Electrical Power and Energy Systems 120 (2020) 105968

Contents lists available at ScienceDirect

Electrical Power and Energy Systems

journal homepage: www.elsevier.com/locate/ijepes

Detection and mitigation of cyber-threats in the DC microgrid distributed control system

Binod P. Poudel[a], Aquib Mustafa[b], Ali Bidram[a,*], Hamidreza Modares[b]

[a] Department of Electrical and Computer Engineering, the University of New Mexico, Albuquerque, NM, 87131, United States
[b] Department of Mechanical Engineering, Michigan State University, East Lansing, MI 48823, United States

ARTICLE INFO

Keywords:
Cyber-security
DC microgrids
Distributed control
Kullback-Liebler divergence
Voltage regulation

ABSTRACT

This paper addresses the cyber-threat detection and mitigation in a DC microgrid distributed control system. Due to the deployment of communication and control technologies, a DC microgrid resembles a cyber-physical system that is highly exposed to cyber-threats. A cyber-threat detection technique is proposed that relies on a Kullback-Liebler divergence-based criterion. This criterion detects the misbehavior of a compromised Distributed Energy Resource (DER) control unit and, consequently, calculates an interior-belief factor and communicates it with its neighboring DERs to inform them of the reliability of its outgoing information. Moreover, DERs calculate an exterior-belief value related to the trustworthiness of the received information from neighbors. The cyber-threat mitigation technique at each DER utilizes the neighbors' interior-belief and its own calculated exterior-belief value for neighboring DERs to slow down and eventually mitigate attacks. The proposed approach requires a communication network with mild graph connectivity. A typical medium-voltage DC microgrid system is simulated to verify the validity of proposed distributed cyber-secure control scheme. It is shown that using the proposed cyber-secure approach, the voltage of a critical bus of microgrid is well regulated and DERs can successfully distinguish cyber-attacks from legitimate events.

1. Introduction

Microgrids as autonomous and controllable small-scale power systems can operate in grid-connected and islanded modes of operation and play an important role in increasing the resilience of critical power infrastructure [1]. Microgrids can be of two main types of AC and DC. DC microgrids have gained much attention recently due to the increased efficiency compared to AC microgrids in delivering power and flexibility for the integration of power sources with DC nature (e.g., photovoltaic and battery energy storage systems). Similar to AC microgrids, DC microgrids utilize a hierarchical control structure including primary, secondary, and tertiary control levels. Primary control conventionally utilizes local droop controllers on DERs to maintain microgrid voltage stability after the islanding. Secondary control deals with the DC microgrid voltage regulation specially after the primary control acts and microgrid voltage level slightly drops. Tertiary control manages the optimal operation of microgrid and the power flow between microgrid and upstream grid in the grid connected mode [2–6]. As one of the major control objectives in DC microgrids, proper voltage regulation while satisfying the proportional power sharing among DERs is of paramount value. The proportional power sharing denotes the power allocation among DERs based on their converter's current ratings and availability of power [7–13]. Voltage regulation can be defined from different point of views. One can refer the voltage regulation objective as to synchronizing the average voltage of DC microgrid to the nominal voltage of microgrid [8]. However, considering the distinct goal of microgrids to increase grid resilience and provide continuous high-quality power support for critical loads, this paper defines the voltage regulation objective as controlling the voltage magnitude at critical buses that serve as microgrid critical loads.

The secondary control of DC microgrid can be implemented through a centralized structure. In this structure, the microgrid central control, located at the control center, is responsible for calculating and sending the voltage and power setpoints to the individual DERs [9]. However, this control structure has a reliability bottleneck which is the single-point-of-failure at the control center. Alternatively, distributed control architecture has been proposed more recently to increase microgrid control system reliability, scalability, and resilience [14–18]. Similar to other cyber-physical systems, distributed voltage regulation of DC microgrids utilizes nested communication and control platforms which highly expose the system to cyber-threats and malicious adversaries. False Data Injection (FDI) attacks target the sensors and control and

* Corresponding author.
E-mail address: bidram@unm.edu (A. Bidram).

https://doi.org/10.1016/j.ijepes.2020.105968
Received 17 August 2019; Received in revised form 7 January 2020; Accepted 24 February 2020

decision-making units which in turn corrupt the data transferred through the communication links and impact the microgrid data integrity [19]. Denial-of-Service (DoS) attacks endanger the availability of communication system services [20]. In this paper, FDI attacks are of concern.

The FDI attacks in smart grids have been investigated in [21–23] where state estimation has been utilized to detect compromised data in Supervisory Control and Data Acquisition (SCADA) or smart grid control system. In [24], an adaptive cusum method is used for FDI attack detection in smart grids. FDI attack detection using Kalman filter, state vectors, graphical methods, model-based techniques, and sparse optimization is addressed in [25–29]. In [30], a sensor fault detection and mitigation scheme for DC microgrids with a centralized control structure is proposed. However, all of these techniques address FDI attack detection in the centralized communication networks. The FDI attack detection in distributed control systems is addressed in [31,32]. In [33–35], noise-resilient microgrid control protocols are proposed. However, these references only focus on the frequency and voltage control of AC microgrids. Moreover, they don't consider attack detection and mitigation. In [36], an observer-based control protocol is proposed to mitigate the impact of cyber-attacks on the distributed voltage regulation of DC microgrids. However, the proposed resilient protocol is not associated with an attack detection scheme and ignores stochastic uncertainties that come with the communication noise. The literate review highlights the requirement for a comprehensive attack resilient control that simultaneously

- facilitates the proper voltage regulation of *DC microgrids*,
- handles FDI attacks on the *distributed control systems*,
- accommodates both FDI attack *detection* and *mitigation* mechanisms,
- accounts for the stochastic uncertainties associated with the communication noise during attack detection and mitigation.

To this end, this paper proposes a resilient distributed secondary control for DC microgrids that accommodates FDI attacks detection and mitigation and accounts for the stochastic uncertainties associated with the communication noise.

The proposed DC microgrid secondary control scheme controls the voltage of a critical bus of DC microgrid and ensures that DERs' power contributions are based on their current ratings. The attack detection technique deploys Kullback-Liebler (KL) divergence to measure the discrepancy between the Gaussian distributions of the actual and expected local voltage and power ratio neighborhood tracking errors. To mitigate the negative impact of cyber-attack, an interior-belief, as an indication of the probability that each DER is affected by an attack is proposed by utilizing the KL-divergence value. The interior-belief value is a measure of trustworthiness of the agent's own outgoing information and is transmitted to neighboring DERs. Moreover, the trustworthiness of the incoming information from neighboring DERs is estimated using an exterior-belief. An exterior-belief between each DER and one of its neighbors is developed based on the relative entropy between DER own information and its neighbor's information. The attack mitigation technique utilizes interior and exterior-belief values to modify distributed control protocols for slowing down the spread of attacks. Since the proposed scheme only relies on the difference between the entropy of the actual and expected data using KL divergence, it can cover a wide range of FDI attacks independent of their dynamics.

This paper makes the following contributions:

- A comprehensive attack *detection* and *mitigation* scheme for DC microgrids is proposed.
- The proposed scheme accounts for the stochastic uncertainties associated with the communication noise. To this end, this paper presents a novel KL-divergence measure for distributed voltage regulation of DC microgrids.

The rest of paper is organized as follows: Section 2 provides some preliminaries on graph theory. Section 3 discusses the distributed voltage regulation protocol. Section 4 discusses the proposed attack modeling and detection mechanism. The attack mitigation technique is discussed in Section 5. The proposed cyber-secure voltage regulation protocol is verified through the simulation of a medium voltage DC microgrid test system in Section 6. Section 7 concludes the paper.

2. Preliminaries on graph theory

The distributed communication network of a DC microgrid is modeled by a graph with DERs as graph nodes and communication links as graph edges. A graph $\mathcal{G} = (\mathcal{V}, \mathcal{E}, \mathcal{A})$ incorporates a nonempty finite set of N nodes $\mathcal{V} = \{v_1, v_2, ..., v_N\}$, a set of edges or arcs $\mathcal{E} \subset \mathcal{V} \times \mathcal{V}$, and the associated adjacency matrix $\mathcal{A} = [a_{ij}] \in \mathbb{R}^{N\times N}$ which describes the connectivity among nodes. If there is an edge from node j to node i (v_j, v_i), then node i receives information from node j as the neighboring node. Each element of adjacency matrix, a_{ij}, denotes the weight of edge (v_j, v_i). The set of neighbors of node i is denoted as $N_i = \{j|(v_j, v_i) \in \mathcal{E}\}$. The in-degree matrix is defined as $\mathcal{D} = diag\{d_i\} \in \mathbb{R}^{N\times N}$ with $d_i = \sum_{j\in N_i} a_{ij}$. The Laplacian matrix is defined as $\mathcal{L} = \mathcal{D} - \mathcal{A}$ [37].

3. Distributed voltage regulation protocol

In this section, first, the DER model in a DC microgrid is discussed. Then, the distributed voltage regulation is proposed.

3.1. DER model in a DC microgrid

The block diagram of a DER in a DC microgrid is shown in Fig. 1. DC microgrids facilitate the smooth integration of power sources with DC nature (e.g., photovoltaic or battery energy storage systems) through DC-DC converters. DER converters are operated through the nested droop and voltage controllers as seen in Fig. 1. The droop controller prescribes a relationship between DER terminal voltage, v_o, and its output current, i_o. This technique facilitates the voltage stability in the microgrid by sharing power among DERs based on the converters' current ratings. The conventional DC droop technique is [38–40]

$$v_o^* = V_n - r_d i_o, \tag{1}$$

where v^*_o is the DC-DC converter voltage reference; V_n is the droop reference; r_d is the droop coefficient that represents a virtual resistance for the DER. The voltage reference, v^*_o, is a control input to the internal voltage controller in Fig. 1 which calculates the required duty cycle for the DC-DC converter to regulate DER output voltage to v^*_o. The droop coefficients are chosen based on the converter current ratings satisfying

$$r_{d1} i_{1,\max} = \cdots = r_{dN} i_{N,\max}, \tag{2}$$

where $i_{k,\max}$ denotes the current rating of k^{th} DER. Eq. (2) ensures that

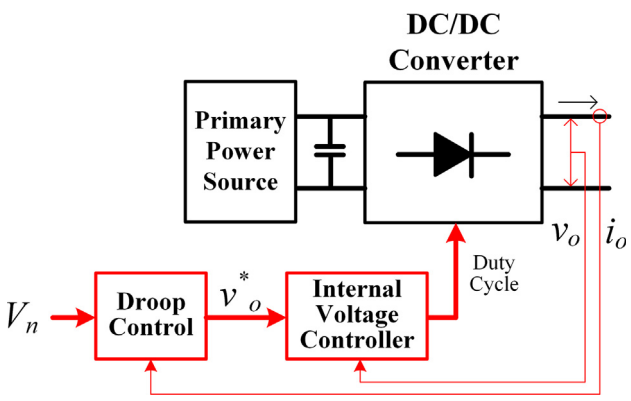

Fig. 1. DER model in a DC microgrid.

in a DC microgrid with small line resistances the DER output currents are proportionally shared based on their current ratings, i.e.,

$$\frac{i_{o1}}{i_{1,\max}} = \cdots = \frac{i_{oN}}{i_{N,\max}}. \tag{3}$$

Moreover, to guarantee that the voltage at the terminal of DC-DC converters does not violate the maximum acceptable deviation limit, the droop coefficients are limited by

$$r_{dk} \leqslant \frac{\Delta v_{k,\max}}{i_{k,\max}}, \tag{4}$$

where $\Delta v_{k,\max}$ is the maximum allowable terminal voltage deviation at k^{th} DER.

3.2. Distributed voltage regulation

The droop control of DERs can effectively maintain the voltage of microgrid in a stable range. However, the microgrid voltage is slightly deviated from the nominal voltage after the droop control takes action. In a DC microgrid with critical loads, it is imperative to regulate the voltage at the critical buses. This crucial task is performed by voltage regulation framework. This paper proposes a distributed voltage regulation scheme which is shown in Fig. 2. As seen, the voltage regulation framework utilizes distributed control protocols on all DERs that can communicate with each other through a distributed communication network. The objective of this section is to design these distributed control protocols such that the voltage of a critical bus of microgrid is regulated at a reference voltage and the DERs' current contributions follow the same pattern as the droop control as shown in (3).

In the proposed voltage regulation framework, a PI controller is used to create a leading voltage, v_{leader}, as

$$v_{leader} = k_p(v_{ref} - v_{crit}) + k_i \int (v_{ref} - v_{crit})dt, \tag{5}$$

where v_{ref} is the microgrid reference voltage determined by distribution system operator supervising the DC microgrid. v_{crit} is the voltage of critical bus of microgrid. k_p and k_i are the PI control parameters. The leading voltage, v_{leader}, is only required to be shared with one of the DERs acting as the leader node on the distributed communication graph.

The distributed voltage regulation protocols at DERs determine the droop references, V_n in (1). These distributed control protocols, shown in Fig. 3, are derived by transforming the microgrid dynamics to a first order multiagent system. For example, for k^{th} DER, this is achieved by differentiating two sides of droop technique as

$$\frac{d}{dt}(V_{nk}) = \frac{d}{dt}(v_{ok}^{*}) + r_{dk} i_{k,\max} \frac{d}{dt}(i_{k,\text{ratio}}), \tag{6}$$

where $i_{k,\text{ratio}}$ denotes the current ratio at k^{th} DER and can be formulated as

$$i_{k,\text{ratio}} = \frac{i_{ok}}{i_{k,\max}}. \tag{7}$$

Using (6), the droop reference for k^{th} DER is build up based on the voltage and current ratio local neighborhood tracking errors as

$$V_{nk} = \int u_{vk} dt, \tag{8}$$

where

$$u_{vk} = C_k(\delta_{vk} + \delta_{ik}), \tag{9}$$

$$\delta_{vk} = \sum_{j \in N_k} a_{kj}(v_{oj} - v_{ok}) + g_k(v_{leader} - v_{ok}), \tag{10}$$

$$\delta_{ik} = \sum_{j \in N_k} a_{kj} r_{dk} i_{k,\max}(i_{j,\text{ratio}} - i_{k,\text{ratio}}), \tag{11}$$

where a_{kj} denotes the elements of the communication graph adjacency matrix. C_k is a fixed control gain. It is assumed that the pinning gain $g_k \geqslant 0$ is nonzero for only one DER that receives the leading voltage information from microgrid control center. The term u_{vk} is defined as an auxiliary control input.

4. Attack modeling and detection

This section presents attack modeling and detection mechanism for the proposed distributed voltage regulation protocol. Attacks can be classified into two main categories: attacks on controller, FDI attacks, and attacks on communication channels, DoS attacks. FDI attacks can be launched by injecting counterfeit signals into DER measurements or tampering the DER control and decision-making unit by manipulating control parameters or protocols. FDI attacks can simply gain access to the DER control and decision-making units through the communication ports and tamper the algorithms and functionalities of these devices to cause a major catastrophe in microgrid. A DoS attack on communication channel can be launched by generating high-amplitude and wide-bandwidth signals to interfere with the original signal before it reaches its neighboring DER, or by blocking the communication channel and preventing transmission of the original signal. However, in a distributed communication network, the remaining communication links can still provide voltage regulation as far as the communication graph is connected. In this paper, FDI attacks are considered. No restriction is

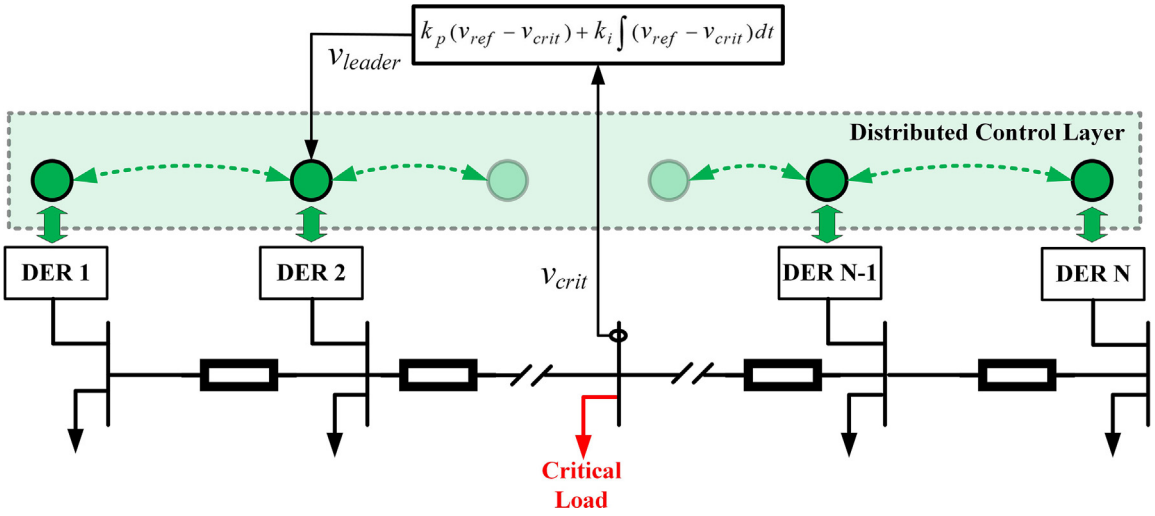

Fig. 2. Distributed voltage regulation framework.

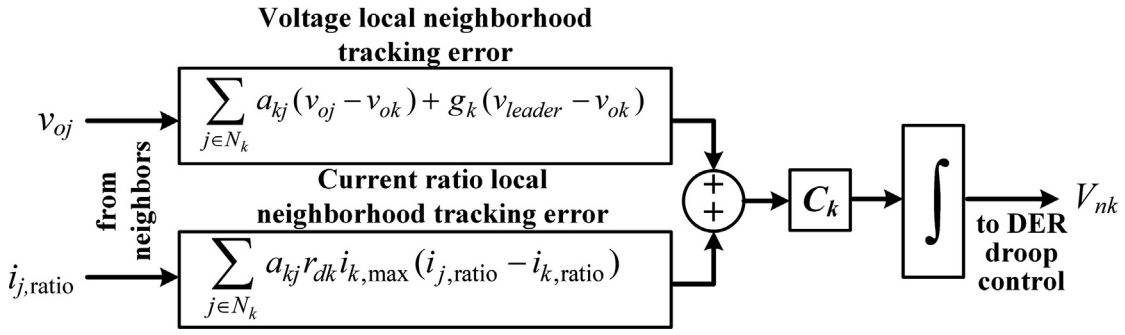

Fig. 3. Distributed voltage regulation protocol at k^{th} DER.

imposed on attack signal.

4.1. Attack detection technique

This subsection presents a relative entropy-based attack detection approach for the distributed voltage regulation of DC microgrids. More specifically, KL divergence, a non-negative measure of the relative entropy between two probability distributions is employed to measure the discrepancy between them.

Definition 1. (*KL divergence*) *[41,42]*). Let X and Z be two random sequences with probability density function $P_X$and P_Z, respectively. The KL divergence measure between P_X and P_Z in continuous-time is defined as

$$D_{KL}(X||Z) = \int P_X(\theta)\log\left(\frac{P_X(\theta)}{P_Z(\theta)}\right)d\theta, \tag{12}$$

with the following properties [41]:

1. $D_{KL}(P_X||P_z) \geqslant 0$,
2. $D_{KL}(P_X||P_z) = 0$, if and only if $P_X = P_z$,
3. $D_{KL}(P_X||P_z) \neq D_{KL}(P_z||P_X)$.

If the sequences X and Z are Gaussian distributed, then the KL divergence in (12) can be simplified in the terms of mean and covariance of sequences as [43]

$$D_{KL}(X||Z) = \frac{1}{2}\left(\log\frac{|\Sigma_Z|}{|\Sigma_X|} - n + tr(\Sigma_Z^{-1}\Sigma_X)\right) + \frac{1}{2}(\mu_Z-\mu_X)^T\Sigma_Z^{-1}(\mu_Z-\mu_X), \tag{13}$$

where μ_X and Σ_X denote the mean and covariance of sequence X, and μ_Z and Σ_Z denote the mean and covariance of sequence Z. Moreover, n denotes the dimension of the sequences [43].

It is assumed that there always exists a low-level communication noise in the distributed communication network of DERs. Therefore, in the presence of the communication noise, one can write the auxiliary control u_{vk} of k^{th} DER as

$$\zeta_{vk} = u_{vk} + \eta_{vk}, \tag{14}$$

where $\eta_{vk}\sim\mathcal{N}(0, \Sigma_{v_k})$ denotes the aggregate Gaussian noise with mean 0 and covariance Σ_{v_k} affecting the incoming neighbors' voltage and current ratio to k^{th} DER. In noisy scenarios, although DERs cannot reach exact synchronization, the expected value of the synchronization error converges to zero with a variance depending on the variance of η_{vk} (i.e., it depends on the statistical properties of the noise).

To design the attack detector, first, the auxiliary control ζ_{vk} in (14) is rewritten with statistical properties and then a novel attack detection mechanism based on KL divergence measure for distributed voltage regulation of DC microgrid is presented. It is shown that in the presence of attack, one can identify different sophisticated attacks based on the change in the statistical properties of the auxiliary control variables as functions of local neighborhood tracking errors.

The communication channels are corrupted by some additive noise. In this paper, it is assumed that the communication noise to be zero mean white Gaussian which is a standard assumption in the literature. The noise associated with electronic devices at the receiver end lies under the category of thermal noise and statistically modeled as Gaussian. Similarly, the communication channel noise which is generated by the receiver front end and surrounding noise can be modeled as an additive Gaussian function [33]. In the absence of attack, since we consider the Gaussian noise in the communication channel, i.e., $\eta_{vk}\sim\mathcal{N}(0, \Sigma_{v_k})$, then auxiliary control ζ_{vk} in (14) can be written as

$$\zeta_{vk} = C_k(\delta_{vk} + \delta_{ik}) + \eta_{vk}, \tag{15}$$

with δ_{vk} and δ_{ik} defined in (10) and (11).

In the presence of attacks, the auxiliary control in (14) is denoted as ζ^a_{vk} and can be written as

$$\zeta^a_{vk} = C_k(\delta_{vk} + \delta_{ik}) + \eta_{vk} + f_k, \tag{16}$$

where f_k denotes the overall deviation in the auxiliary control protocol due to the attacks on the DER controller. From (16), one has the following statistical properties

$$\zeta^a_{vk}\sim\mathcal{N}(\mu_{f_k}, \Sigma_{f_k} + \Sigma_{v_k}), \tag{17}$$

where μ_{f_k} and Σ_{f_k} are mean and covariance of the injected overall attack signal f_k, respectively.Now, since both ζ^a_{vk} and ζ_{vk} have normal Gaussian distributions, then according to (13) the KL divergence $D_{\text{KL}}(\zeta^a_{vk}||\zeta_{vk})$ between control sequences ζ^a_{vk} and ζ_{vk} becomes [43]

$$D_{KL}(\zeta^a_{vk}||\zeta_{vk}) = \frac{1}{2}\left(\log\frac{|\Sigma_{\zeta_{vk}}|}{|\Sigma_{\zeta^a_{vk}}|} - 1 + tr\left(\Sigma^{-1}_{\zeta_{vk}}\Sigma_{\zeta^a_{vk}}\right)\right) + \frac{1}{2}\left(\mu_{\zeta_{vk}} - \mu_{\zeta^a_{vk}}\right)^T\Sigma^{-1}_{\zeta_{vk}}\left(\mu_{\zeta_{vk}} - \mu_{\zeta^a_{vk}}\right), \tag{18}$$

where $\mu_{\zeta_{vk}}$ and $\Sigma_{\zeta_{vk}}$ denote the mean and covariance of ζ_{vk} and $\mu_{\zeta^a_{vk}}$ and $\Sigma_{\zeta^a_{vk}}$ denote the mean and covariance of ζ^a_{vk}.

The average of KL divergence over a window with the length of T is defined as

$$\Omega_m = \frac{1}{T}\int_m^{m+T-1} D_{KL}(\zeta^a_{vk}||\zeta_{vk})dk \tag{19}$$

to detect the change due to adversarial input. In the following theorem, it is shown that the effect of attack in a distributed microgrid can be detected based on the control sequences ζ^a_{vk} and ζ_{vk}.

Theorem 1.. *In a DC microgrid control system, for each DER,*

(a) Ω_m *in* (19) *becomes zero, if there is no attack on the microgrid distributed control system;*
(b) Ω_m *defined in* (19) *is greater than a predefined threshold* θ_1, *if the DER control unit is subject to an FDI attack.*

Proof.. In the absence of attacks, the statistical properties of sequences ζ^a_{vk} and ζ_{vk}, respectively, in (15) and (16) are the same because μ_{f_k} and Σ_{f_k} become zero as $f_k = 0$. Therefore, the KL divergence $D_{KL}(\zeta^a_{vk}||\zeta_{vk})$ in

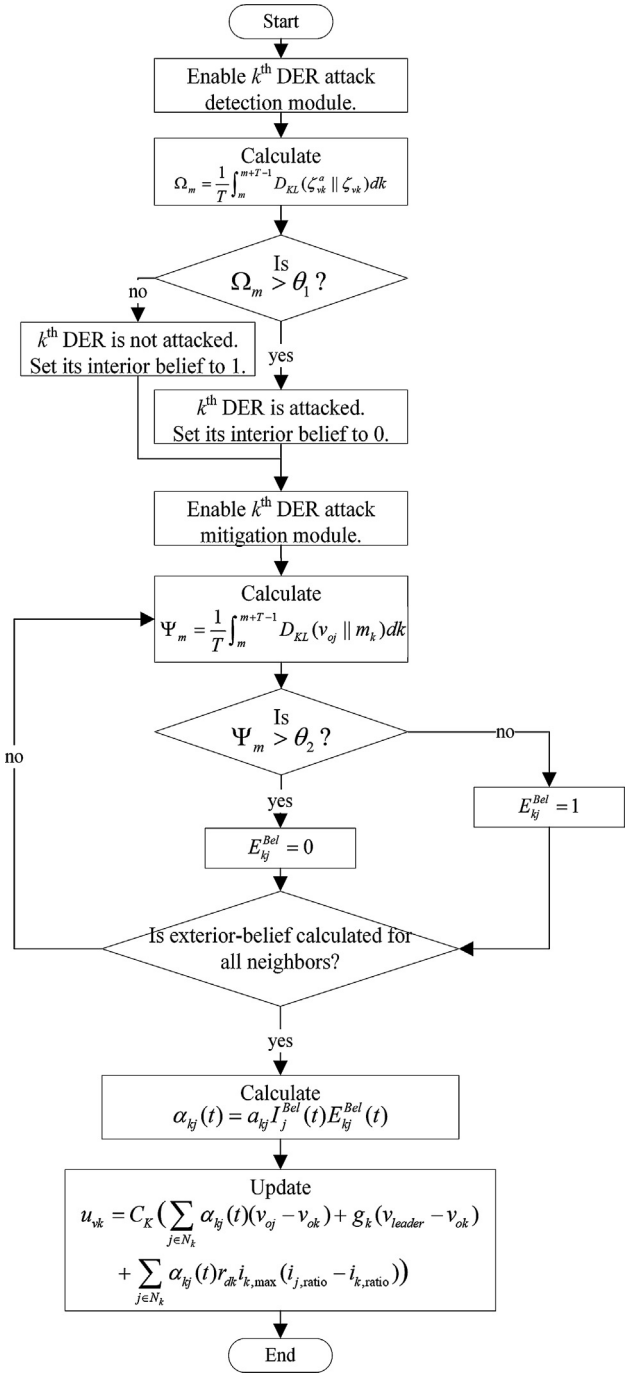

Fig. 4. Attack detection and mitigation mechanism.

(18) becomes zero based on (13) which yields Ω_i in (19) to be zero. This completes the proof of part (a).

For the proof of Part (b), using (16) and (17) in (18), the KL divergence between ζ_{vk}^a and ζ_{vk} becomes

$$D_{KL}(\zeta_{vk}^a \| \zeta_{vk}) = \frac{1}{2}\left(\log \frac{|\Sigma_{v_k}|}{|\Sigma_{f_k} + \Sigma_{v_k}|} + tr\left(\Sigma_{v_k}^{-1}\Sigma_{f_k}\right) + \mu_{f_k}^T \Sigma_{v_k}^{-1}\mu_{f_k}\right). \tag{20}$$

Then, using (19), one has

$$\Omega_k = \frac{1}{T}\int_k^{k+T-1} \frac{1}{2}\left(\log \frac{|\Sigma_{v_k}|}{|\Sigma_{f_k} + \Sigma_{v_k}|} + tr\left(\Sigma_{v_k}^{-1}\Sigma_{f_k}\right) + \mu_{f_k}^T \Sigma_{v_k}^{-1}\mu_{f_k}\right) > \theta_1, \tag{21}$$

where T and θ_1 denote the sliding window size and the predefined positive design threshold, respectively. This completes the proof.

Remark 1.. Once the microgrid distributed control system experiences an FDI attack, the average KL divergence at each individual DER starts to deviate from zero. This deviation can be used to identify a possible attack in the microgrid control system. If a DER is directly exposed to the FDI attack, its average KL divergence experiences much larger deviations than the other DERs. The DERs that are farther to the source of attack experience a lower average KL divergence value. Comparing Ω_m in (19) against the threshold θ_1, one can identify if a DER is directly under FDI attack.

5. Attack mitigation technique

This section presents the cyber-secure distributed voltage regulation technique for DC microgrids based on the proposed attack detection algorithm in the previous section. To this end, first we introduce the notion of interior and exterior belief of DERs about their own information and neighbor's information, respectively. Then the presented beliefs are incorporated in the distributed voltage regulation protocols.

5.1. Belief of DERs about their own measured voltage

To measure the level of trustworthiness of each DER about its own measured voltage or the voltage value that is transmitted to the neighboring DERs, an interior-belief is presented. In the presence of attack, a DER reduces its level of trustworthiness about its own measured voltage and informs its immediate neighbors about its interior-belief which prevents the propagation of attack in the microgrid.

Using Ω_m in (19) and the threshold θ_1, the interior-belief of k^{th} DER about its own measured voltage is defined as

$$I_k^{Bel}(t) = \begin{cases} 1, & \text{if } D_{KL}(\zeta_{vk}^a \| \zeta_{vk}) < \theta_1 \\ 0, & \text{if } D_{KL}(\zeta_{vk}^a \| \zeta_{vk}) > \theta_1 \end{cases}, \tag{22}$$

where $I_k^{Bel}(t)$ is the interior-belief of k^{th} DER. As discussed earlier, if Ω_m is greater than θ_1, then a DER is directly under FDI attack. Under this condition the interior-belief of DER is forced to zero.

5.2. Belief of DERs about their Neighbor's measured voltage

To evaluate the level of confidence of a DER on its neighbor's measured voltage, we introduce the notion of exterior-belief. Exterior-belief depends on the DER belief on each of its neighbors using only locally available information. Using exterior-belief, the DERs can identify the compromised neighbor and discard its information in their control protocol. In the worst-case scenario, a compromised DER may always transmit an interior-belief value of 1 to its neighbors to deceive them. However, neighboring DERs can identify the corrupted DER based on the exterior-belief values and discard the corrupted DER information. Using the KL divergence between exchanged information of the k^{th} DER and its neighbor, one can define the measure Ψ_m to identify the compromised neighboring DERs as

$$\Psi_m = \frac{1}{T}\int_m^{m+T-1} D_{KL}(v_{oj} \| m_k)dk, \tag{23}$$

where $m_k = \frac{1}{n(N_k)}\sum_{j\in N_k} v_{oj}$ with $n(N_k)$ as the number of DER's neighbors. For the neighboring DER under direct attack, the KL divergence $D_{KL}(v_{oj} \| m_k)$ becomes very high and exceeds a threshold θ_2. Using this threshold value, the exterior-belief $E_{kj}(t)$ is defined as

$$E_{kj}(t) = \begin{cases} 0, & \text{if } D_{KL}(v_{oj} \| m_k) > \theta_2 \\ 1, & \text{if } D_{KL}(v_{oj} \| m_k) < \theta_2 \end{cases}. \tag{24}$$

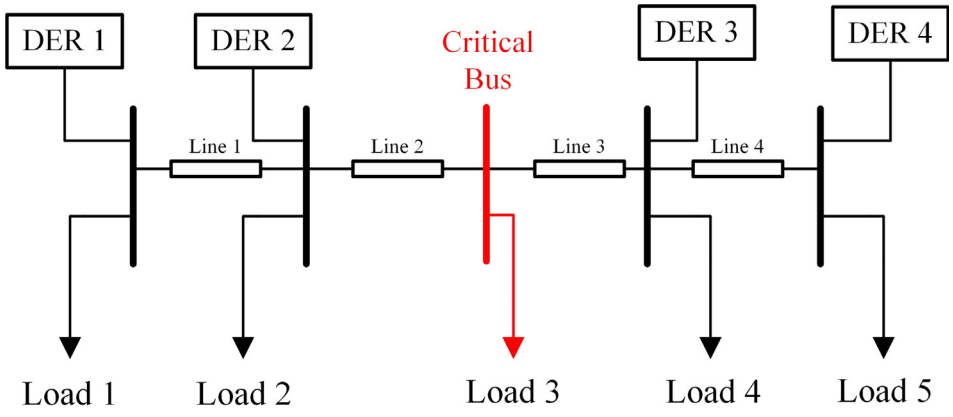

Fig. 5. Single line diagram of 4-DER microgrid test system.

Table 1
Specification of DERs.

	DER1	DER2	DER3	DER4
Nominal Output voltage (V)	1500	1500	1500	1500
Nominal Output current (A)	40	20	20	40
Nominal power (kW)	60	30	30	60

Table 2
Specification of Loads.

Load 1 (Ω)		Load 2 (Ω)		Load 3 (Ω)		Load 4 (Ω)		Load 5 (Ω)	
R	150	*R*	150	*R*	112.5	*R*	150	*R*	150

Table 3
Specification of Lines.

Line 1 (Ω)		Line 2 (Ω)		Line 3 (Ω)		Line 4 (Ω)	
R	0.427	*R*	0.8538	*R*	0.8538	*R*	0.427

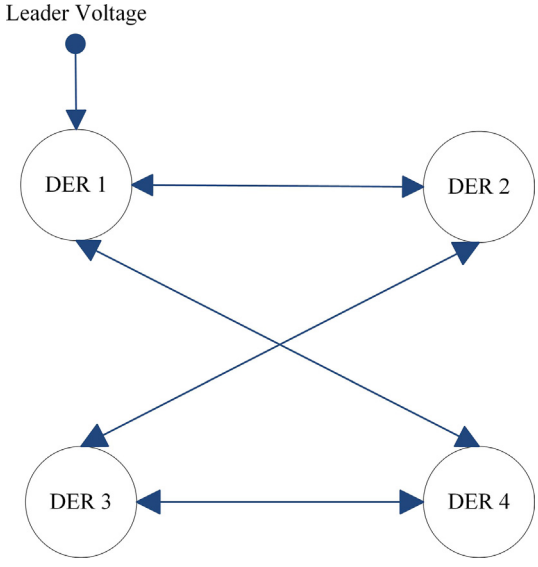

Fig. 6. Communication graph of 4-DER microgrid test system.

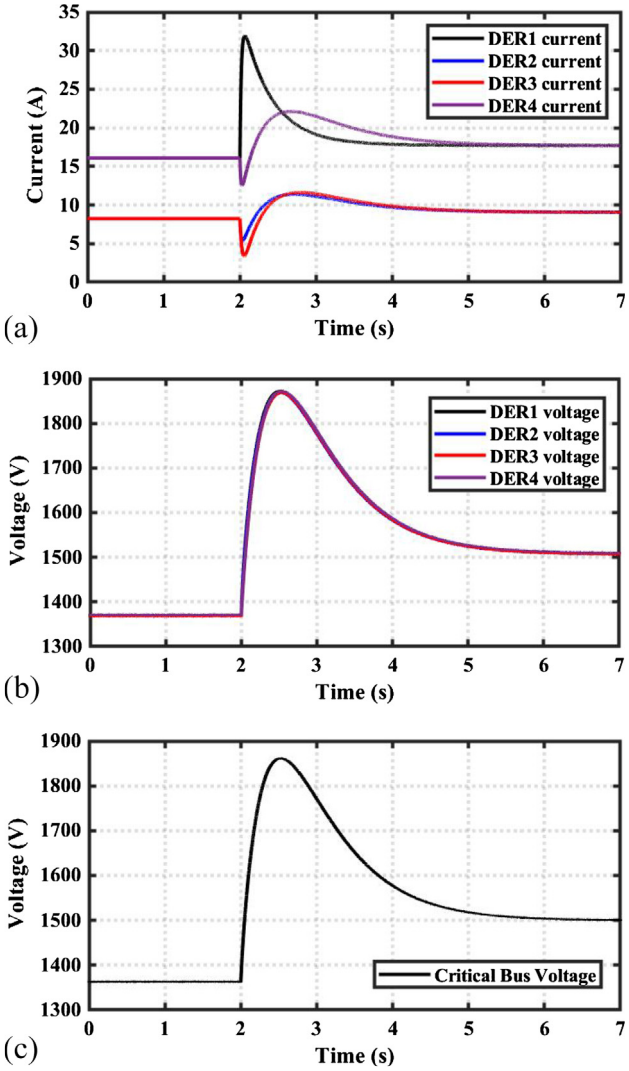

Fig. 7. 4-DER Microgrid distributed voltage regulation without cyber-attack: (a) DERs' output current; (b) DERs' terminal voltage magnitude; (c) critical bus voltage.

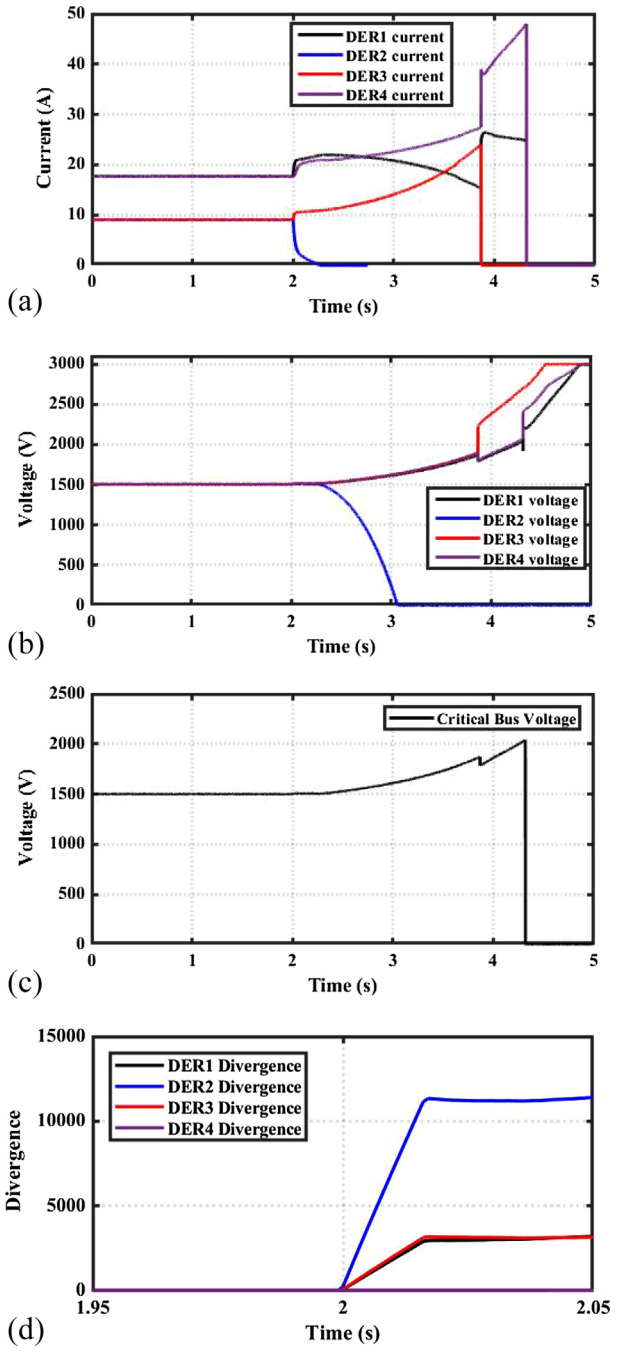

Fig. 8. 4-DER Microgrid distributed voltage regulation with cyber-attack: (a) DERs' output current; (b) DERs' terminal voltage magnitude; (c) critical bus voltage; (d) average KL divergence for each DER.

5.3. The mitigation mechanism using interior and Exterior-belief values

In Fig. 4, the proposed FDI attack mitigation and detection scheme for distributed voltage regulation of DC microgrids is illustrated. Both interior and exterior-belief values in (22) and (24) are incorporated to update the auxiliary control in (9) as

$$u_{vk} = C_K\Big(\sum_{j\in N_k}\alpha_{kj}(t)(v_{oj}-v_{ok}) + g_k(v_{leader}-v_{ok}) + \sum_{j\in N_k}\alpha_{kj}(t)r_{dk}i_{k,\max}(i_{j,\text{ratio}}-i_{k,\text{ratio}})\Big), \quad (25)$$

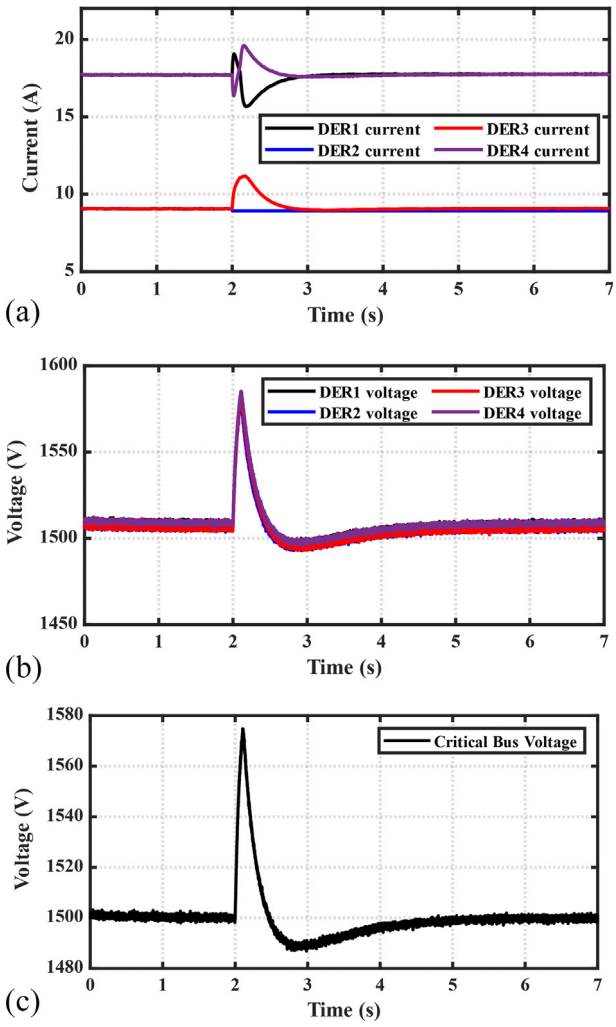

Fig. 9. 4-DER Microgrid distributed voltage regulation equipped with cyber-attack detection and mitigation: (a) DERs' output current; (b) DERs' terminal voltage magnitude; (c) critical bus voltage.

where $\alpha_{kj}(t) = a_{kj}I_j^{Bel}(t)E_{kj}^{Bel}(t)$ which incorporates the received interior-belief from j^{th} DER and locally calculated exterior-belief for j^{th} DER. The term $\alpha_{kj}(t)$ prevents the flow of information from attacked DERs to healthy ones and has a critical role for slowing down the spread of cyber-attack impact in the distributed communication network.

Remark 2.. The proposed attack detection and mitigation schemes are formulated for the attacks affecting the DER voltage measurements. Without loss of generality, similar formulation can be developed for interior and exterior-belief values corresponding to DER current ratios.

6. Simulation results

In the following, the simulation results are provided for two different MVDC microgrids to show the scalability of the proposed attack detection and mitigation scheme.

6.1. Simulation results for a 4-DER MVDC microgrid

The single line diagram of 4-DER MVDC microgrid system is shown in Fig. 5. Herein, an MVDC system is utilized since MVDC microgrids have gained much attention in shipboard power systems. The MVDC microgrid shown in Fig. 5 is built to replicate a typical MVDC ship power system. Load and generator values are selected accordingly [44]. This DC microgrid system is simulated in MATLAB/Simulink. The

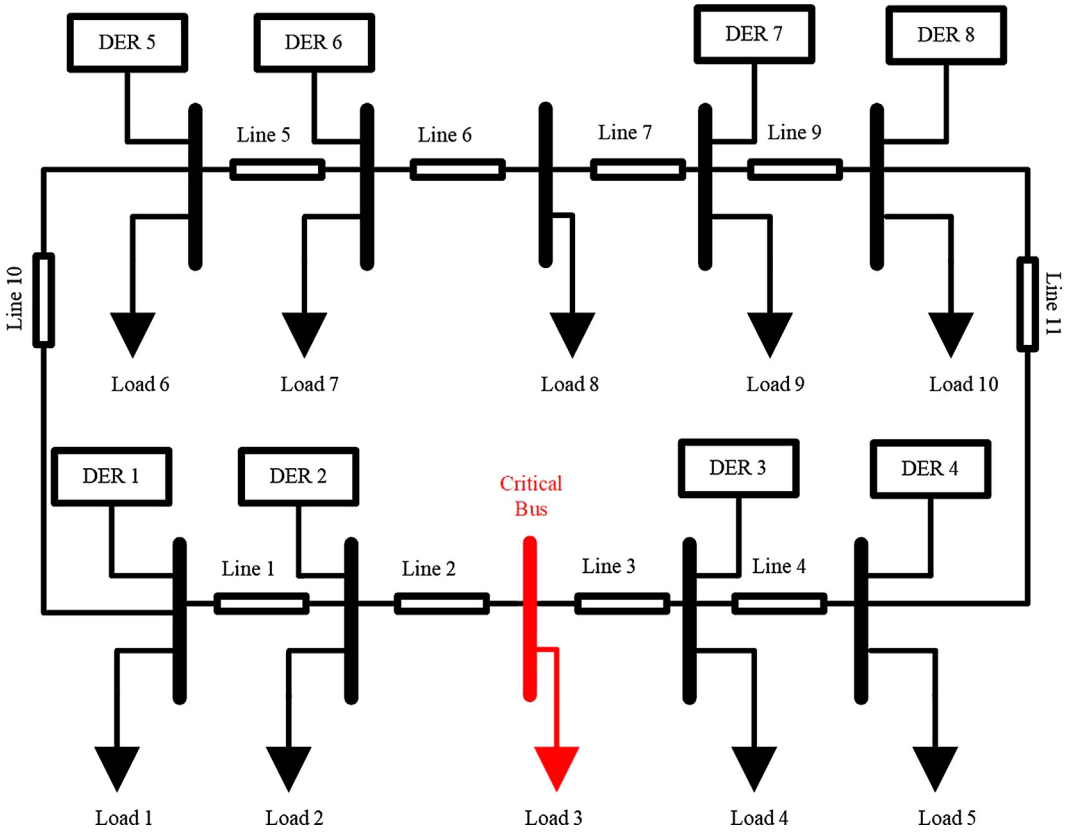

Fig. 10. Single line diagram of 8-DER microgrid test system.

Table 4
Specification of DERs.

	DER1,5	DER2,6	DER3,7	DER4,8
Nominal Output voltage (V)	1500	1500	1500	1500
Nominal Output current (A)	40	20	20	40
Nominal power (kW)	60	30	30	60

microgrid includes four DERs and five loads. Load 3 is a critical load which is highlighted in Fig. 5. v_{ref} in (5) is equal to the nominal voltage of microgrid which is 1500 V. Both k_p and k_i in (5) are set to 1. The specification of DERs, lines, and loads are provided in Tables 1, 2, and 3, respectively. It is assumed that DERs communicate through the communication graph depicted in Fig. 6. We assume zero-mean Gaussian communication noise with following statistical properties $\mathcal{N}(0, 0.5)$. DER 1 is the only DER that knows the leading voltage information with the pinning gain $g_1 = 1$. The control gain C_k is set to 10.

Simulation studies include three test cases to verify the performance of proposed voltage regulation scheme under different scenarios. *Case 1.A* demonstrates the voltage restoration capability of proposed distributed voltage regulator in the absence of cyber-attacks. *Case 1.B* considers the effect of FDI attacks on the microgrid distributed control system. *Case 1.C* verifies the effectiveness of proposed attack detection and mitigation schemes.

6.1.1. Case 1.A: voltage regulation of DC microgrid in the absence of cyber-attacks

In this test case, DC microgrid is islanded at $t = 0$ s. The distributed voltage regulator is applied at $t = 2$ s. The DERs' output current and terminal voltage magnitudes and critical bus voltage magnitude are shown in Fig. 7(a), (b), and (c), respectively. As seen, after the microgrid is islanded, the droop voltage technique is able to maintain microgrid voltage stability while sharing the DC microgrid load among DERs based on their current ratings. However, the critical bus voltage drops below the nominal voltage of microgrid. After the distributed voltage regulator is applied, the critical bus voltage is restored to the microgrid nominal voltage. Moreover, DERs contribute to the microgrid load based on their current ratings.

6.1.2. Case 1.B: impact of FDI attack on voltage regulation of DC microgrid

In this test case, an FDI attack is applied to DER 2 at $t = 2$ s. The simulated attack takes control of DER 2's control unit and shares an exponential corrupted value of $1500 + e^{(t+3)}$ V with its neighboring DERs. The DERs' output current and terminal voltage values, critical bus voltage magnitude, and KL divergence average values in (19) are shown in Fig. 8(a), (b), (c), and (d), respectively. As seen, before attack, distributed voltage regulator regulates the critical bus voltage at 1500 V. After the FDI attack is applied, the DERs' and critical bus voltage magnitudes start to diverge from the microgrid nominal voltage. The DER 3 and 4 output currents start to increase until the overcurrent protection of DERs, set to 1.2 pu, is activated and DERs are shut down. After these two DERs are shut down, microgrid experiences

Table 5
Specification of Loads.

Load 1,6 (Ω)		Load 2,7 (Ω)		Load 3,8 (Ω)		Load 4,9 (Ω)		Load 5,10 (Ω)	
R	150	R	150	R	112.5	R	150	R	150

Table 6
Specification of Lines.

Line 1, 4, 5, 9, 10, 11 (Ω)		Line 2, 3, 6, 7 (Ω)	
R	0.427	R	0.8538

a voltage collapse.

6.1.3. Case 1.C: microgrid distributed voltage regulation with Cyber-attack detection and mitigation

In this test case, similar to *Case 1.B* an FDI attack is applied to DER 2 at $t = 2$ s. The cyber-secure distributed voltage regulator is applied at $t = 2$ s. The thresholds θ_1 and θ_2 in (22) and (24) are set to 6000 and 3000, respectively. The DERs' output current and terminal voltage values and critical bus voltage magnitude are shown in Fig. 9(a), (b), and (c), respectively. As seen, after the distributed voltage regulator is applied, the critical bus voltage is restored to the microgrid nominal voltage. Moreover, DERs contribute to the microgrid load based on their current ratings. The healthy DERs utilize interior and exterior-belief values to ignore the compromised DER. Microgrid remains stable and supplies the loads continuously.

6.2. Simulation results for an 8-DER MVDC microgrid

The single line diagram of 8-DER MVDC microgrid system is shown in Fig. 10. This DC microgrid system is simulated in MATLAB/Simulink. The microgrid includes eight DERs and ten loads. Load 3 is a critical load which is highlighted. v_{ref} in (5) is equal to the nominal voltage of microgrid which is 1500 V. Both k_p and k_i in (5) are set to 1. The specification of DERs, lines, and loads are provided in Tables 4, 5, and 6, respectively. It is assumed that DERs communicate through the communication graph depicted in Fig. 11. We assume zero-mean Gaussian communication noise with following statistical properties $\mathcal{N}(0, 0.5)$. DER 1 is the only DER that knows the leading voltage information with the pinning gain $g_1 = 1$. The control gain C_k is set to 10.

6.2.1. Case 2.A: 8-DER microgrid distributed voltage regulation with cyber-attack detection and mitigation

In this test case, an FDI attack similar to *Case 1.B* is applied to DER 2 at $t = 2$ s. The cyber-secure distributed voltage regulator is also applied at also $t = 2$ s. The thresholds θ_1 and θ_2 in (22) and (24) are set to 6000 and 3000, respectively. The DERs' output current and terminal voltage values and critical bus voltage magnitude are shown in Fig. 12(a), (b), and (c), respectively. As seen, after the distributed voltage regulator is applied, the critical bus voltage is restored to the microgrid nominal voltage. Moreover, DERs contribute to the microgrid load based on their current ratings. The healthy DERs utilize interior and exterior-

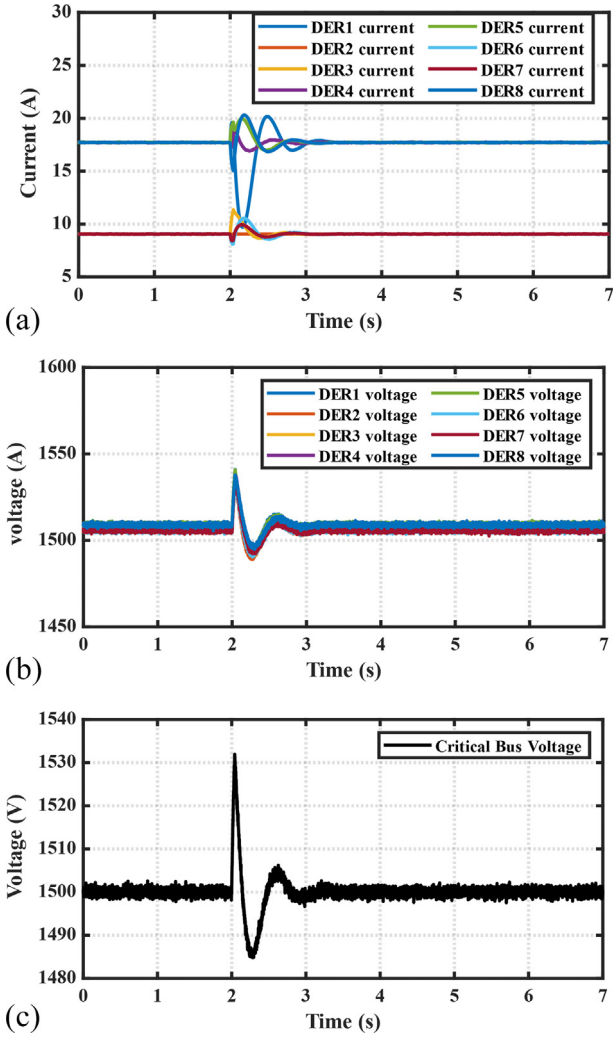

Fig. 12. Microgrid distributed voltage regulation equipped with cyber-attack detection and mitigation: (a) DERs' output current; (b) DERs' terminal voltage magnitude; (c) critical bus voltage.

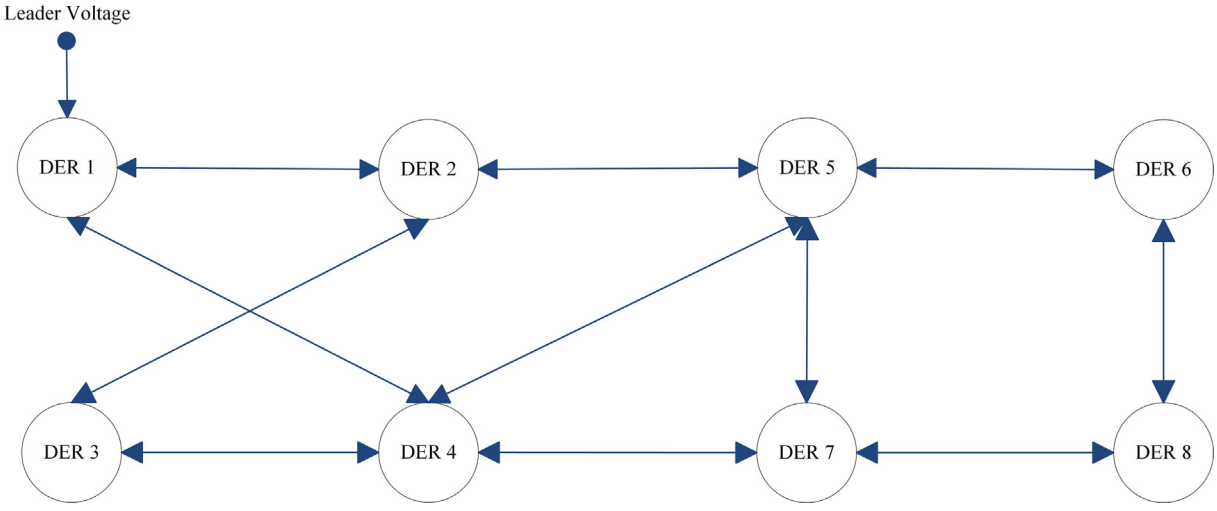

Fig. 11. Communication graph of the 8-DER microgrid test system.

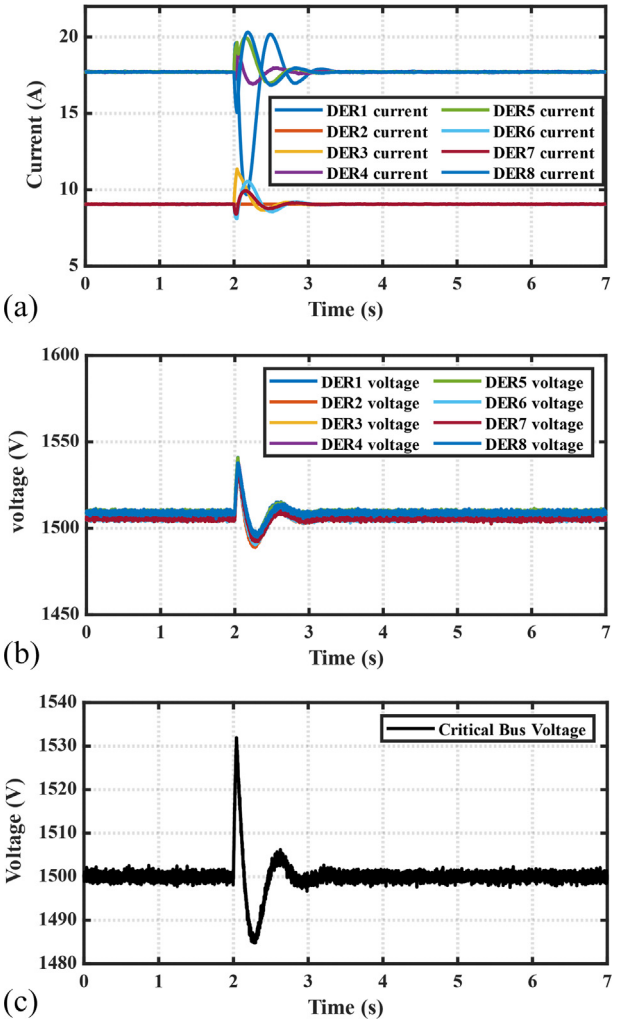

Fig. 13. 8-DER Microgrid distributed voltage regulation with packet loss equipped with cyber-attack detection and mitigation: (a) DERs' output current; (b) DERs' terminal voltage magnitude; (c) critical bus voltage.

belief values to ignore the compromised DER. Microgrid remains stable and supplies the loads continuously.

6.2.2. Case 2.B: 8-DER microgrid distributed voltage regulation with cyber-attack detection and mitigation and communication packet loss

In this test case, the packet loss effect in the microgrid voltage regulation is simulated assuming that the communication links between (DER 2, DER 3), (DER 4, DER 5), and (DER 6, DER 8) are broken during [2.95 s, 3 s], [3.95 s, 4 s], [4.95 s, 5 s], [5.95 s, 6 s], and [6.95 s, 7 s] time intervals. An FDI attack similar to *Case 1.B* is applied to DER 2 at $t = 2$ s. The DERs' output current and terminal voltage values and critical bus voltage magnitude are shown in Fig. 13(a), (b), and (c), respectively. As seen, after the distributed voltage regulator is applied, the critical bus voltage is restored to the microgrid nominal voltage. Moreover, DERs contribute to the microgrid load based on their current ratings. This verifies the performance of proposed attack detection and mitigation scheme under communication packet loss.

7. Conclusion

This paper proposes a cyber-attack detection and mitigation scheme for the distributed voltage control of critical loads in DC microgrids. Distributed current and voltage controllers are implemented in each DER to implement the voltage regulation scheme. Each DER shares its voltage and current information with its neighbors on the communication graph. A relative entropy-based detection and mitigation scheme for FDI attacks on the DC microgrid distributed control system is proposed. KL divergence is utilized as a measure to identify possible FDI attacks on DERs. The negative impact of cyber-attacks is mitigated though the introduction of interior and exterior-belief values by utilizing KL divergence. The interior-belief value is a measure of trustworthiness of the DER's own outgoing information and is transmitted to neighboring DERs. An exterior-belief value is a measure for the trustworthiness of incoming information from neighboring DERs. The attack mitigation technique utilizes interior and exterior belief values to modify weighted control protocols to slow down the spread of attacks. The validity of proposed attack detection and mitigation schemes is verified through simulating a typical medium-voltage DC microgrid system in MATLAB/Simulink.

CRediT authorship contribution statement

Binod P. Poudel: Conceptualization, Methodology, Software, Validation, Writing - original draft, Writing - review & editing. **Aquib Mustafa:** Conceptualization, Methodology, Software, Validation. **Ali Bidram:** Conceptualization, Methodology, Software, Validation, Writing - original draft, Writing - review & editing. **Hamidreza Modares:** Conceptualization, Methodology, Writing - original draft, Writing - review & editing.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgement

This paper is based upon work supported by the National Science Foundation EPSCoR Program under Award #OIA-1757207.

Appendix A. Supplementary material

Supplementary data to this article can be found online at https://doi.org/10.1016/j.ijepes.2020.105968.

References

[1] Ton DT, Smith MA. The U.S. Department of Energy's microgrid initiative. Electr J 2012;25:84–94. https://doi.org/10.1016/j.tej.2012.09.013.
[2] Dragicevic T, Lu X, Vasquez JC, Guerrero JM. DC microgrids-Part I: A review of control strategies and stabilization techniques. IEEE Trans Power Electron 2016;31(7):4876–91. https://doi.org/10.1109/TPEL.2015.2478859.
[3] Dragicevic T, Lu X, Vasquez JC, Guerrero JM. DC microgrids-Part II: A review of power architectures, applications and standardization issues. IEEE Trans Power Electron 2016;31(5):3528–49. https://doi.org/10.1109/TPEL.2015.2464277.
[4] Wu D, Tang F, Dragicevic T, Guerrero JM, Vasquez J. Coordinated control based on bus-signaling and virtual inertia for islanded dc microgrids. IEEE Trans Smart Grid 2015;6(6):2627–38. https://doi.org/10.1109/TSG.2014.2387357.
[5] Moayedi S, Davoudi A. Unifying distributed dynamic optimization and control of islanded DC microgrids. IEEE Trans Power Electron 2017;32(3):2329–46. https://doi.org/10.1109/TPEL.2016.2565517.
[6] Shadmand MB, Balog RS. Multi-objective optimization and design of photovoltaic-wind hybrid system for community smart dc microgrid. IEEE Trans Smart Grid 2014;5(5):2635–43. https://doi.org/10.1109/TSG.2014.2315043.
[7] Kumar M, Srivastava S, Singh S. Control strategies of a dc microgrid for grid connected and islanded operations. IEEE Trans Smart Grid 2015;6(4):1588–601. https://doi.org/10.1109/TSG.2015.2394490.
[8] Nasirian V, Moayedi S, Davoudi A, Lewis F. Distributed cooperative control of dc microgrids. IEEE Trans Power Electron 2015;30(4):2288–303. https://doi.org/10.1109/TPEL.2014.2324579.
[9] Guerrero JM, Vasquez JC, Matas J, de Vincuna LG, Castilla M. Hierarchical control of droop-controlled ac and dc microgrids-A general approach toward standardization. IEEE Trans Ind Electron 2011;58(1):158–72. https://doi.org/10.1109/TIE.2010.2066534.
[10] Bracale A, Caramia P, Carpinelli G, Mancini E, Mottola F. Optimal control strategy of a DC micro grid. Int J Electr Power Energy Syst 2015;67:25–38. https://doi.org/

10.1016/j.ijepes.2014.11.003.
[11] Babaiahgari B, Habib Ullah M, Park JD. Coordinated control and dynamic optimization in DC microgrid systems. Int J Electr Power Energy Syst 2019;113:832–41. https://doi.org/10.1016/j.ijepes.2019.05.076.
[12] Shahida MU, Khana MM, Hashmia K, Asad Khana RB, Yuningc J, Tanga H. Renewable energy source (RES) based islanded DC microgrid with enhanced resilient control. Int J Electr Power Energy Syst 2019;113:461–71. https://doi.org/10.1016/j.ijepes.2019.05.069.
[13] Tah A, Das D. An enhanced droop control method for accurate load sharing and voltage improvement of isolated and interconnected dc microgrids. IEEE Trans Sustain Energy 2016;7(3):1194–204. https://doi.org/10.1109/TSTE.2016.2535264.
[14] Moayedi S, Nasirian V, Lewis F, Davoudi A. Team-oriented load sharing in parallel dc-dc converters. IEEE Trans Ind Appl 2015;51(1):479–90. https://doi.org/10.1109/TIA.2014.2336982.
[15] Liu X, He H, Wang YW, Xu Q, Guo F. Distributed hybrid secondary control for a DC microgrid via discrete-time interaction. IEEE Trans Energy Convers 2018;33(4):1865–75. https://doi.org/10.1109/TEC.2018.2850279.
[16] Rahman MS, Hossain MJ, Lu J, Pota HR. A need-based distributed coordination strategy for EV storages in a commercial hybrid AC/DC microgrid with an improved interlinking converter control topology. IEEE Trans Energy Convers 2018;33(3):1372–83. https://doi.org/10.1109/TEC.2017.2784831.
[17] Kou P, Liang D, Gao L. Distributed coordination of multiple PMSGs in an islanded DC microgrid for load sharing. IEEE Trans Energy Convers 2017;32(2):471–85. https://doi.org/10.1109/TEC.2017.2649526.
[18] Nasirian V, Davoudi A, Lewis FL, Guerrero JM. Distributed adaptive droop control for dc distribution systems. IEEE Trans Energy Convers 2014;29(4):944–56. https://doi.org/10.1109/TEC.2014.2350458.
[19] Liu X, Li Z. False data attacks against AC state estimation with incomplete network information. IEEE Trans Smart Grid 2017;8(5):2239–48. https://doi.org/10.1109/TSG.2016.2521178.
[20] Chlela M, Mascarella D, Joos G, Kassouf M. Fallback control for isochronous energy storage systems in autonomous microgrids under denial-of-service cyber-attacks. IEEE Trans Smart Grid 2018;9(5):4702–11. https://doi.org/10.1109/TSG.2017.2667586.
[21] Xue D, Jing X, Liu H. Detection of false data injection attacks in smart grid utilizing ELM-based OCON framework. IEEE Access 2019;7:31762–73. https://doi.org/10.1109/ACCESS.2019.2902910.
[22] He Y, Mendis GJ, Wei J. Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism. IEEE Trans Smart Grid 2017;8(5):2505–16. https://doi.org/10.1109/TSG.2017.2703842.
[23] Hug G, Giampapa JA. Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks. IEEE Trans Smart Grid 2012;3(3):1362–70. https://doi.org/10.1109/TSG.2012.2195338.
[24] Huang Y, Tang J, Cheng Y, Li H, Campbell KA, Han Z. Real-time detection of false data injection in smart grid networks: An adaptive cusum method and analysis. IEEE Syst J 2016;10(2):532–43. https://doi.org/10.1109/JSYST.2014.2323266.
[25] Manandhar K, Cao X, Hu F, Liu Y. Detection of faults and attacks including false data injection attack in smart grid using kalman filter. IEEE Trans Control Netw Syst 2014;1(4):370–9. https://doi.org/10.1109/TCNS.2014.2357531.
[26] Mohammadpourfard M, Sami A, Weng Y. Identification of false data injection attacks with considering the impact of wind generation and topology reconfigurations. IEEE Trans Sustain Energy 2018;9(3):1349–64. https://doi.org/10.1109/TSTE.2017.2782090.
[27] Bi S, Zhang YJ. Graphical methods for defense against false-data injection attacks on power system state estimation. IEEE Trans Smart Grid 2014;5(3):1216–27. https://doi.org/10.1109/TSG.2013.2294966.
[28] Mo Y, Chabukswar R, Sinopoli B. Detecting integrity attacks on scada systems. IEEE Trans Control Syst Technol 2014;22(4):1396–407. https://doi.org/10.1109/TCST.2013.2280899.
[29] Liu L, Esmalifalak M, Ding Q, Emesih VA, Han Z. Detecting false data injection attacks on power grid by sparse optimization. IEEE Trans Smart Grid 2014;5(2):612–21. https://doi.org/10.1109/TSG.2013.2284438.
[30] Saha S, Roy TK, Mahmud MA, Haque ME, Islam SN. Sensor fault and cyber attack resilient operation of DC microgrids. Int J Electr Power Energy Syst 2018;99:540–54. https://doi.org/10.1016/j.ijepes.2018.01.007.
[31] Pasqualetti F, Bicchi A, Bullo F. Consensus computation in unreliable networks: A system theoretic approach. IEEE Trans Autom Control 2012;57(1):90–104. https://doi.org/10.1109/TSG.2017.2667586.
[32] Pasqualetti F, Dorfler F, Bullo F. Attack detection and identification in cyber-physical systems. IEEE Trans Autom Control 2013;58(11):2715–29. https://doi.org/10.1109/TAC.2013.2266831.
[33] Dehkordi NM, Baghaee HR, Sadati N, Guerrero JM. Distributed noise-resilient secondary voltage and frequency control for islanded microgrids. IEEE Trans Smart Grid 2019;10(4):3780–90. https://doi.org/10.1109/TSG.2018.2834951.
[34] Shrivastva S, Subudhi B, Das S. Noise-resilient voltage and freqneucy synchronization of an autonomous microgrid. IET Gener Transm Distrib 2019;13(2):189–200. https://doi.org/10.1049/iet-gtd.2018.6409.
[35] Lia J, Lu X, Yu X. Stochastic distributed frequency and load sharing control for microgrids with communication delays. IEEE Syst J 2019;13(4):4269–80. https://doi.org/10.1109/JSYST.2019.2901711.
[36] Abhinav S, Modares H, Lewis FL, Davoudi A. Resilient cooperative control of DC microgrids. IEEE Trans Smart Grid 2019;10(1):1083–5. https://doi.org/10.1109/TSG.2018.2872252.
[37] Qu Z. Cooperative control of dynamical systems: Applications to autonomous vehicles. New York: Springer-Verlag; 2009.
[38] Huang PH, Liu PC, Xiao W, El Moursi MS. A novel droop-based average voltage sharing control strategy for dc microgrids. IEEE Trans Smart Grid 2015;6(3):1096–106. https://doi.org/10.1109/TSG.2014.2357179.
[39] Nobrega Tahim A, Pagano D, Lenz E, Stramosk V. Modeling and stability analysis of islanded dc microgrids under droop control. IEEE Trans Power Electron 2015;30(8):4597–607. https://doi.org/10.1109/TPEL.2014.2360171.
[40] Lu X, Guerrero JM, Sun K, Vasquez JC. An improved droop control method for dc microgrids based on low bandwidth communication with dc bus voltage restoration and enhanced current sharing accuracy. IEEE Trans Power Electron 2014;29(4):1800–12. https://doi.org/10.1109/TPEL.2013.2266419.
[41] Kullback S, Leibler RA. On information and suciency. Ann Math Stat 1951;22(1):79–86.
[42] Basseville M, Nikiforov IV. Detection of abrupt changes: Theory and application. Prentice Hall Englewood Cliffs; 1993.
[43] Cover TM, Thomas JA. Elements of information theory. New York, NY, USA: Wiley-Interscience; 2006.
[44] IEEE recommended practice for 1 kV to 35 kV medium-voltage DC power systems on ships. IEEE Std 1709-2010, 2010: 1-54. http://dx.doi.org/10.1109/IEEESTD.2010.5623440.