A NDO Based Attack Detection Observer and Isolation Strategy in Distributed DC Microgrid with FDIA

Daming Zhang\textsuperscript{1*}, Chuanlin Zhang\textsuperscript{2}

\textsuperscript{1}Collage of Automation Engineering, Shanghai University of Electric Power, Shanghai, 200090, China
\textsuperscript{2}Collage of Automation Engineering, Shanghai University of Electric Power, Shanghai, 200090, China
\textsuperscript{*}Corresponding author’s e-mail: ethan.zhang@mail.shiep.edu.cn

Abstract. In this paper, an isolation scheme is proposed to mitigate adverse effects of false data injection attack (FDIA) in cyber layer of distributed DC microgrids. Firstly, the attack signal in communication link is effectively estimated by the nonlinear disturbance observer (NDO). Secondly, an isolation mechanism is designed to distributively insulate the misbehaving agent of cooperative control, and further to mitigate adverse effects on voltage regulation and power sharing in DC microgrids. Thirdly, considering the changes in load distribution during the process of isolation, a domination controller for stabilizing DC/DC boost converter is introduced to ensure the rapid voltage convergence with accurate tracking over a wide operating range. Simulation results are conducted on an islanded DC MG test system to verify the effectiveness of the proposed scheme.

1. Introduction
The DC microgrids are evolving into complex integration named cyber-physical-systems (CPSs), combining sensing, communication, control and physical environment. However, such CPSs are vulnerable to cyber attacks, because of the absence of a central entity to monitor all DC-DC converter activities, which leads to a limited global situational awareness [1]. There are various types of cyber attacks on CPS, e.g., false-data injection attack (FDIA) [2], denial of service [3], and random attacks [4]. Such attacks are adept at disrupting the network stability as well as control structures. Several instances have been reported in the past, which became a critical concern for the control centers. This paper focuses on investigation of FDIA\textsuperscript{s}, as the most prominent cyber attack example, which alter the system state by injecting false data into the compromised sensors/actuators.

Despite alleviating the burden of singularity in centralized systems, distributed schemes in DC microgrids are also more vulnerable to cyber attacks which are always remotely launched via compromised data, communication protocols and cyber channels. Several instances reported in the past, have become a critical concern for the control centers [4]. The impact of the communication-channel cyber attacks on the dynamic performances of the island microgrids secondary frequency control have been investigated in [5]. In [6], a trust-based cooperative controller is proposed to calculate the trustworthiness of incoming information at each converter, and detect misbehavior of neighbouring converters using a dynamic trust estimation mechanism, in order to minimize propagation of compromised data. However, the online computation of these factors involves additional integration and segmentation, which adds a lot of computing burden. In addition, in order to provide an attack resilient...
operation, it requires at least half of the adjacent converters to be reliable, which limits its resilience in the worst case. The article [7] suggests an upper bound based mitigation condition based on the total number of compromised units, termed as F-total, or the local compromised agents in the neighbourhood of each unit, termed as F-local. This method is able to counteract the attacks on sensors and communication links, but it might also unnecessarily abandon neighbours information and then affect the cyber graph connectivity during a load change when there is no attack. In [8], a kind of noise filtration technique with certain statistical properties is proposed to manage time-varying attack signals. However, this method is invalid against cyber attacks based on full knowledge of physical-cyber networks.

In this paper, a new attack detection and isolation scheme in DC microgrids is proposed. Considering the cooperative communication network model of secondary control layer in distributed DC microgrids, the FDIA signal in communication link is estimated, based on the idea of the nonlinear disturbance observer (NDO), and the misled agents in cyber layer are isolated. Then the communication network is reconstructed with N-m nodes which are detected that there are no attack signals. Besides, during the process of isolation and network reconstruction, the power changes for every converter. In order to ensure voltage stability, fast dynamics and accurate tracking at wide operating range, a domination controller is designed for stabilizing the DC/DC boost converter feeding CPL.

The remainder of this paper is organized as follows. A brief overview of distributed secondary control objectives in dc microgrids is depicted and the model of FDIA is given in Section II. In Section III, the detection of FDIA based on NDO techniques and isolation strategy with domination controller is proposed. Section IV presents the simulation of an islanded DC microgrid under the FDIA to verify the proposed approach. Finally, Section V gives the concluding remarks.

Figure 1. The controller layer of a whole DC distribution microgrid system consisting of three DGs.

2. System Model and Problem Formulation

2.1. Preliminaries
In a typical distributed DC microgrid, the physical layer consists of the distributed sources (including the power electronics converters), transmission lines, and loads. And cyber layer, comprised of all the communication links, realizes the information exchange among the connected agents.

The global voltage regulation and proportional load sharing are the two objectives of the secondary/primary control, which require the proper voltage set point assignment for the individual converters [9]. The voltage set point for the droop control of each local converter can be expressed as,

\[ V_{i}^{\text{ref}} = V^* - r_i j_{L,i} + \delta_i \]  

(1)
where the \( V^* \) is the reference voltage of the dc/dc converter, \( r_i \) is the droop coefficient (virtual impedance) of the \( i \)th subsystem, determining the assignment of power output among dc sources, \( I_{ij} \) is the current of \( i \)th converter and \( \delta_i \) is the correction term provided through cooperation among converters, which resulted from voltage regulators (sometimes with current regulators) that help fine adjustment of the local voltage set points, i.e., to provide global voltage regulation and proportional load sharing.

\[
\delta_i = k_p (V_i^* - x_i) + k_i \int (V_i^* - x_i) dt
\]  

(2)

The cooperative secondary controller consists of a dynamic consensus algorithm as seen in (3) and a PI controller (2), in which \( k_p \) and \( k_i \) are the proportional and integral parameters respectively, \( x_i \) is state value of output voltage via consensus algorithm, \( a_{ij} \) is element of the Laplace matrix.

\[
\dot{x}_i = \dot{V}_{ci} + \sum_{j \in N_i} a_{ij} (x_j(t) - x_i(t))
\]  

(3)

This updating protocol is commonly referred to as dynamic consensus. The local measurement \( V_{ci} \) is directly fed into the estimation protocol, in case of any voltage variation at node \( i \), and the local consensus state \( x_i \) immediately responds. Then, the change in \( x_i \) propagates through the communication network and affects all other estimations.

2.2. Modeling the False Data Injection Attack

In this work, the most common additive data attacks are considered. The additive data attack influences the output signal of secondary dynamic consensus algorithm by sending an additional value into the communication links. The FDIA signal sent from agent \( j \) to agent \( i \) is modeled as,

\[
\dot{x}_i^f = \dot{V}_{ci} + \sum_{j \in N_i} a_{ij} (x_j(t) - x_i^f(t) + f_i)
\]  

(4)

where \( f_i \) is the corrupt data added to the communicated information, \( x_i^f \) is the local consensus state corrupted by FDIA.

3. Detection and Isolation Strategy of FDIA

3.1. FDIA detection via NDO

On the basis of (4), the matrix form of FDIA signal in communication links of cyber layer is shown below,

\[
\dot{X}' = \dot{V} + LX' + F
\]  

(5)

where the \( X' \) is the matrix form of corrupted local consensus state, \( L \) is the Laplacian matrix of the consensus algorithm and the \( F \) is the matrix form of FDIA. According to NDO technology, the attack signal can be observed by,

\[
\dot{Z} = \dot{V} + LX' + \hat{F}, \quad \hat{F} = K (A - Z)
\]  

(6)

where the \( \hat{F} \) denotes the estimation of FDIA signal vector, and \( K = \text{diag}[k_{1}, \ldots, k_{n}] \) is the observer gain to be designed. Combining (5)-(6), the dynamics of FDIA signal estimation error are derived, given by
\[ \dot{e}_F = -Ke_F, \]
which implies that the FDIA signal estimation error will converge to zero as time goes to infinity if the observer gain \( K \) is chosen as a Hurwitz Matrix.

We can use the following test to illustrate the effectiveness of the proposed attack detection observer. A microgrid consisting of 3 DGs with boost converter feeds a constant power load of 500W, which are controlled by conventional PI controllers. The involved parameters of this microgrid system are listed in Table 1.

### Table 1. Electrical Parameters of a MG with 3 DGs

| Parameter                              | Value   |
|----------------------------------------|---------|
| DC bus voltage reference               | 100V    |
| Converter input voltage                | 50V     |
| Inductance                             | 3e-3H   |
| Capacitance                            | 2200e-6F|
| Switching frequency                    | 20kHz   |
| Local load at DG3                      | 30 \( \Omega \) |
| Line impedance of node 1               | 1.0 \( \Omega \) |
| Line impedance of node 2               | 1.1 \( \Omega \) |
| Line impedance of node 3               | 1.2 \( \Omega \) |
| The common point CPL at dc bus         | 500W    |
| Observer gain of node \( i \), \( i = 1, 2, 3 \) | 1000    |
| Local load at DG1                      | 40 \( \Omega \) |
| Local load at DG2                      | 40 \( \Omega \) |

It is noted from (5) that the additive data attack influences the secondary average state of consensus \( x_i \) by sending real time false signal to its neighbors by adding an additional value \( f_i \). As the additive \( f_i \) is normally random, a sinusoid signal \( f_i = A\sin(\omega t) \) and a constant signal \( f_i = C \) are respectively considered to be the FDIA signals added by adversary [5].

- Case 1: A sinusoid data attack in DG1 \( f_i = 100\sin(35t) \) is launched at \( t = 0.5s \);
- Case 2: A constant data attack in DG2 \( f_i = 10 \) is launched at \( t = 0.5s \).

The dynamics of the voltage and current of 3 DGs of case 1 and case 2 and trajectories of different \( f_i \) and the estimation \( \hat{f}_i \) are shown in Fig. 2-3. As is shown in two figures, the system runs normally in 0.5s, and the power is allocated proportionally as 1:2:3. And the dynamics of the voltage and current vary irregularly with comparison to the nominal case when false data attacks are launched. In case 1, the system operates normally before \( t = 0.5s \), and sinusoid data attack launched at 0.5s. It can be seen that the oscillations of voltage and current are obvious and which cause the power allocation error. In case 2, the constant data attack launched at 0.5s results in the voltage deviation and then eventually leads system to unstable. The trajectories of different FDIA signals \( f_i \) and the estimation \( \hat{f}_i \) are also shown, illustrating the effectiveness of the proposed attack detection observer.

![Figure 2. Dynamics of the sinusoidal FDIA investigation and its estimation.](image1)

![Figure 3. Dynamics of the constant FDIA investigation and its estimation.](image2)
3.2. Isolation Strategy and Control

Considering the actual operation of microgrids, when cyber attacks occur at a single point or several points, the corrupted nodes will inevitably send the adverse information to their neighbor agents. Because of the fully connected network, the voltage performance of the whole system will further be impacted. The primary controllers of corrupted agents receive the false voltage reference value, but they still retain the ability of tracking reference value. Therefore, the proposed isolation strategy is to remove the nodes from the communication link which were detected to be under attack. When isolated, the nodes diagnosed with FDIA no longer participate in global voltage regulation and proportional load sharing, merely supply their own local load. And the nodes that run safely reconstitute a new connected graph of \( N - m \) nodes, as is shown in Fig. 4. \( N \) is the number of total agents and \( m \) is the number of corrupted ones’. The new network can still ensure that the participating nodes’ voltages are restored to the set value and the common power load reassigned.

![Figure 4. Dynamics of the constant FDIA investigation and its estimation.](image)

3.3. Domination Controller Design

In order to guarantee the good transient dynamic of voltages and currents of different DGs in the process of isolation, a domination controller with strong robustness is designed to stabilize DC/DC boost converters. By using the NDO in [10], the uncertainties in system are reconstructed as a lumped disturbance, such as the sensor error, delay, line resistance, etc. The robust domination controller ensures the output voltages of DGs rapidly track the reference values during isolation.

In a typical DC microgrid, every DC/DC source through a DC/DC boost converter supplying the main DC bus, whose dynamic function can be expressed as,

\[
L_i \ddot{i}_{Li} = E_i - (1 - u_i)V_{C_i}, \quad C_i \dot{V}_{C_i} = (1 - u_i)i_{Li} - \frac{P_o}{V_{C_i}}
\]  

(7)

Variables with subscript \( i \) mean that they are associated with the \( i \)th subsystem. The \( i_{Li} \) and \( V_{C_i} \) denotes the instantaneous inductor current and capacitor voltage respectively and the \( u_i \) is the duty cycle generated by the controllers. \( E_i \) means the input voltage of source. \( P_o \) is the lumped power load [11], [12].

The control objective is to ensure the converter output DC voltage \( V_{C_i} \) to track the reference voltage \( V_i^{ref} \), which is shown in (1). Considering the nonlinear terms in (7), the exact feedback linearization is introduced to transform the system model with two new states. The new coordinates mean the total stored energy and rate of change of energy respectively. According to [10], the systems states are designed as,

\[
x_{i1} = 0.5L_i i_{Li}^2 + 0.5C_i V_{C_i}^2, \quad x_{i2} = E_i i_{Li}, \quad d_{i1} = -P_o
\]  

(8)

and the system is transformed to,

\[
\dot{x}_{i1} = x_{i2} + d_i, \quad \dot{x}_{i2} = v_i
\]  

(9)
The term of $d_i$ can be seen as the coupling of $i$th subsystem imposed by outside electrical components.

The original control objective of the DC/DC boost converter is to design the control law $u_i$, ensuring the voltage $V_{C_i}$ of every DG$_i$ track its reference value $V^\text{ref}_i$, the new system input after the coordinate transformation should be constructed to satisfy the asymptotic tracking of state $x_i$ to its reference value $x_i^\ast$. According to [11], The $d_i$ can be estimated by NDO in (11) and the updated desired goal is given in (11),

$$
\dot{p}_i = x_{i1} + \hat{d}_i, \quad \hat{d}_i = l_i(x_{i1} - p_i)
$$

$$
x_{i1}^\ast = 0.5L_iE_i^2(\hat{d}_i)^2 + 0.5C_i(V_i^\text{ref})^2
$$

For analysis above, it can be concluded that the objective of the primary control is to track the state $x_{i1}$ to the reference value $x_{i1}^\ast$ asymptotically. For this purpose, a new set of coordinates is introduced as,

$$
z_{i1} = x_{i1} - x_{i1}^\ast, \quad z_{i2} = x_{i2} - x_{i2}^\ast, \quad \delta_i = v_i - v_i^\ast
$$

Taking the derivative of $z_{i1}$ and $z_{i2}$ along their trajectory yields, the system in (13) is finally transformed to a canonical form as,

$$
z_{i1} = z_{i2} + (d_i - \hat{d}_i), \quad \dot{z}_{i2} = \delta_i
$$

In order to stabilize this dynamics, $\delta_i$ could be designed as the linear combination of $z_{i1}$ and $z_{i2}$, i.e., $\delta_i = -k_{i1}z_{i1} - k_{i2}z_{i2}$, where $k_{i1}$ and $k_{i2}$ are positive constants as the controller gains.

The closed-loop system above is globally asymptotically stable and the output voltage of DG$_i$ can track its reference value $V_{C_i}^\text{ref}$ asymptotically.

4. Stability Analysis

In this system, any trajectory of all the intermediate states will be uniformly bounded. The close loop system in (13) can be expressed as $\dot{z}_i = \Lambda_i z_i + \psi_i$, where $z_i = [z_{i1} \quad z_{i2}]^T$, $\Lambda_i = [0 \quad 1; -k_{i1} \quad -k_{i2}]$ and $\psi_i = [\hat{d}_i \quad 0]^T$ are system matrices. A Lyapunov equation is selected as $V_i = z_i^TP_i z_i$. $P_i$ is a positive definite and symmetrical matrix. The derivative, $\dot{V}_i = -\|z_i\|^2 + 2z_i^TP_i\psi_i \leq -\|z_i\|^2 + D_i \|z_i\|$, where $D_i = 2\lambda_{\text{max}}(P_i)\|\psi_i\| \leq 0.5D_i + 0.5\|z_i\|^2$, $\lambda_{\text{max}}(P_i)$ is the maximum eigenvalue of $P_i$. Hence the following relation holds $\dot{V}_i \leq -0.5\|z_i\|^2 + 0.5D_i^2 \leq -0.5\lambda_{\text{max}}^{-1}(P_i)V_i + 0.5D_i^2$.

For the global stability of the whole system, Lyapunov function $V$ can be expressed as $V = \sum V_i = Z^TPZ$, where $Z = [z_{11}^T \ldots z_{n1}^T]$ and $P = \text{diag}[P_1 \ldots P_n]$. The derivative of $V$ is $\dot{V} \leq -0.5\sum \|z_i\|^2 + 0.5\sum D_i^2 \leq -0.5\lambda_{\text{max}}^{-1}(P)V + D$, where $D = n \cdot \max \{D_i\}$,

- **Step 1:** Defining $\Omega_{\varepsilon} = \{z \in R^{2n} | V \leq \varepsilon\}$ where $\varepsilon > 0$ is a constant which can be arbitrarily small, it is apparent that $\Omega_{\varepsilon} \subset R^{2n}$. Choosing $k_{i1}$ and $k_{i2}$ sufficiently to satisfy $D \leq -0.5\lambda_{\text{max}}^{-1}(P)\varepsilon$. Then, for any value of $z \in R^{2n}$, $\dot{V} \leq -0.5\lambda_{\text{max}}^{-1}(P)V + D \leq 0$.

- **Step 2:** Since $\psi_i$ is zero at steady state, therefore $D = 0$ and then $\dot{V} \leq 0$. 

6
From the two steps above, the Lyapunov function is negative definite, and finally the whole system is stable.

5. Simulation Results

System model described by Table 1. with the proposed controller above is simulated in MATLAB/Simulink to validate the effectiveness of the proposed isolation scheme.

Figure 6 (a) and (b) show the comparison of converters’ voltages and power dynamic with or without isolation in case 1. The system operates normally before $t = 0.5s$, when false data attack launched, the oscillations of voltages and currents are obvious and which cause the power allocation error among all the DGs. In contrast, utilizing the proposed isolation method, the attack is detected at $t = 0.5s$, the system changes the communication network and a new agreement is reached between DG2 and DG3. In particular, the isolation causes variation of power loads to every converter. The robustness of the suggested domination controller ensures the stability of all the DGs when loads change. Accordingly, the voltages of DG2 and DG3 restore to the reference value 100V, and the voltage of DG1 drops due to droop mechanism correspondingly. Fig. 7(b) also shows the isolation of DGi prevents the power sharing from the preset proportion being deteriorated. The dynamics of the voltage and output power of DGi of case 2 are shown in Fig. 8-9.

From Fig. 8 (a), it is indicated that the voltage of DGi become deviant under the constant data attack at $t = 0.5s$ and the system will eventually turn to unstable. In Fig. 9 (a), power sharing also degrades since $t = 0.5s$. However, when employing the isolation method, the DG2 is offline and its voltage drops after when FDIA signal is detected at $t = 0.6s$, which can be seen Fig. 8 (a). The DG2 only supply its local load and the power output of DG1 and DG3 rapidly restore rational proportion in Fig. 9 (b) after $t = 0.6s$.

![Figure 5. Converter voltages considering the link between DG1 and DG2 under sinusoid FDIA.](image1)

![Figure 6. Power allocation considering the link between DG1 and DG2 under sinusoid FDIA.](image2)

![Figure 7. Converter voltages considering the link between DG1 and DG2 under constant FDIA.](image3)

![Figure 8. Power allocation considering the link between DG1 and DG2 under constant FDIA.](image4)
6. Conclusions
In this paper, a novel FDIA isolation scheme for a networked distributed DC microgrid system is proposed. First, a new kind of attack detection observer has been presented in secondary control layer. Based on NDO, the proposed observer can ensure the accurate estimation of FDIA signal in communication link of cyber layer in MG. Subsequently, we propose a mechanism to isolate the misleading agents to alleviate voltage degradation. The suggested domination controller ensures the dynamic property and stable state performance in switching network connection. The proposed isolation strategy could provide a more resilient implementation choice for DC microgrids which might be confronted with FDIA.

Acknowledgments
This work is supported by Shanghai Rising-Star program (NO. 20QA1404000).

References
[1] Beg, O. A., Johnson, T. T., and Davoudi, A. (2017) Detection of False-Data Injection Attacks in Cyber-Physical DC Microgrids. IEEE Transactions on Industrial Informatics, vol. 13, no. 5, pp. 2693-2703.
[2] Srikantha, P. and Kundur, D. (2015) Denial of service attacks and mitigation for stability in cyber-enabled power grid. In: IEEE Power Energy Society Innovative Smart Grid Technologies Conference (ISGT), pp. 1-5.
[3] Zhong, X. and Yu, L. and Brooks, R. and Venayagamoorthy, G. K. (2015) Cyber security in smart DC microgrid operations,” In: IEEE First International Conference on DC Microgrids (ICDCM), pp. 86-91.
[4] Y. Yan and Y. Qian and Sharif, H. and Tipper, D. (2012) A Survey on Cyber Security for Smart Grid Communications. J IEEE Communications Surveys Tutorials, vol. 14, no. 4, pp. 998-1010.
[5] Liu, S. and Liu, X.P. and Wang, X. (2016) Effects of cyber attacks on islanded microgrid frequency control. In: IEEE 20th International Conference on Computer Supported Cooperative Work in Design (CSCWD), pp. 461-464.
[6] Abhinav, S. and Modares, H. and Lewis, F. L. and Davoudi, A. (2014) Resilient Cooperative Control of DC Microgrids. J IEEE Transactions on Smart Grid, vol. 1, no. 4, pp. 370-379.
[7] Pasqualetti, F. and Bicchi, A. and Bullo, F. (2012) Consensus Computation in Unreliable Networks: A System Theoretic Approach. J IEEE Transactions on Smart Grid, vol. 57, no. 1, pp. 90-104.
[8] Abhinav, S. and Schizas, I. D. and Lewis, F. L. and Davoudi, A. (2018) Distributed Noise-Resilient Networked Synchrony of Active Distribution Systems. J IEEE Transactions on Smart Grid, vol. 9, no. 2, pp. 836-846.
[9] Guo, F. Xu, Q. Wen, C. Wang, L. and Wang, P. (2018) Distributed secondary control for power allocation and voltage restoration in islanded dc microgrids,” J IEEE Transactions on Sustainable Energy, vol. 9, no. 4, pp. 1857-1869.
[10] Q. Xu, C. Zhang, C. Wen and P. Wang, (2019) A Novel Composite Nonlinear Controller for Stabilization of Constant Power Load in DC Microgrid. J IEEE Transactions on Smart Grid, vol. 10, no. 1, pp. 752-761.
[11] Q. Xu, Y. Xu, C. Zhang and P. Wang, (2020) A Robust Droop-Based Autonomous Controller for Decentralized Power Sharing in DC Microgrid Considering Large-Signal Stability. J IEEE Transactions on Industrial Informatics, vol. 16, no. 3, pp. 1483-1494.
[12] P. Lin, C. Zhang, P. Wang and J. Xiao, (2020) A Decentralized Composite Controller for Unified Voltage Control With Global System Large-Signal Stability in DC Microgrids. J IEEE Transactions on Smart Grid, vol. 10, no. 5, pp. 5075-5091.