Decentralized Anomaly Identification in Cyber-Physical DC Microgrids

Gupta, Kirti; Sahoo, Subham; Mohanty, Rabindra; Panigrahi, Bijaya Ketan; Blaabjerg, Frede

Published in:
2022 IEEE Energy Conversion Congress and Exposition, ECCE 2022

DOI (link to publication from Publisher):
10.1109/ECCE50734.2022.9947581

Publication date:
2022

Document Version
Early version, also known as pre-print

Decentralized Anomaly Identification in Cyber-Physical DC Microgrids

Kirti Gupta
Department of Electrical Engineering
Indian Institute of Technology, Delhi
Delhi, 110016, India
Email: Kirti.Gupta@ee.iitd.ac.in

Subham Sahoo
Department of Energy
Aalborg University
Aalborg, 9220, Denmark
Email: sssa@energy.aau.dk

Rabindra Mohanty
Department of Electrical Engineering
IIT (BHU), Varanasi
Uttar Pradesh, 221005, India
Email: rabindra.eee@itbhu.ac.in

Bijaya Ketan Panigrahi
Department of Electrical Engineering
Indian Institute of Technology, Delhi
Delhi, 110016, India
Email: Bijaya.Ketan.Panigrahi@ee.iitd.ac.in

Frede Blaabjerg
Department of Energy
Aalborg University
Aalborg, 9220 , Denmark
Email: fbl@energy.aau.dk

***Abstract*—DC microgrids with distributed control architectures enhance the operational reliability, scalability and flexibility. However, the underlying communication infrastucture makes the system highly susceptible to cyber attacks. These attacks in DC microgrids cause severe impact, that can be easily misinterpreted as faults, which can then maloperate the protection decision. Although various protection schemes have been established, a tailor-made scheme to distinguish faults from cyber attacks is needed to ensure reliability of supply. In this paper, we use a two dimensional plane with deviation of current (δI) and voltage (δV) at the terminal of each converter to distinguish between cyber attacks and faults in DC microgrids. As this scheme is governed based on physics of secondary controller operation, it is simple to implement and scalable to any physical topology. The performance of the proposed scheme is tested with real time simulation in OPAL-RT environment with HYPERSIM software for different topologies including radial, ring and mesh networks. In addition, the scheme is also tested and verified for simultaneous cyber attack on multiple converters. The simulation results validates that the proposed decentralized scheme is effective in both detecting and localizing cyber-physical anomalies within 2 ms.**

***Index Terms*—Decentralized anomaly characterization, cyber-physical systems, cyber attacks, faults.**

I. Introduction

Microgrids have evolved into a cyber-physical systems with the incorporation of cooperative secondary control framework [1]. Such an architecture facilitates scalability, flexibility and a reliable alternative to centralized mechanism that requires high communication bandwidth and prone to single-point-of-failure. The distributed control configuration involves exchanging information among the neighboring power electronic converters through communication network. The reliance on communication infrastructure for information exchanges makes the system susceptible to potential cyber attacks. Moreover, the physical devices (like converters, sensors, lines connecting distributed energy resources) themselves are prone to faults/failures.

An anomaly can be termed as abnormal behaviour, as an outcome of either fault or a cyber attack [2]. In a unipolar DC system, physical anomalies may range from pole to ground faults (bus/lines), failure of device or sensor faults. On the other hand, cyber anomalies may be broadly classified in two categories. Amongst data availability and data integrity attacks, this work investigates the latter one into consideration, which is commonly known as false data injection attacks (FDIAs). The attacker may inject malicious packets of data in the information being exchanged through communication links to affect the integrity of information. The attacker may also hijack the controller to generate the references, which can deteriorate the system performance and may also affect the stability of the system. The data when delayed temporarily or permanently (commonly known as denial of service (DoS)) falls under the category of data availability attacks. The fast transient response of the DC microgrid system under such disturbances is yet another challenge, which mandates a fast and accurate decision [4].

In DC microgrids, protection decision has to be taken within few milliseconds [5]. The current derivative (di/dt)-based protection is a simple yet effective method for fault detection. In a multi-bus DC microgrid, the major problem associated with di/dt method is false triggering at multiple converters based on the selected threshold, due to low impedance of dc cables, system topology and threshold value. Therefore, it is necessary to add an anomaly identification algorithm to avoid false triggering of circuit breaker (CB). Although recent literature separately discusses detection of the physical [6]–[10] and cyber anomalies [11], [12], few attention is paid on distinguishing between these anomalies. In [13], a data driven approach termed as an intelligent anomaly identification technique is presented which can distinguish and localize faults and cyber attacks. Albeit it excludes the mathematical modeling effort, yet it suffers from

overfitting and training requirement associated to diverse scenarios. Another contribution in this area of research is provided in [2], which shows a parametric time frequency logic framework. It is a model-free approach and detect anomaly traces by extracting the time-frequency content from training input. In [14], localized frequency and average voltage samples of inverters are plotted against each other for 100 ms window to distinguish cyber attacks and faults. This time margin may be very long for DC systems as faults need to be isolated in a much smaller duration of time [15]. This mandates strict boundaries on the time of anomaly detection and classification. Further, this decision would be directed towards protection schemes [16] or cyber attack mitigation schemes [17], [18] for further action.

To bridge this gap, this paper presents a decentralized approach towards this problem. The proposed method utilizes local I and V information and plot their deviations in $\delta I - \delta V$ plane. Further, according to the regions traversed in the $\delta I - \delta V$ plane, anomalies are distinguished within 2 ms. Real-time validation of the proposed method in various network configurations like radial, ring and mesh networks have been performed, which verifies that the proposed scheme is effective in both identifying and localizing the cyber and physical anomalies.

The key contributions of this work can be summarized as:

- A decentralized anomaly detection mechanism has been designed which takes the local measurements of current and voltages at the sampling frequency of 4 kHz. Further, their deviations are plotted in $\delta I - \delta V$ plane and according to the travel of the trajectories in various regions the anomalies can be identified.
- The proposed scheme is efficient in identifying and localizing the anomaly in 2 ms. This decision can further be directed to the protection systems or cyber attack mitigation tools accordingly for further actions.
- The method does not require laying out additional sensors for anomaly identification. Since the method is decentralized, it is scalable to different network configurations.
- The proposed method is also tested and validated for cyber attacks on multiple converters. It both identifies and localizes the anomalies.

The remainder of the paper is organized as: preliminaries on graph theory and cooperative secondary control is presented in Section II, a brief description of the problem is presented in the Section III. The proposed scheme is discussed in the Section IV with the performance validation of the developed scheme is presented in the Section V. Finally, the work is concluded in Section VI .

II. Preliminaries

A. Graph Theory

In Fig. 1, an undirected cyber graph is considered, where each node represents an agent, also denoted as $\mathbf{x} = \{x_1, x_2, \ldots, x_N\}$ and are linked by edges via an associated adjacency matrix, $\mathbf{A}_{\mathrm{G}} = [a_{ij}] \in R^{N\times N}$, where the communication weight a_{ij} (from node j to node i) is modeled using the specified law: $a_{ij} > 0$, if $(\psi_i, \psi_j) \in \mathbf{E}$, where $\mathbf{E}$ is an edge connecting two nodes, with ψ_i and ψ_j being the local and neighboring node, respectively. It should be noted that if there is no cyber link between psi_i and ψ_j, then a_{ij} = 0. Any given agent at ψ_i node share current and voltage information with neighbors $N_i = \{j \mid (\psi_j, \psi_i) \in \mathbf{E}\}$. The matrix representing incoming information can be given as, $\mathbf{D}_{\text{in}} = \mathtt{diag}\{d_i^{in}\}$, where $d_i^{in} = \sum_{j\in N_i} a_{ij}$. Similarly, the matrix representing outcoming information can be given as, $\mathbf{D}_{\text{out}} = \mathtt{diag}\{d_i^{out}\}$, where $d_i^{out} = \sum_{i\in N_j} a_{ji}$. Assembling the sending and receiving end information into a single matrix, we obtain the Laplacian matrix $\mathbf{L}$ = $[l_{ij}]$, where l_{ij} are its elements designed using, $\mathbf{L}$ = $\mathbf{D}_{\text{in}}$–$\mathbf{A}_{\mathrm{G}}$.

B. Cooperative Secondary Control

In the conventional cooperative secondary control framework, each converter comprises of an average consensus based voltage regulator and current regulator. The secondary control arrangement generates two voltage correction terms from two PI controllers respectively. The cooperative control architecture relies on the relative information from the neighbours connected via sparse communication network. In contrast to the existing cooperative control framework, this paper considers a secondary control framework as a linear first-order multi-agent systems (MAS). It consists of a single PI controller for each secondary controller, which generates an auxiliary control input using information exchanges from neighbouring converters [19]. This voltage correction term is then directed to the droop controller to drive the system in such a manner to attain the desirable objectives of average voltage regulation and proportional current sharing in a much faster way as compared to the conventional framework. The DC microgrid testbed with the objectives of average voltage regulation and proportional current sharing through cooperative control is shown in Fig. 4. In the equations presented further, the superscript i represents the i^{th} agent or the parameters corresponding to it. The overall voltage equation for i^{th} agent with primary and secondary controllers can be represented by:

$$V^i(t) = V^* - R^i I^i(t) + \Delta V^i(t) \tag{1}$$

where it consists of the droop term from primary control and the voltage correction term ($\Delta V^i(t)$) from secondary control. The voltage correction term is further shown by (2),

$$\Delta V^i(t) = K_{pv}^i \dot{e}_v^i(t) + K_{iv}^i e_v^i(t) \tag{2}$$

where, K_{pv}^i and K_{iv}^i are the proportional and integral gains corresponding to the secondary controller. Further, the equation for secondary cooperative controller is represented by (3),

$$\dot{e}_v^i(t) = -g_i\left(\bar{V}^i(t) - V^*\right) - \sum_{j\in N_i} a_{ij}\left(R^i I^i(t) - R^j I^j(t)\right) \tag{3}$$

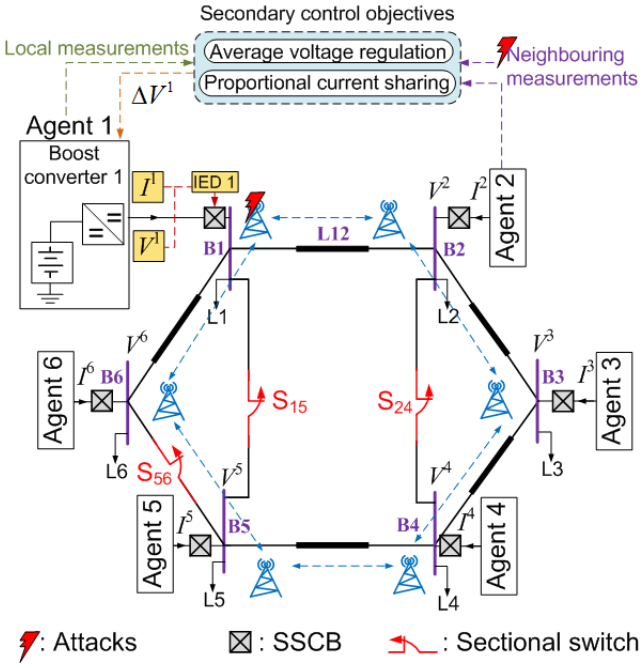

Fig. 1: Test microgrid model with DC/DC boost converters.

The average voltage of the i^{th} agent ($\bar{V}^i(t)$) is shown by (4).

$$\dot{\bar{V}}^i(t) = \dot{V}^i(t) + \sum_{j \in N_i} a_{ij} \left(\bar{V}^j(t) - \bar{V}^i(t) \right) \tag{4}$$

The distributed secondary control involves information sharing between the neighbour agents through communication links. Such exchanges of information among the neighbours can make the system prone to malicious attacks which in turn may deteriorate the performance of the microgrid or even destablize them [20].

III. Problem Formulation

In the Fig. 1, each DC/DC boost converter is connected to the associated bus (B) via solid state circuit breaker (SSCB). These SSCBs are controlled by their respective intelligent electronic device (IED) using local voltage and current information. Further, depending on the position of sectional switches, network topology can be transformed into radial (all switches open), ring (only S_{56} closed) or mesh (all switches closed). The fault detection algorithm and the problem associated with it while dealing with different types of cyber-physical anomalies is presented further.

A. Fault Detection

The current is collected at IED with a sampling rate of 4 kHz. The disturbance index (d) to detect any disturbance in the system, is calculated as:

$$d = \frac{1}{K\Delta t} \left(\sum_{k=1}^{K} |i_{k+1} - i_k| \right) \tag{5}$$

where, i_k is the sample value of current for k^{th} instant, Δt is the sampling interval and K = 4 (there are 4 samples in 1 ms). To keep a track on only magnitude change of current, absolute value of the difference in current is taken in (5). A disturbance is ensured when d exceeds the threshold value, φ; else suggests a normal state. The threshold value, φ can be calculated as [4], [16]:

$$\begin{aligned} \varphi &= \frac{1}{K\Delta t} \left(\sum_{k=1}^{K} |i_{k+1} - i_k| \right) \\ &= \frac{1 \times 10A}{4 \times 250 \times 10^{-6} s} = 10000 A/s \end{aligned} \tag{6}$$

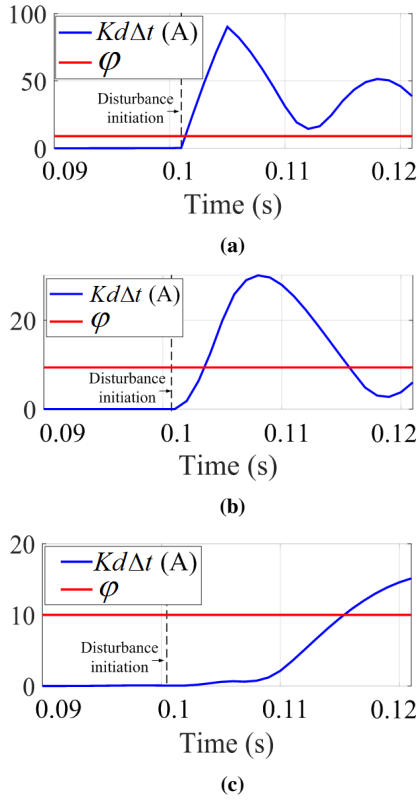

Fig. 2: $Kd\Delta t$ for agent 1 for (**a**) fault on bus (B1); (**b**) fault between line (L12); (**c**) cyber attack on voltage signal.

For high security operation of IEDs, sum of four consecutive sample-to-sample differences is set to 10 A i.e, $\sum_{k=1}^{K} |i_{k+1} - i_k|$ = 10 A, which is well within the allowable load change limit. Fig. 2 shows $Kd\Delta t$ for physical and cyber anomalies. It is to be noted that $d > \varphi$ even for cyber attacks. As a result, it gives rise to false tripping decisions and alarms in the protection system. Hence, the proposed anomaly identification scheme can facilitate accurate decision support and security management.

IV. Proposed Decentralized Anomaly Identification Scheme

Let the information shared between the agents be, $x^i(t) = [V^i(t), I^i(t)]$. The voltage correction term is represented by

$\Delta V^i(t)$. The attacks can be balanced where the system has feasible solution satisfying all the objectives; or unbalanced where the system disregards the objectives. The work presented, considers the unbalanced attacks where the system may go beyond the bounds of operation, specified further. This may unnecessarily activate the relays, which can lead to shutdown of the microgrid. Assuming that the attacker modifies these signals in the form of a step change as expressed in (7).

$$x^{iC}(t) = x^i(t) + x^{iA}(t) \tag{7}$$

In this work, it is assumed that an adversary gains control over the voltage correction term signal generated by the secondary controller directed towards the primary control. Hence, the attacker can modify the voltage correction term as presented by (8).

$$\Delta V^{iC}(t) = \Delta V^i(t) + \Delta V^{iA}(t) \tag{8}$$

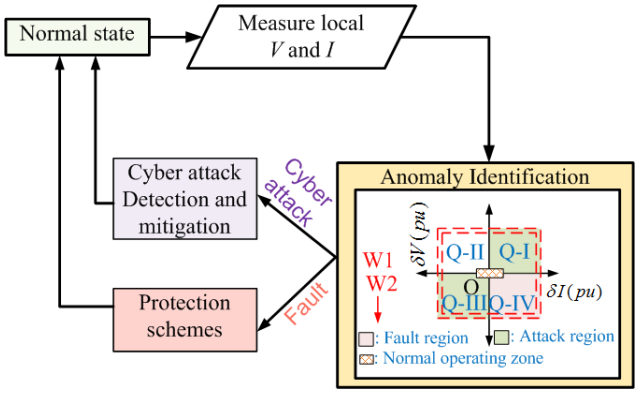

Fig. 3: Proposed decentralized anomaly detection scheme.

Combining equations (1)–(4), we get the change in local current w.r.t. local voltage corresponding to i^{th} agent as:

$$\frac{\dot{I}(t)^i}{\dot{V}(t)^i} = \frac{\left[\left(1 + K^i_{pv} \sum_{j\in N_i} a_{ij}\right) R^i\right]^{-1} \left[\begin{array}{l} K^i_{pv} \sum_{j\in N_i} a_{ij} R^j \dot{I}^j(t) - \left(1 + K^i_{pv} g_i\right) \dot{\bar{V}}^i(t) - \\ \bar{V}^i(t) \sum_{j\in N_i} a_{ij} + \sum_{j\in N_i} a_{ij} \bar{V}^j(t) + K^i_{iv} e^i_v(t) \end{array}\right]}{\dot{\bar{V}}^i(t) - \sum_{j\in N_i} a_{ij} \left(\bar{V}^j(t) - \bar{V}^i(t)\right)} \tag{9}$$

Further, the normal operating range of voltage is $\pm 5\%$ [21] and for current maximum overload taken is 120% of the rated current. Using these pre-defined values we can obtain the region of normal operating zone around the origin, O (0,0) as shown by hashed orange region. A buffer data of voltage and current measurements for 2 ms window (W) is stored as pre-disturbance values, which is constantly updated. These are denoted as V^{pre} and I^{pre} for voltage and current values respectively sampled at the rate of 4 kHz sampling frequency. Further, using (9), we can obtain the deviation of current with respect to deviations in voltage. The movement of trajectory in different quadrants specifies the existence of the type of anomaly like, the fault region in quadrant IV and attack regions in quadrant I and III, as shown in Fig. 3. Further, the experimental results justify the effectiveness of the proposed physics-based decentralized anomaly identification scheme which correctly identifies and localizes the type of anomaly. It further directs the decision to the corresponding protection/mitigation schemes so that the system can be restored back to its normal state. The decision time by the proposed scheme is within 2 ms, which is quite fast and also mandatory in DC microgrid systems. The time criticality in a DC systems protection is because the DC-link capacitor of the power electronic converter discharges rapidly during anomalies (say faults) which can cause the DC bus voltage to drop sharply. In addition, protection system is activated only if the current exceeds the threshold value (φ). It can be seen in Fig.2b and Fig.2c, protection system is enabled after a few milliseconds (greater than 2 ms) after initiation of cyber attack to detect it as fault. However, the proposed scheme is effective in correctly identifying the anomalies within 2 ms.

The scheme is simple, does not require any additional sensors and is scalable to different network configurations. These features suggest the feasibility of the installation of the proposed scheme in the industrial applications. The proposed scheme can be easily implemented in the IED to detect the anomalous situations and direct commands to the concerned protection/cyber mitigation schemes for further action. Till now, the proposed scheme has been tested for FDI attacks on the voltage correction signals generated by the secondary controller and proved to work effectively. Apart from such attacks, an adversary can also generate attack scenarios such as denial of service (DoS) attacks which disrupts the availability of the signals. Other type of cyber attacks may include time delay attacks. As microgrid is a time critical cyber-physical infrastructure so time delay greater than the allowed limits can cause severe impacts and can also lead to the instability of the system. In addition, an attacker can also generate FDI attacks on other communicated signals as well. Hence, in future

signatures of these distinct cyber attacks will be studied. The experimental results for the proposed decentralized anomaly identification mechanism on a DC microgrid system simulated in a real-time OPAL-RT environment is presented in the next section.

V. Experimental Result and Discussion

The proposed scheme has been tested and validated using real-time OP-5700 simulator [22] for DC microgrid operating at a voltage reference of 400 V with six DC/DC boost converters. These converters are rated equally for 30 kW with $L = 3mH$, $C = 250\mu F$. The line resistance R_{ij} ($R_{12} = 1\Omega$, $R_{23} = 2\Omega$, $R_{34} = 1\Omega$, $R_{45} = 2\Omega$, $R_{56} = 1\Omega$, $R_{61} = 2\Omega$, $R_{15} = 1.5\Omega$ and $R_{24} = 1.5\Omega$) connects i^{th} and j^{th} agent. The controller gains ($K_{pv} = 0.1$, $K_{iv} = 1$) are same for each agent. These boost converters are further rearranged in different network topologies such as ring and mesh to test the robustness of the proposed scheme.

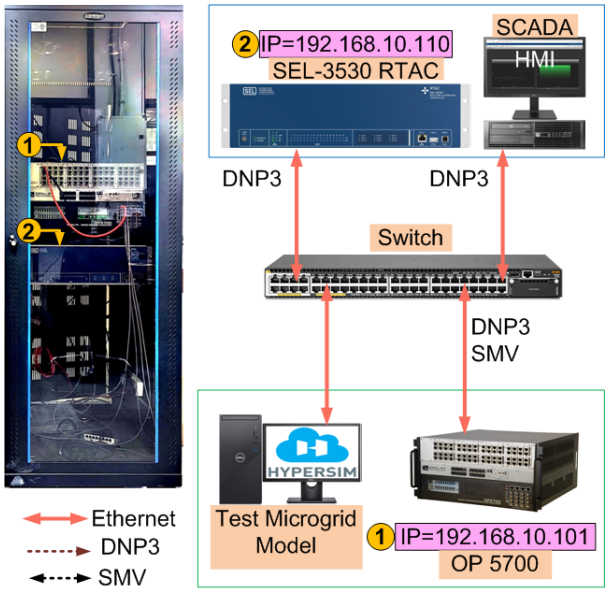

Fig. 4: Real-time co-simulation platform.

The change in voltage is $\delta V[k] = V[k] - V^{pre}$ and change in current is $\delta I[k] = I[k] - I^{pre}$. These deviations of voltages and currents are plotted on δI-δV plane. The trajectory of these deviations are studied to characterize the type of anomalous situation. It can be seen in the Fig. 5, that the trajectory traverses in cyber attack and fault regions indicating the presence of cyber and physical anomalies, respectively for various network topologies.

In addition, the proposed scheme has also been tested with cyber attack on multiple converters. The Fig. 6 shows that when cyber attack is initialted at agent 1 and 2 corresponding to converters 1 and 2, the proposed scheme is effective in localizing the anomalies as well along with identifying it. It shows that the scheme correctly identifies the anomaly as cyber anomaly and also localizes it to the agents 1 and 2.

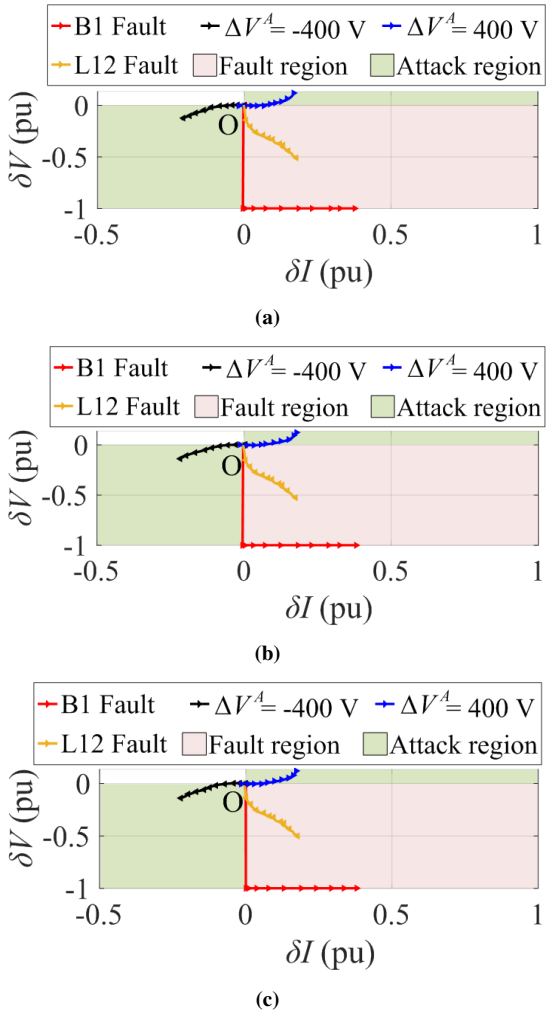

Fig. 5: Trajectories of δV w.r.t. δI in 5 ms at agent 1 for (**a**) radial; (**b**) ring; (**c**) mesh topology for cyber-physical anomalies. The fault and attack regions are shown by pink and green shaded portions, respectively.

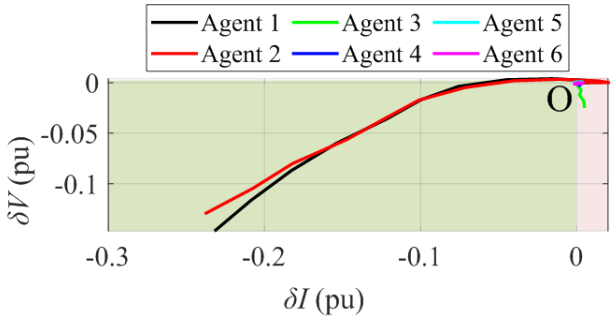

Fig. 6: Cyber attack on multiple converters (1 and 2) in a radial network.

Further, a comparison between the prior developed anomaly detection schemes is tabulated in the Table I. It shows that the proposed scheme is quite effective in identifying and localizing cyber and physical anomalies within 2 ms with low computational burden. It is simple and has no requirement of additional sensors making it scalable to distinct network configurations. The proposed scheme is decentralized hence

TABLE I: Comparative Evaluation of the Proposed Decentralized Anomaly Identification Mechanism for DC Microgrid.

Features	[2]	[13]	[14]	**This paper**
Decentralized concept	✗	✗	✓	✓
Anomaly classification	✓	✓	✓	✓
Anomaly localization	✗	✓	Not tested	✓
Decision time	Not specified	Not specified	100 ms	Within 2 ms
Computational complexity	High	High	Low	Low
Additional assets	Training data	Training data	✗	✗

depends only on the local measurements of voltage and current data.

VI. Conclusions and Future Work

In this work, a decentralized anomaly identification scheme for DC microgrid is proposed and validated for radial, ring and mesh network topologies. The proposed scheme utilizes only local V and I to characterize and locate the cyber and physical anomalies within 2 ms. It is computationally effective, has no requirement of additional sensors hence scalable to different network topologies. Moreover, this scheme is also effective in identifying and localizing anomalies during simultaneous attacks. The response and signatures of other cyber attacks like DoS, replay attacks will be studied as a future scope of this work.

References

[1] 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, April 2015, doi: 10.1109/TPEL.2014.2324579.

[2] O. A. Beg, L. V. Nguyen, T. T. Johnson and A. Davoudi, "Cyber-Physical Anomaly Detection in Microgrids Using Time-Frequency Logic Formalism," *IEEE Access*, vol. 9, pp. 20012-20021, 2021, doi: 10.1109/ACCESS.2021.3055229.

[3] K. Gupta, S. Sahoo, R. Mohanty, B. K. Panigrahi and F. Blaabjerg, "Decentralized Anomaly Characterization Certificates in Cyber-Physical Power Electronics Based Power Systems," 2021 *IEEE 22nd Workshop on Control and Modelling of Power Electronics (COMPEL)*, 2021, pp. 1-6, doi: 10.1109/COMPEL52922.2021.9645984.

[4] S. Augustine, M. J. Reno, S. M. Brahma and O. Lavrova, "Fault Current Control and Protection in a Standalone DC Microgrid Using Adaptive Droop and Current Derivative," *IEEE J. Emerg. Sel. Topics Power Electron.*, vol. 9, no. 3, pp. 2529-2539, June 2021, doi: 10.1109/JESTPE.2020.2984609.

[5] S. Beheshtaein, R. M. Cuzner, M. Forouzesh, M. Savaghebi and J. M. Guerrero, "DC Microgrid Protection: A Comprehensive Review," *IEEE J. Emerg. Sel. Topics Power Electron.*, doi: 10.1109/JESTPE.2019.2904588.

[6] D. Ye and T. -Y. Zhang, "Summation Detector for False Data-Injection Attack in Cyber-Physical Systems," *IEEE Trans. Cybern.*, vol. 50, no. 6, pp. 2338-2345, June 2020, doi: 10.1109/TCYB.2019.2915124.

[7] R. Mohanty and A. K. Pradhan, "Protection of Smart DC Microgrid With Ring Configuration Using Parameter Estimation Approach," *IEEE Trans. Smart Grid*, vol. 9, no. 6, pp. 6328-6337, Nov. 2018, doi: 10.1109/TSG.2017.2708743.

[8] N. K. Sharma, S. R. Samantaray and C. N. Bhende, "VMD-Enabled Current-Based Fast Fault Detection Scheme for DC Microgrid," *IEEE Syst. J.*, vol. 16, no. 1, pp. 933-944, March 2022, doi: 10.1109/JSYST.2021.3057334.

[9] R. Mohanty and A. K. Pradhan, "DC Ring Bus Microgrid Protection Using the Oscillation Frequency and Transient Power," *IEEE Syst. J.*, vol. 13, no. 1, pp. 875-884, March 2019, doi: 10.1109/JSYST.2018.2837748.

[10] K. A. Saleh, A. Hooshyar and E. F. El-Saadany, "Ultra-High-Speed Traveling-Wave-Based Protection Scheme for Medium-Voltage DC Microgrids," *IEEE Trans. Smart Grid*, vol. 10, no. 2, pp. 1440-1451, March 2019, doi: 10.1109/TSG.2017.2767552.

[11] S. Sahoo, J. C. -H. Peng, S. Mishra and T. Dragičević, "Distributed Screening of Hijacking Attacks in DC Microgrids," *IEEE Trans. Power Electron.*, vol. 35, no. 7, pp. 7574-7582, July 2020, doi: 10.1109/TPEL.2019.2957071.

[12] M. R. Habibi, S. Sahoo, S. Rivera, T. Dragičević and F. Blaabjerg, "Decentralized Coordinated Cyberattack Detection and Mitigation Strategy in DC Microgrids Based on Artificial Neural Networks," *IEEE J. Emerg. Sel. Topics Power Electron.*, vol. 9, no. 4, pp. 4629-4638, Aug. 2021, doi: 10.1109/JESTPE.2021.3050851.

[13] A. A. Khan, O. A. Beg, M. Alamaniotis, and S. Ahmed, "Intelligent anomaly identification in cyber-physical inverter-based systems," *Electric Power Systems Research*, vol. 193, p. 107024, 2021.

[14] S. Sahoo, J. C. Peng, A. Devakumar, S. Mishra and T. Dragičević, "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.

[15] R. Mohanty, S. Sahoo, A. K. Pradhan and F. Blaabjerg, "A Cosine Similarity-Based Centralized Protection Scheme for dc Microgrids," *IEEE J. Emerg. Sel. Topics Power Electron.*, vol. 9, no. 5, pp. 5646-5656, Oct. 2021, doi: 10.1109/JESTPE.2021.3060587.

[16] L. Kong and H. Nian, "Fault Detection and Location Method for Mesh-Type DC Microgrid Using Pearson Correlation Coefficient," *IEEE Trans. Power Del.*, vol. 36, no. 3, pp. 1428-1439, June 2021, doi: 10.1109/TPWRD.2020.3008924.

[17] M. S. Sadabadi, S. Sahoo and F. Blaabjerg, "Stability-Oriented Design of Cyberattack-Resilient Controllers for Cooperative DC Microgrids," *IEEE Trans. Power Electron.*, vol. 37, no. 2, pp. 1310-1321, Feb. 2022, doi: 10.1109/TPEL.2021.3104721.

[18] S. Sahoo, T. Dragičević and F. Blaabjerg, "Multilayer Resilience Paradigm Against Cyber Attacks in DC Microgrids," *IEEE Trans. Power Electron.*, vol. 36, no. 3, pp. 2522-2532, March 2021, doi: 10.1109/TPEL.2020.3014258.

[19] S. Zuo, T. Altun, F. L. Lewis and A. Davoudi, "Distributed Resilient Secondary Control of DC Microgrids Against Unbounded Attacks," *IEEE Trans. Smart Grid*, vol. 11, no. 5, pp. 3850-3859, Sept. 2020, doi: 10.1109/TSG.2020.2992118.

[20] M. Leng, S. Sahoo, F. Blaabjerg and M. Molinas, "Projections of Cyber Attacks on Stability of DC Microgrids - Modeling Principles and Solution," *IEEE Trans. Power Electron.*, 2022, doi: 10.1109/TPEL.2022.3175237.

[21] U. Vuyyuru, S. Maiti, C. Chakraborty and B. C. Pal, "A Series Voltage Regulator for the Radial DC Microgrid," *IEEE Trans. Sustain. Energy*, vol. 10, no. 1, pp. 127-136, Jan. 2019, doi: 10.1109/TSTE.2018.2828164.

[22] K. Gupta, S. Sahoo, B. K. Panigrahi, F. Blaabjerg, and P. Popovski, "On the Assessment of Cyber Risks and Attack Surfaces in a Real-Time Co-Simulation Cybersecurity Testbed for Inverter-Based Microgrids," *Energies*, vol. 14, no. 16, p. 4941, 2021. [Online]. Available: https://www.mdpi.com/1996-1073/14/16/4941.