2025 IEEE Energy Conversion Conference Congress and Exposition (ECCE) | 979-8-3315-4130-9/25/$31.00 ©2025 IEEE | DOI: 10.1109/ECCE58356.2025.11260430

An Ergodic CuSum Algorithm for False Data Injection Attacks Detection in DC Microgrids

Ge Yang
Department of Electrical Engineering
University at Buffalo
Buffalo, USA
gyang22@buffalo.edu

Zhongchang Sun
Department of Electrical Engineering
University at Buffalo
Buffalo, USA
zhongcha@buffao.edu

Shaofeng Zou
School of Electrical, Computer
and Energy Engineering
Arizona State University
Phoenix, USA
zou@asu.edu

Xiu Yao
Department of Electrical Engineering
University at Buffalo
Buffalo, USA
xiuyao@buffalo.edu

Luis Herrera
Department of Electrical Engineering
University at Buffalo
Buffalo, USA
lcherrer@buffalo.edu

***Abstract*—DC microgrids have widely adopted hierarchical control architecture through distributed generation units (DGUs) to enhance reliability and scalability. However, this makes the system vulnerable to false data injection attacks (FDIAs), which can disrupt system stability or shift the operating point. While observers are commonly used to detect FDIAs, some FDIAs can be stealthy, or observers lack sufficient sensitivity for reliable identification. To address this, we propose a quickest change detection (QCD) method based on an unknown input observer (UIO) estimation error model to detect the FDIAs that are stealthy to the UIOs. The Ergodic CuSum algorithm is designed and can be efficiently updated using estimation error observations. The approach is validated through Simulink and real-time simulations.**

***Index Terms*—Microgrid, Observer, Attack, CuSum, Detection.**

I. Introduction

Modern dc microgrids commonly adopt a hierarchical control architecture [1], which relies on the exchange of measurement data to ensure coordinated operation. However, this reliance on communication networks introduces vulnerabilities to cyber attacks. Among various attack types, false data injection attacks (FDIAs) are among the most frequently reported in dc microgrids [2], [3]. By compromising communicated data, FDIAs can disrupt control coordination and shift the desired operation of the microgrid system [4]. As a result, timely and accurate detection of FDIAs is essential to ensure the system's security and reliability.

Detection strategies for FDIAs have primarily focused on analyzing the system's current and voltage signals to identify abnormal behavior during an attack. Machine learning (ML) based approaches have been explored in [5]–[7], where measurement data under various operating conditions are used to train models for FDIA detection and mitigation. These ML-based methods are advantageous when accurate system models are unavailable, as they can infer system behavior directly from measurements. However, ML-based methods require large datasets covering both normal and various attack scenarios, and the training models can be complex to implement in dc microgrid systems. Another common approach in microgrids involves deploying observers within the system to provide a secure state estimation and attack detection [8]–[11]. In [10], an advanced sliding mode observer is proposed for FDIA detection and resilient control. Data-driven observers are designed to detect the FDIAs in dc microgrids without using the accurate system parameters in [11]. However, certain FDIAs can be carefully designed to shift the system to a different operating point while maintaining overall stability, and can bypass observer-based detectors [12], [13]. To solve the low sensitivity of observers to the potential FDIAs, in [13], a proactive perturbation is applied to enable the UIO-based locators to identify the deception FDIAs. In [14], a Kalman filter-based detection method is developed for detecting the FDIA that can bypass the traditional residual detection method.

In recent research, quickest change detection methods are explored for detecting attacks in power systems [15]–[17], and this type of method aims to determine a change of the observed statistics as quickly as possible based on the online observations and specific decision rules while controlling the false alarm rate. A Markov chain-based analytical model is developed for the smart grid system, enabling real-time detection of FDIAs using a new normalized Rao-CuSum algorithm [15]. In [16], an adaptive nonparametric CuSum-based detector is proposed to detect FDIAs and coordinated cyber-physical attacks in the smart grid system. In [17], the state estimation is performed using the Kalman filter, and a generalized CuSum algorithm is employed for the attack detection in the smart grid system. Although the generalized likelihood ratio test (GLRT)

This work was supported by the National Science Foundation under Grant ECCS 2339434.

979-8-3315-4130-9/25/$31.00 ©2025 IEEE

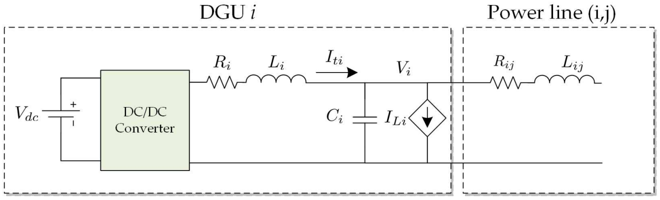

Fig. 1. Electrical scheme of the DGU and power line (i, j).

can handle unknown parameters, it becomes computationally expensive when dealing with complex system models [18]. Another challenge in implementing the QCD framework lies in defining the pre- and post-change models and efficiently computing the probability density based on system observations. To reduce the computation load, an Ergodic CuSum algorithm was proposed in [19] for autoregressive models, utilizing a forward variable to compute the probability density at each time step efficiently. However, this method has not been studied for FDIA detection in dc microgrids.

To address the above challenges, this paper proposes a novel Ergodic CuSum-based framework for detecting FDIAs that are stealthy to observer-based detectors. The QCD problem is formulated using the estimation error dynamics of a UIO, combining the UIO's advantage of requiring fewer sensors with the strong detection capability of the CuSum algorithm. Probability density functions for pre- and post-change models are derived based on the key lemmas from [19], and an Ergodic CuSum algorithm is then developed to detect FDIAs. This approach enables practical deployment in real dc microgrid systems. The rest of this paper is organized as follows. In Section II, the model of dc microgrid system and the UIO design are introduced. The FDIA model and Cusum algorithm are demonstrated in Section III. The Simulink simulation results and real-time simulation test results are presented in Sections IV and V. Finally, the conclusion of this paper is presented in Section VI.

II. DC Microgrid model and observer design

A. Discrete-time DGU model

The considered microgrid is modeled by a set of distribution generation units (DGUs), which are connected through a set of resistive and inductive power lines. We consider that the power lines will have different lengths and thicknesses, thus the line inductance and resistance can vary. Each DGU is modeled as a dc voltage source, which is connected to a dc–dc converter. The DGU is assumed to supply a local dc load, which is modeled as a current load input. The diagram of a DGU is presented in Fig. 1. A cooperative current consensus-based controller [20] is used to regulate the current, and a cyber layer is introduced for DGUs to share the measurements. The communication link (j, i) represents data transmission from DGU j to i, and we define communicated current as $I_{(j,i)}$. The controller with primary and secondary layers is presented in Fig. 2. The current regulator computes the local DGU's current consensus with its neighbors to generate a correction term η_i, defined as:

$$\eta_i = \int \bar{I}^i_{avg} = \int \sum_{j\in\mathcal{N}_i} c_i \left(I_{tj} - I_{ti}\right), \tag{1}$$

where c_i is the consensus gain and $\mathcal{N}_i$ denotes the set of neighboring DGUs for DGU i. The correction term η_i is added with the global reference voltage V_{ref} and a droop control term to form the final local voltage reference. By comparing this local reference with the local voltage V_i and feeding the error into the voltage controller (can be a PI controller or integrator), a state variable ν_i is generated for the feedback controller.

The states and inputs in each DGU are $x_i = [V_i \; I_{ti} \; \nu_i \; \eta_i]^T$ and $u_i = [I_{net} + I_{Li} \; V_{\text{ref}} \; \sum_{j\in\mathcal{N}_i} I_{(j,i)} \;]^T$. I_{Li} represents the load current, and I_{net} is the current from neighbors through physical lines. $I_{(j,i)}$ is the current from communication network. Then the continuous-time model of DGU i can be derived as:

$$\begin{aligned} x_i(t+1) &= A_i x_i(t) + B_i u_i(t) \\ y_i(t) &= C_i x_i(t). \end{aligned} \tag{2}$$

The matrices in the model are the following:

$$A_i = \begin{pmatrix} 0 & \frac{1}{C_i} & 0 & 0 \\ \frac{k_1-1}{L_i} & \frac{k_2-R_i}{L_i} & \frac{k_3}{L_i} & 0 \\ -1 & -r_{droop,i} & 0 & 1 \\ 0 & -N_i c_i & 0 & 0 \end{pmatrix} \quad B_i = \begin{pmatrix} -\frac{1}{C_i} & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & c_i \end{pmatrix}, \tag{3}$$

where $k_1, k_2,$ and k_3 are the feedback controller gains and N_i represents the total number of neighboring DGUs for DGU i. The droop gain is defined as $r_{droop,i}$. The forward Euler method is used for system discretization, and the discrete-time model of DGU i is:

$$\begin{aligned} x_i(t+1) &= A^d_i x_i(t) + B^d_i u_i(t) \\ y_i(t) &= C^d_i x_i(t). \end{aligned} \tag{4}$$

B. UIO Design

UIO is designed to track communicated states based on the discrete-time model in (4) by considering inputs within that DGU as unknown inputs. We consider full output measurement is available from the DGU and define $y_{(j,i)}$ as the communication from DGU j to DGU i. The designed UIO model for communication link (j, i) is expressed as:

$$\begin{aligned} z_{(j,i)}(t+1) &= F_{(j,i)} z_{(j,i)}(t) + K_{(j,i)} y_{(j,i)}(t) \\ \hat{x}_{(j,i)}(t) &= z_{(j,i)}(t) + H_{(j,i)} y_{(j,i)}(t) \\ \hat{y}_{(j,i)}(t) &= C^d_i \hat{x}_{(j,i)}(t), \end{aligned} \tag{5}$$

where $\hat{x}_{(j,i)}$ are the estimated states and $\hat{y}_{(j,i)}$ are the estimated outputs/measurements. The estimation error dynamics can be

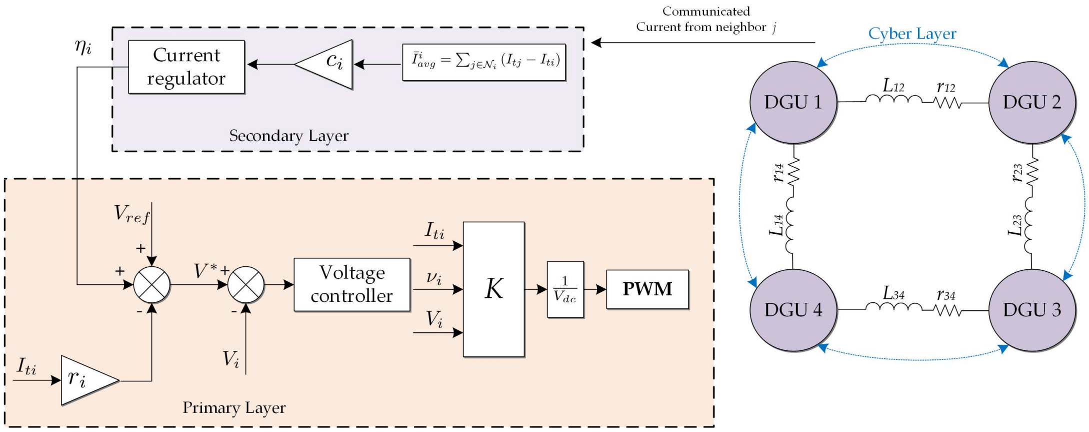

Fig. 2. An example dc microgrid system model with ring network. The network is composed of four interconnected DGUs (four communication links), and the dc source input to each DGU is a generator based on the buck converter using the cooperative controller.

derived using (4) and (5):

$$\begin{aligned}
&e_{(j,i)}(k+1) = x_j(k+1) - \hat{x}_{(j,i)}(k+1)\\
&= x_j(k+1) - \hat{x}_{(j,i)}(k+1)\\
&= A_j^d x_j(k) + B_j^d u_j(k) - [F_{(j,i)} z_{(j,i)}(k)\\
&\quad + K_{(j,i)} y_{(j,i)}(k) + H_{(j,i)} C_j^d (A_j^d x_j(k) + B_j^d u_j(k))]\\
&= (A_j^d - H_{(j,i)} C_j^d A_j^d - K_1^{(j,i)} C_j^d) e_{(j,i)}(k)\\
&\quad + (A_j^d - H_{(j,i)} C_j^d A_j^d - K_1^{(j,i)} C_j^d - F_{(j,i)}) z_{(j,i)}(k)\\
&\quad + [(A_j^d - H_{(j,i)} C_j^d A_j^d - K_1^{(j,i)} C_j^d) H_{(j,i)} - K_2^{(j,i)}] y_{(j,i)}(k)\\
&\quad + (I - H_{(j,i)} C_j^d) B_j^d u_j(k).
\end{aligned} \tag{6}$$

$K_{(j,i)} = K_1^{(j,i)} + K_2^{(j,i)}$. Similar to [21], in order to decouple the influence of unknown inputs u_j on the observer, the following conditions should be satisfied:

$$(I - H_{(j,i)} C_j^d) B_j^d = 0 \tag{7}$$

$$F_{(j,i)} = A_j^d - H_{(j,i)} C_j^d A_j^d - K_1^{(j,i)} C_j^d \tag{8}$$

$$K_2^{(j,i)} = F_{(j,i)} H_{(j,i)}. \tag{9}$$

Using (7)-(9), the error dynamics in (6) can be reduced to:

$$e_{(j,i)}(k+1) = F_{(j,i)} e_{(j,i)}(k). \tag{10}$$

The gain $K_1^{(j,i)}$ should be selected such that all eigenvalues of $F_{(j,i)}$ lie within the unit circle, ensuring that the estimation error converges to zero. Placing these eigenvalues closer to the origin enhances the tracking performance. $K_1^{(j,i)}$ exists if and only if the pair $(C_j^d, A^*_{(j,i)})$ is observable, where

$$A^*_{(j,i)} = (I - H_{(j,i)} C_j^d) A_j^d. \tag{11}$$

The FDIA can target any communication link (j,i), altering the transmitted data as:

$$y_{(j,i)}(t) = y_j(t) + \phi_{(j,i)}(t - T^a_{(j,i)}), \tag{12}$$

where $T^a_{(j,i)}$ and $\phi_{(j,i)}$ denote the attack's initiation time and attack vector. In the work, since the current-consensus controller used in the DGU relies solely on communicated current measurements, false data is injected only into the communicated current to influence the control action.

III. CumSum Algorithm

A. Probability Density Calculation

The pre- and post-change models are formulated from the observer estimation error models under nominal operation and FDIA, and we leverage the Gaussian property of the innovation noise and the measurement noise in the models:

$$\text{Pre-change:} \quad \begin{aligned} e_{(i,j)}(t) &= F e_{(i,j)}(t-1) + \omega(t)\\ y^e_{(i,j)}(t) &= e_{(i,j)}(t) + \nu(t). \end{aligned} \tag{13}$$

$$\text{Post-change:} \quad \begin{aligned} e_{(i,j)}(t) &= F e_{(i,j)}(t-1) + \omega^*(t)\\ y^e_{(i,j)}(t) &= e_{(i,j)}(t) + \nu(t), \end{aligned} \tag{14}$$

where $y^e_{(i,j)}$ is the observed signal. In the pre-change model, $\omega_t \sim \mathcal{N}(0, R_\omega)$ is the innovation noise and $\nu_t \sim \mathcal{N}(0, I)$ is the measurement noise. The covariance matrix in measurement noise ν_t is an identity matrix I. In the post-change model, FDIA induces a mean shift in the estimation error, represented as a nonzero mean vector in the innovation noise ($\omega^* \sim \mathcal{N}(e^a, R_\omega)$). The mean value e^a can be obtained from simulation or theoretical calculation. Consider a FDIA occurs (i,j) at time t_0, the pre-and post-change probability densities are defined as $p_\infty^{(i,j)}(y^e_{(i,j)}(t_0), \cdots y^e_{(i,j)}(t))$ and $p_{t_0}^{(i,j)}(y^e_{(i,j)}(t_0), \cdots y^e_{(i,j)}(t))$ respectively.

For simplicity, in the following derivation, we use e_t to denote the estimation error and y^e_t as the observation. We now define the following forward variable to compute the likelihood function based on [19]:

$$\alpha_t(e_t) = p(y^e_{t_0}, \cdots, y^e_t, e_t). \tag{15}$$

For the pre-change model, we can have the probability density expressed with the forward variable $\alpha_t^{pre}(e_t)$:

$$p_\infty(y^e_{t_0}, \cdots, y^e_t) = \int \alpha_t^{pre}(e_t) de_t. \tag{16}$$

Then the forward variable at time $t+1$ can be expressed as:

$$\alpha_{t+1}^{pre}(e_{t+1}) = \int \alpha_t^{pre}(e_t) f_1(e_{t+1}|e_t) g_1(y_{t+1}^e|e_{t+1}) de_t. \quad (17)$$

The forward variable $\alpha_t(e_t)$ is a Gaussian function, and the proof is provided in [19]. The forward variable satisfies the following equation:

$$\begin{aligned}\alpha_t^{pre}(e_{t-1}) &= \frac{c_{t-1}^{pre}}{\sqrt{(2\pi)^K \det(\Sigma_{t-1}^{pre})}} \\ &\cdot \exp(-\frac{1}{2}(e_{t-1} - \mu_{t-1}^{pre})^\top \Sigma_{t-1}^{-1}(e_{t-1} - \mu_{t-1}^{pre})),\end{aligned} \quad (18)$$

where Σ_t and μ_t are the covariance matrix and mean vector of the forward variable. The term K is determined by the state's dimensions. For time t we can have:

$$\alpha_t^{pre}(e_t) = \int \alpha_{t-1}^{pre}(e_{t-1}) f_1(e_t|e_{t-1}) g_1(y_t^e|e_t)\, de_{t-1} \quad (19)$$

By solving (19), we can express the forward variable at time t as:

$$\begin{aligned}\alpha^{pre}(e_t) &= \frac{c_t^{pre}}{\sqrt{(2\pi)^K \det(\Sigma_t^{pre})}} \\ &\cdot \exp(-\frac{1}{2}(e_t - \mu_t^{pre})^\top (\Sigma_t^{pre})^{-1}(e_t - \mu_t^{pre})),\end{aligned} \quad (20)$$

and the parameters Σ_{t-1}^{pre} and μ_{t-1}^{pre} can be updated as:

$$\begin{aligned}\Sigma_t^{pre} &= (F\Sigma_{t-1}^{pre}F^\top + R_\omega)(F\Sigma_{t-1}^{pre}F^\top + R_\omega + I)^{-1}, \\ \mu_t^{pre} &= (F\Sigma_{t-1}^{pre}F^\top + R_\omega + I)^{-1} F\mu_{t-1}^{pre} \\ &\quad + (F\Sigma_{t-1}^{pre}F^\top + R_\omega)(F\Sigma_{t-1}^{pre}F^\top + R_\omega + I)^{-1} y_t^e.\end{aligned} \quad (21)$$

Then the ratio of coefficient $\frac{c_t^{pre}}{c_{t-1}^{pre}}$ can be obtained:

$$\begin{aligned}\frac{c_t^{pre}}{c_{t-1}^{pre}} &= \frac{1}{\sqrt{(2\pi)^K \det(F\Sigma_{t-1}^{pre}A^\top + R_\omega + I)}} \\ &\cdot \exp(-\frac{1}{2}((F\mu_{t-1}^{pre} - y_t)^\top (F\Sigma_{t-1}^{pre}F^\top \\ &+ R_\omega + I)^{-1}(F\mu_{t-1}^{pre} - y_t))).\end{aligned} \quad (22)$$

The conditional density of the pre-change model can be rewritten using the forward variable:

$$\begin{aligned}p_\infty(y_t^e|y_1^e, \ldots, y_{t-1}^e) &= \frac{p_\infty(y_1^e, \ldots, y_t^e)}{p_\infty(y_1^e, \ldots, y_{t-1}^e)} \\ = \frac{\int \alpha_t^{pre}(e_t)de_t}{\int \alpha^{pre}(e_{t-1})de_{t-1}} &= \frac{c_t^{pre}}{c_{t-1}^{pre}},\end{aligned} \quad (23)$$

Then the additive form for the log likelihood function is

$$\log p_\infty\left(y_1^e, \cdots, y_t^e\right) = \sum_{i=1}^{t} \log \frac{c_i^{pre}}{c_{i-1}^{pre}}. \quad (24)$$

Similarly, to calculate the conditional probability density of the post-change model, the mean change e^a needs to be considered when calculating the forward variable:

$$\alpha_t^{post}(e_t) = \int \alpha_{t-1}^{post}(e_{t-1}) f(e_t|e_{t-1}) g(y_t^e|e_t)\, de_{t-1}. \quad (25)$$

The expression for the forward variable at time t can be expressed as:

$$\begin{aligned}\alpha_t^{post}(e_t) &= \frac{c_t^{post}}{\sqrt{(2\pi)^K \det(\Sigma_t^{post})}} \\ &\cdot \exp(-\frac{1}{2}(e_t - \mu_t^{post})^\top (\Sigma_t^{post})^{-1}(e_t - \mu_t^{post})),\end{aligned} \quad (26)$$

Then the updating rule for the parameters of the forward variable: α_t^{post}:

$$\begin{aligned}\Sigma_t^{post} &= (F\Sigma_{t-1}^{post}F^\top + R_\omega)(F\Sigma_{t-1}^{post}F^\top + R_\omega + I)^{-1}, \\ \mu_t^{post} &= (F\Sigma_{t-1}^{post}F^\top + R_\omega + I)^{-1}(F\mu_{t-1}^{post} + e^a) \\ &\quad + (F\Sigma_{t-1}^{post}F^\top + R_\omega)(F\Sigma_{t-1}^{post}F^\top + R_\omega + I)^{-1} y_t^e.\end{aligned} \quad (27)$$

The ratio of coefficient $\frac{c_t^{post}}{c_{t-1}^{post}}$ can be obtained:

$$\begin{aligned}\frac{c_t^{post}}{c_{t-1}^{post}} &= \frac{1}{\sqrt{(2\pi)^K \det(F\Sigma_{t-1}^{post}F^\top + R_\omega + I)}} \\ &\cdot \exp(-\frac{1}{2}((F\mu_{t-1}^{post} - y_t^e - e^a)^\top (F\Sigma_{t-1}^{post}F^\top \\ &+ R_\omega + I)^{-1}(F\mu_{t-1}^{post} - y_t^e - e^a))).\end{aligned} \quad (28)$$

Then, the conditional probability under the post-change model can be expressed as:

$$\begin{aligned}p_{t_0}(y_t^e|y_{t_0}^e, \ldots, y_{t-1}^e) &= \frac{p_{t_0}(y_{t_0}^e, \ldots, y_t^e)}{p_{t_0}(y_{t_0}^e, \ldots, y_{t-1}^e)} \\ = \frac{\int \alpha_t(e_t)de_t}{\int \alpha^{post}(e_{t-1})de_{t-1}} &= \frac{c_t^{post}}{c_{t-1}^{post}}.\end{aligned} \quad (29)$$

The log likelihood function:

$$\log p_{t_0}\left(y_{t_0}^e, \cdots, y_t^e\right) = \sum_{i=t_0}^{t} \log \frac{c_i^{post}}{c_{i-1}^{post}}. \quad (30)$$

By introducing two forward variables, the mean and covariance of the forward variable can be updated with the observation signal from the UIO using (21) and (27). Then the log-likelihood functions for both the pre-change and post-change models can be calculated efficiently.

B. Ergodic CuSum Algorithm

Consider $t - t_0 + 1$ observations are collected from a UIO, we define the likelihood ratio L_t:

$$L_t = \frac{p_{t_0}(y_{t_0}^e \cdots y_t^e)}{p_\infty(y_{t_0}^e \cdots y_t^e)}. \quad (31)$$

Then the log-likelihood ratio is:

$$\log L_t = \log p_{t_0}\left(y_{t_0}^e, \cdots, y_t^e\right) - \log p_\infty\left(y_1^e, \cdots, y_t^e\right). \quad (32)$$

Using (24) and (30), we can get an additive form for updating the L_t based on the previous step:

$$\begin{aligned}\log L_t &= \sum_{i=t_0}^{t} \log \frac{c_i^{post}}{c_{i-1}^{post}} - \sum_{i=1}^{t} \log \frac{c_i^{pre}}{c_{i-1}^{pre}} \\ &= \log L_{t-1} + \log(\frac{c_t^{post}}{c_{t-1}^{post}}) - \log(\frac{c_t^{pre}}{c_{t-1}^{pre}}).\end{aligned} \quad (33)$$

For each step, with the observation y_t^e from the system, the parameters of the forward variable and $\log L_t$ can be updated recursively. Then we design the Ergodic CuSum statistic as:

$$\begin{aligned} D_t &= \max_{0 \le i \le t} \left(\log L_t - \log L_i \right) \\ &= \max \left(0, D_{t-1} + \log L_t - \log L_{t-1} \right). \end{aligned} \tag{34}$$

Under nominal operation, system observations are more likely to follow the pre-change distribution, causing the calculated statistic D_t to remain near zero or show no significant variation. However, when an FDIA occurs, D_t begins to increase continuously. Based on the CuSum statistic's behavior, the Ergodic CuSum algorithm is designed to detect FDIAs on communication link (i, j) as follows:

$$\begin{aligned} \text{No FDIA} : D_{(i,j)} &< T \\ \text{FDIA detected} : D_{(i,j)} &\ge T, \end{aligned} \tag{35}$$

where T is a threshold. A FDIA point/time τ can be detected whenever

$$\tau = \inf \left\{ t : D_t \ge T \right\}. \tag{36}$$

In the Ergodic CuSum algorithm, the CuSum statistic grows continuously over time. This property simplifies the design of the detection threshold T, as the statistic $D_{(i,j)}$ will eventually exceed it. In contrast, most observer-based methods produce estimation errors that converge to a steady state, making threshold selection more challenging.

IV. Simulation Verification

The dc microgrid system shown in Fig. 2 is used to validate the proposed CuSum-based detection method in MATLAB Simulink, with simulation parameters provided in Table I. The simulation time step is set to 10 μs. The nominal dc output voltage of each DGU is 200 V, while the input voltage of the generator converters is 270 V. With a load current of 3 A, each DGU delivers an output power of 600 W. Eight UIOs are designed to cover the eight communication links in the system, and eight corresponding CuSum-based detectors are then developed to detect potential FDIAs. The squared norm of the residuals ($||r_{(j,i)}||_2^2 = ||e_{(j,i)}||_2^2$) generated by the UIOs, along with the CuSum statistics $D_{(j,i)}$, are collected for FDIA detection and comparison.

A. Load Change Test

During normal operation, the voltage and current at each DGU are regulated to 200 V and 3 A with the current consensus-based controller. To test the performance of the proposed detection framework under nominal conditions, a load change is applied at DGU 1 at $t = 1.5$ s. As shown in Fig. 3, the coordinated control among the DGUs maintains equal current sharing. The residuals generated by the UIOs and the CuSum detection signals $D_{(j,i)}$ remain unaffected, confirming that no false alarms are triggered during the normal load variation.

TABLE I
SYSTEM PARAMETERS

DGU i	C_i(mF)	L_i (mH)	$R_i(\Omega)$	$P_i(W)$
1	3	3	1.1	600
2	4	3	2	600
3	5	4	3.1	600
4	6	5	4	600
Line (i,j)	$R_{(i,i)}$(mΩ)	$L_{(i,j)}$ (μH)		
$(1,2)$	1	10		
$(1,4)$	2	20		
$(2,3)$	4	40		
$(3,4)$	5	50		

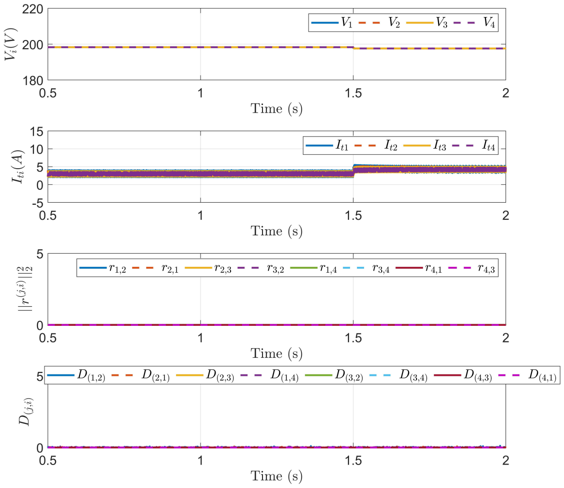

Fig. 3. Simulation results of normal load change in DGU 1.

B. FDIA at $(2,1)$

In the first scenario, a FDIA is introduced at $(2,1)$. As shown in Fig. 4, the current sharing among DGUs is disrupted, and the system shifts to a different operating point. The UIO residual for link $(2,1)$ initially increases and then decreases (close to 0), indicating that UIO is insensitive to the FDIA, which allows the attack to bypass detection. In contrast, the CuSum-based detection statistic $D_{(2,1)}$ shows a significant and sustained increase, clearly identifying the presence and location of the attack.

C. Multiple FDIAs at $(1,2)$ and $(1,4)$

In the second scenario, two different FDIAs are introduced at communication links $(1,2)$ and $(1,4)$ at different times (Fig. 5). During both attack periods, the UIOs fail to detect the FDIAs, as indicated by the low increment of the residuals. In contrast, the CuSum-based detectors respond effectively: when the FDIA at $(1,4)$ occurs, the corresponding CuSum-based detection statistic $D_{(1,4)}$ increases, while other detection statistics remain unchanged. Subsequently, when the FDIA at $(1,2)$ is launched, $D_{(1,2)}$ increases. These results demonstrate that the proposed algorithm can successfully detect multiple FDIAs independently without conflict.

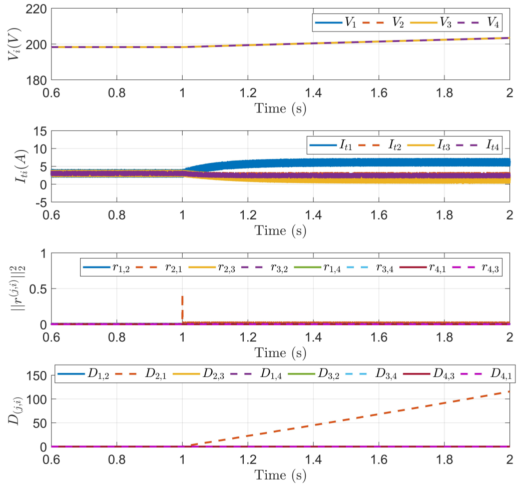

Fig. 4. Simulation results of attack at $(2, 1)$.

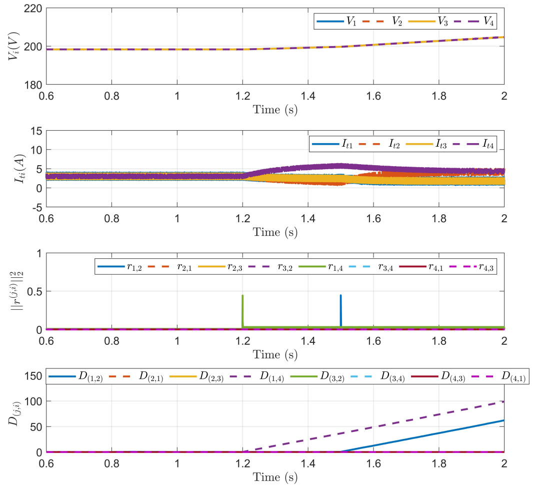

Fig. 5. Simulation results of attacks at $(1, 2)$ and $(1, 4)$.

V. Real-time Simulation Test

To comprehensively validate the proposed FDIA detection framework, the system in Fig. 2 with the same component parameters in Table I is built in the OPAL-RT simulator to conduct the real-time simulation. The simulation time step and switching frequency are set to 20 μs and 5 kHz. The dc microgrid is operating at a voltage reference 200 V and the desired load current is ranging from 5 A to 8 A. The UIOs and Cusum-based detectors are built for 8 communication links in the system. To prevent OPAL-RT analog output saturation, a high flag signal (1 V) is triggered when $D_{(i,j)}$ exceeds the threshold of 0.8, indicating the attack detection result.

In the first scenario, a load change occurs in DGU 1, causing its output current to increase from 5 A to 8 A, as shown in Fig. 6. During this normal operation, the current consensus algorithm ensures equal current sharing and power output across all DGUs. All detection signals from CuSum-based detectors remain constant, indicating no false alarms are triggered during the load variation. In the second scenario, an FDIA is introduced at the communication link $(1, 2)$. As a result, equal current sharing is disrupted, and the current from DGU 2 increases significantly, as shown in Fig. 7. Notably, only the detection signal $D_{(1,2)}$ increases at the time of the attack, accurately indicating the location of the FDIA.

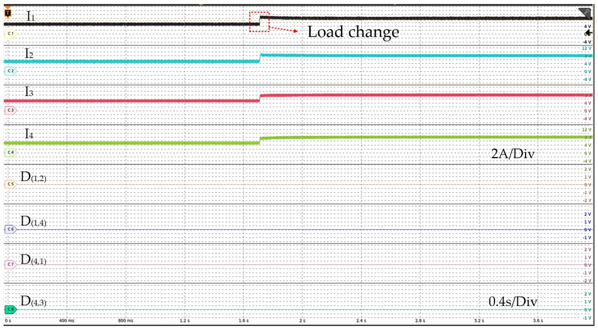

Fig. 6. Real-time simulation results with load change.

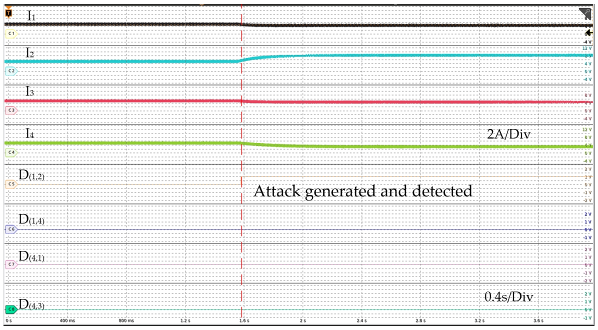

Fig. 7. Real-time simulation results with FDIA at $(1, 2)$.

VI. Conclusion

In this paper, a novel detection framework based on the Ergodic CuSum algorithm is proposed for detecting FDIAs in cooperative dc microgrids composed of DGUs. The proposed framework can detect the FDIAs that are stealthy to traditional observer-based detectors. By utilizing UIOs, the method eliminates the need to measure the input signals within DGUs, thereby reducing sensor requirements and system complexity. The approach leverages the UIO estimation error model to formulate the QCD problem, enabling implementation of the CuSum algorithm in dc microgrid systems. With the use of the forward variable, the CuSum statistics can be effectively updated with the observation from the observer. Both MATLAB/Simulink and real-time simulation results validate the effectiveness of the approach, demonstrating its ability to accurately detect multiple FDIAs that bypass the observer-based detector without false alarms.

References

[1] J. M. Guerrero, J. C. Vasquez, J. Matas, L. G. de Vicuna, and M. Castilla, "Hierarchical control of droop-controlled ac and dc microgrids—a gen-

eral approach toward standardization," *IEEE Transactions on Industrial Electronics*, vol. 58, no. 1, pp. 158–172, 2011.

[2] Y. Mo, T. H.-J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli, "Cyber–physical security of a smart grid infrastructure," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 195–209, 2012.

[3] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, "A review of false data injection attacks against modern power systems," *IEEE Transactions on Smart Grid*, vol. 8, no. 4, pp. 1630–1638, 2017.

[4] H. Sandberg, S. Amin, and K. H. Johansson, "Cyberphysical security in networked control systems: An introduction to the issue," *IEEE Control Systems Magazine*, vol. 35, no. 1, pp. 20–23, 2015.

[5] E. Tian, Z. Wu, and X. Xie, "Codesign of fdi attacks detection, isolation, and mitigation for complex microgrid systems: An hbf-nn-based approach," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 35, no. 5, pp. 6156–6165, 2024.

[6] M. Elimam, Y. J. Isbeih, S. K. Azman, M. S. E. Moursi, and K. A. Hosani, "Deep learning-based pmu cyber security scheme against data manipulation attacks with wadc application," *IEEE Transactions on Power Systems*, vol. 38, no. 3, pp. 2148–2161, 2023.

[7] A. Kavousi-Fard, W. Su, and T. Jin, "A machine-learning-based cyber attack detection model for wireless sensor networks in microgrids," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 1, pp. 650–658, 2021.

[8] A. J. Gallo, M. S. Turan, F. Boem, T. Parisini, and G. Ferrari-Trecate, "A distributed cyber-attack detection scheme with application to dc microgrids," *IEEE Transactions on Automatic Control*, vol. 65, no. 9, pp. 3800–3815, 2020.

[9] G. Yang, L. Herrera, and X. Yao, "Detection of false data injection and series arc faults in dc microgrids based on unknown input observers," in *2023 IEEE Energy Conversion Congress and Exposition (ECCE)*, 2023, pp. 1155–1159.

[10] H. Shafei, M. Farhangi, L. Li, R. P. Aguilera, and H. H. Alhelou, "A novel cyber-attack detection and mitigation for coupled power and information networks in microgrids using distributed sliding mode unknown input observer," *IEEE Transactions on Smart Grid*, vol. 16, no. 2, pp. 1667–1681, 2025.

[11] G. Yang, L. Herrera, and X. Yao, "False data injection attack detection in dc microgrids based on data-driven unknown input observers," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, pp. 1–1, 2025.

[12] 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 Transactions on Power Electronics*, vol. 36, no. 8, pp. 9565–9577, 2021.

[13] M. Liu, C. Zhao, J. Xia, R. Deng, P. Cheng, and J. Chen, "Pddl: Proactive distributed detection and localization against stealthy deception attacks in dc microgrids," *IEEE Transactions on Smart Grid*, vol. 14, no. 1, pp. 714–731, 2023.

[14] Y. Liu and L. Cheng, "Relentless false data injection attacks against kalman-filter-based detection in smart grid," *IEEE Transactions on Control of Network Systems*, vol. 9, no. 3, pp. 1238–1250, 2022.

[15] S. Nath, I. Akingeneye, J. Wu, and Z. Han, "Quickest detection of false data injection attacks in smart grid with dynamic models," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 10, no. 1, pp. 1292–1302, 2022.

[16] T. Zhou, K. Xiahou, L. Zhang, and Q. H. Wu, "Real-time detection of cyber-physical false data injection attacks on power systems," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 10, pp. 6810–6819, 2021.

[17] M. N. Kurt, Y. Yılmaz, and X. Wang, "Distributed quickest detection of cyber-attacks in smart grid," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 8, pp. 2015–2030, 2018.

[18] T. L. Lai, "Information bounds and quick detection of parameter changes in stochastic systems," *IEEE Transactions on Information Theory*, vol. 44, no. 7, pp. 2917–2929, 1998.

[19] Z. Sun and S. Zou, "Quickest change detection in autoregressive models," *IEEE Transactions on Information Theory*, vol. 70, no. 7, pp. 5248–5268, 2024.

[20] V. Nasirian, S. Moayedi, A. Davoudi, and F. L. Lewis, "Distributed cooperative control of dc microgrids," *IEEE Transactions on Power Electronics*, vol. 30, no. 4, pp. 2288–2303, 2015.

[21] J. Chen and R. J. Patton, *Robust model-based fault diagnosis for dynamic systems*. Springer Science & Business Media, 2012, vol. 3.