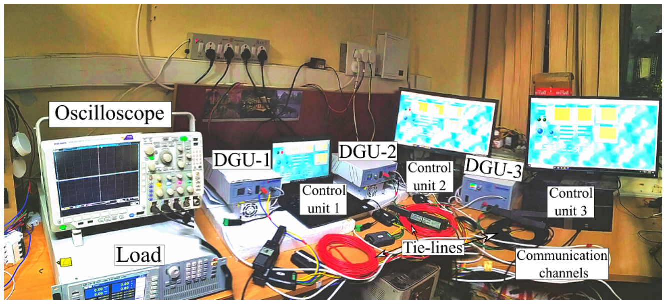

Fig. 8. A three DGU based cyber-physical dc microgrid experimental setup.

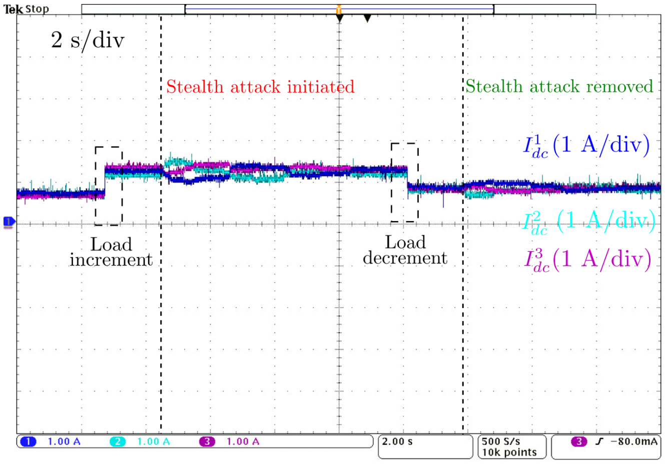

Fig. 9. Experimental validation of stealth attack on current sensor of DGU 1 & 3 in a three DGU experimental setup.

B. Experimental Result of Stealth Attack in dc microgrid

A single line diagram of three DGUs based cyber-physical dc microgrid is presented in Fig. 7 is developed using commercially available dc-dc converters [13] and National Instruments (NI) Labview software as shown in Fig. 8. Modbus communication protocol is utilized for communicating the estimated voltage and current sensor values from n^{th} DGU to adjacent DGUs. The laboratory-scale dc microgrid prototype is used to validate the stealth attack on current sensor measurement and detection scheme. The current sensor measurements are manipulated in secondary control, which is implemented in the Labview platform with attack vector $I^a_{dc} = [0.1; 0; -0.1]$ A. It's worth noting that the experimental results were presented in terms of measurable quantities such as output currents because commercial DC/DC converters lacked an acquisition channel, and attack index $b_n(t)$ is calculated in the secondary control unit using (12). The experimental result of stealth attack implementation in the dc microgrid is presented in Fig. 9. Initially, the load increased in the dc microgrid, and all DGUs equally sharing load; soon after, a stealth attack launched with the attack vector mentioned previously. After the attack initiation, all the DGUs output current reach a consensus, thus satisfying (8). Consequently, the calculated attack index changes between positive and negative values for the attacked DGUs otherwise attack index is zero, thus provides an alarm in the attacked DGU nodes.

V. Conclusion

This paper presented a stealth attack on current sensor information to the secondary control in a distributed controlled dc microgrid. An attack index was proposed to detect such attacks and calculated using local and communicated neighbor information. The proposed method effectively utilized existed low bandwidth communication to detect the presence of attacked DGU. The proposed attack detection scheme was validated by simulation on four DGU based dc microgrids, and results showed accurate detection of the attacked DGU.

References

[1] S. Anand, B. G. Fernandes, and J. M. Guerrero, "Distributed control to ensure proportional load sharing and improve voltage regulation in low-voltage DC microgrids," *IEEE Trans. Power Electron.*, vol. 28, no. 4, pp. 1900–1913, 2013, doi: 10.1109/TPEL.2012.2215055.

[2] T. Dragicevic, X. Lu, J. C. Vasquez, and 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, doi: 10.1109/TPEL.2015.2478859.

[3] 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, doi: 10.1109/TPEL.2014.2324579.

[4] D. Pullaguram, S. Mishra, and N. Senroy, "Event-Triggered Communication Based Distributed Control Scheme for DC Microgrid," *IEEE Trans. Power Syst.*, vol. 33, no. 5, pp. 5583–5593, Sep. 2018, doi: 10.1109/TPWRS.2018.2799618.

[5] S. Sahoo and S. Mishra, "An adaptive event-triggered communication-based distributed secondary control for DC microgrids," *IEEE Trans. Smart Grid*, vol. 9, no. 6, pp. 6674–6683, 2018, doi: 10.1109/TSG.2017.2717936.

[6] CISA, "Recommended Cybersecurity Practices for Industrial Cybersecurity," 2020.

[7] O. A. 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, doi: 10.1109/TSG.2018.2832544.

[8] S. Sahoo, S. Mishra, J. C. Peng and T. Dragičević, "A Stealth Cyber-Attack Detection Strategy for DC Microgrids," *IEEE Trans. Power Electron.*, vol. 34, no. 8, pp. 8162-8174, Aug. 2019, doi: 10.1109/TPEL.2018.2879886.

[9] S. Sahoo, J. C.-H. Peng, A. Devakumar, S. Mishra, and T. Dragicevic, “On Detection of False Data in Cooperative DC Microgrids—A Discordant Element Approach,” *IEEE Trans. Ind. Electron.*, vol. 67, no. 8, pp. 6562–6571, Aug. 2020, doi: 10.1109/TIE.2019.2938497.

[10] A. Cecilia, S. Sahoo, T. Dragičević, R. Costa-Castelló and F. Blaabjerg, ”Detection and Mitigation of False Data in Cooperative DC Microgrids With Unknown Constant Power Loads,” *IEEE Trans. Power Electron.*, vol. 36, no. 8, pp. 9565-9577, Aug. 2021, doi: 10.1109/TPEL.2021.3053845.

[11] J. Zhang, S. Sahoo, J. C. -H. Peng and F. Blaabjerg, ”Mitigating Concurrent False Data Injection Attacks in Cooperative DC Microgrids,” *IEEE Trans. Power Electron.*, vol. 36, no. 8, pp. 9637-9647, Aug. 2021, doi: 10.1109/TPEL.2021.3055215.

[12] R. Lu, J. Wang, and Z. Wang, “Distributed Observer-Based Finite-Time Control of AC Microgrid under Attack,” *IEEE Trans. Smart Grid*, vol. 12, no. 1, pp. 157–168, 2021, doi: 10.1109/TSG.2020.3017793.

[13] Silov Solutions Pvt. Ltd., 2021. [Online] Available: http://www.silovsolutions.com/