A DECENTRALIZED UNKNOWN INPUT OBSERVER-BASED FALSE DATA INJECTION DETECTION FRAMEWORK FOR DC MICROGRIDS

Anik Ghosh[1], Sajal k. Das[2], Yao Gao[3], Guo Chen[4], S.M Muyeen[5]*

[1]*Department of Mechatronics Engineering, Rajshahi University of Engineering and Technology, Bangladesh*
[2]*School of computer science, Queensland University of Technology, Brisbane, Australia*
[3]*Department of Electrical Automation, Shanghai Maritime University, Shanghai, China*
[4]*School of Electrical Engineering and Telecommunications, The University of New South Wales, Sydney, Australia*
[5] *Department of Electrical Engineering, Qatar University, Doha 2713, Qatar*
**anik21.mte.ruet@gmail.com*

Keywords: ATTACK DETECTION, FDI, DC MICROGRID, DUIO

Abstract

Dc microgrid cluster are widely adopted due to flexible utilization of renewable energy sources. However, their reliance on communication networks, make them vulnerable to stealthy cyber-attacks which can disrupt system dynamics and lead to unstable microgrid operation. To address this critical issue, a decentralized unknown input observer (DUIO) based false data injection (FDI) attack detection framework is proposed. First, a comprehensive modelling of DC microgrid cluster is developed considering line resistance, loads, grid forming converter, unknown disturbances. Subsequently, an unknown input observer (UIO) is carefully designed to monitor system dynamics. When malicious data is injected into measurement, UIO incorporates residual checking technique along with threshold comparing procedure to identify cyber-attack. To validate the framework, microgrid model tested in MATLAB environment against three distinct categories of FDI attacks and load changing scenario. The results show robust performance in terms of cyber-attack detection in DC microgrids which is essential for stable grid operations.

1. Introduction

In recent days, DC microgrid (MG) cluster has been adopted because of having flexible utilization of renewable energy sources [1] Additionally, it has been regarded as a promising remedy for the problems like economic energy production, energy conversion and transmission losses, and constant supply of energy[2]. While reducing control complexities, DC MG cluster offers both grid connected and islanded mode control making them suitable for applications in power generation and transportation systems[3].

Though having these advantages, because of highly reliance on communication due to co-operative control make them vulnerable to cyber-attacks[4]. A few notable incidents like Natanz nuclear plant attack, US oil resource attack[5]. Then, to enhance the resilience against these attacks, it is important to implement counter measures against these attacks. To keep the system stable, detection of cyber-attack is the first and foremost criteria and based on this detection counter measures can be implemented.

Efforts have been made to design architectures to detect cyber-attacks including false data injection (FDI), replay attacks, distributed denial of service (DDOS), latency attacks in power systems. These architectures rely on either deterministic or probabilistic approach.

Probabilistic approaches utilize data driven detection scheme, including machine learning (ML) techniques to detect cyber-attacks. ML techniques like Artificial neural network (ANN), long short-term memory (LSTM), deep learning (DL), ensemble learning (EL), auto encoder, pattern recognition are commonly used in detection scheme[6]. These data driven techniques demonstrate decent performances in term of FDI attack detection. Though having outstanding detection rate, these techniques require large datasets. Additionally, higher computational complexity and latency in detection make them incompatible in large DC Microgrid Cluster.

On the contrary, model-based detection approaches utilize system dynamics to monitor unusual changes in states and flag cyber-attack. In compared to data driven approaches, model-based detection offers less computational overhead and mitigate the issue of higher latency in detection. Various model-based approaches like parity based[7] attack detection utilize decomposition technique to detect FDI attack. Similar technique like Observer based detection techniques have appeared as a promising solution to detect FDI attack. This study [8] utilizes Luenberger observer which incorporates residual technique to detect cyber-attack. But Luenberger observer, which is based on all known input assumption, is not feasible in most practical cases due to linearization error of system modelling and disturbances.

To tackle this limitation, this study proposed a distributed unknown input observer (DUIO) where a separate UIO is coupled with each MG of the cluster. DUIO estimates system states accurately in case of unknown inputs like disturbances, system modelling errors and change in loads. Consequently,

residual is only sensitive to FDI and offer robust performance against load changes and other disturbances. This framework computes the residual based on attacked measurements and estimated measurements. Furthermore, it compares the residual with predefined threshold and flags FDI attack in case of residual surpluses the threshold. This proposed framework is evaluated in MATLAB Simulink against FDI, load changing conditions and disturbances to demonstrate the efficacy and proposed one demonstrated an outstanding performance in case of detect stealthy FDI. This paper is organized as follows: following introductory section, methodology section provides detailed methodology of proposed framework, and it is validated in result section. Finally, last section concludes the paper.

2. Methodology

2.1 System modelling

The DC microgrid cluster consists of 4 interconnected grids illustrated in Fig. 1. Subsequently, grid *i* of the cluster can be modelled as using (1) and (2) considering cyber-attack initiated by altering the states.

$$\dot{x}(t+1) = A\,x(t) + B\,u(t) + E_d\,D(t) + F_a\,\alpha(t) \quad (1)$$

$$y(t) = C\,x(t) \quad (2)$$

where $x(t) \triangleq [V_i, I_i]$ represent PCC voltage and filter current of i^{th} coupling point. Subsequently, $\boldsymbol{A}$ matrix defines inter-

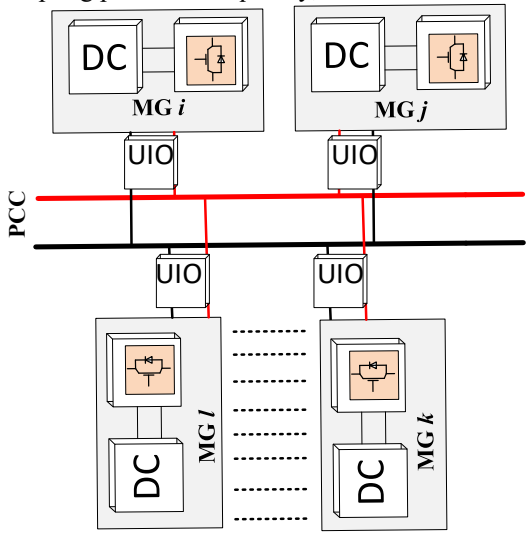


Fig. 1 Proposed DC microgrid Cluster with DUIO

relation between states, while $\boldsymbol{B}$ matrix defines how input affect states and matrix $\boldsymbol{E_d}$ and $\boldsymbol{F_a}$ defines disturbance and attack matrix respectively. Furthermore, α is denoted as FDI attack and *D* is disturbances due to unmodeled dynamics like high switching of Buck converter. Last of all, matrix C governs output relation and outputs of each coupling point are PCC voltage and filter current.

2.1 Attack modelling

When system measurement is affected by inaccurate data is considered as FDI attack. In this study, DC gain bias attack (a constant bias injected into system), time varying ramp attack and sinusoidal attack are considered are listed in Table 1.

Table 1. Cyber-attack injected in this study

Attack Type	Attack Value
DC gain bias	$\alpha_1 = 1.5$
Ramp	$\alpha_2 = 1 + 0.5t$
Sinusoidal	$\alpha_3 = 3 + sin(0.4\pi * t)$

2.2 DUIO framework

This section outlines the architectural design of the proposed Decentralized Unknown Input Observer (DUIO) framework for dynamic state estimation in the microgrid (MG) cluster, as depicted in Fig. 1. In the framework, each MG is integrated with its own Unknown Input Observer (UIO). Traditional observers, such as the Luenberger observer, are not suitable for this application, as they require complete knowledge of all system inputs for accurate state estimation. To overcome this limitation, UIO-based estimation is adopted, offering a robust approach capable of accommodating unknown inputs like external disturbances and linearization errors commonly encountered in power system models[9].

2.2.1 Design of UIO: Let us define, a virtual dynamic system (stated as observer) in (3) and estimated states are computed using (4) where ***F, T, K, H*** are the matrices needed to be designed.

$$\dot{z} = Fz(t) + TBu(t) + Ky(t) \quad (3)$$

$$\hat{x} = z(t) + H\,y(t) \quad (4)$$

To effectively observe the system described in equation (2), the state estimation error e(t) must asymptotically approach zero over time.

$$e(t) = \hat{x} - x \quad (5)$$

UIO design procedure is outlined in Algorithm 1. Initial step consists of checking two sufficient conditions 1) *rank (CE) = rank(E)* and 2) *(C, A1)* is observable where, $A1 = A - E[(CE)^T(CE)]^{-}1(CE)^T CA$. After that, design matrices are computed satisfying the conditions outlined in [10] which ends the process of UIO design. Subsequently, UIO is ready to estimate accurate estimation If all the mentioning conditions are satisfied. These can be used for FDI attack detection, and the methodology is described in the following section.

Algorithm 1: DUIO based attack detection framework

Input	*Measurement ($\boldsymbol{V_i}$, $\boldsymbol{I_i}$), input u(t), $\boldsymbol{A_i}$,$\boldsymbol{B_i}$, $\boldsymbol{E_{id}}$, $\boldsymbol{C_i}$*
Output	*Attack Flag F_{fdi}*
1	***UIO design for i^{th} measurement***
2	*Step 1: Check rank condition*
3	*Step 2: Check observability*
4	*Step 3: Compute F, T, K, H*
5	***Residual based Attack Detection***
6	*Step 1: Collect corrupted measurements*
7	*Step 2: Compute estimated states using (6)*
8	*Step 3: Generate residual using (7)*
9	*Step 4: Check residual cross threshold*
10	*Step 5: Assign F_{fdi} based on step 4*

2.2.1 FDI attack detection using UIO: After observer design, this section outlines how DUIO can be utilized to detect FDI attack. This proposed DUIO operates individually in a decentralized manner in MG cluster by generating the residual between estimated states and measurements by using (7). Where estimated states are computed utilizing (6) using the estimated states of UIO.

$$\hat{\boldsymbol{y}}(\boldsymbol{t}) = \boldsymbol{C}\,\boldsymbol{z}(\boldsymbol{t}) + \boldsymbol{C}\,\boldsymbol{H}\,\boldsymbol{y}(\boldsymbol{t}) \quad (6)$$

$$\boldsymbol{r}(\boldsymbol{t}) = \boldsymbol{y}(\boldsymbol{t}) - \hat{\boldsymbol{y}}(\boldsymbol{t}) \quad (7)$$

The entire residual generation process is illustrated using block diagram representation of attack detection framework in Fig.2.

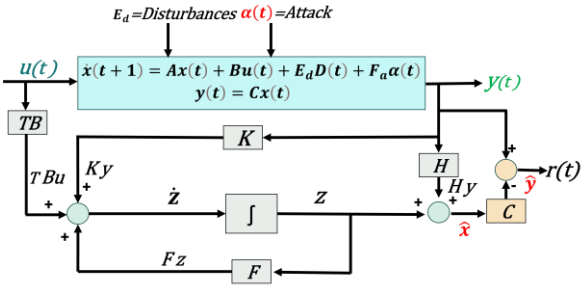


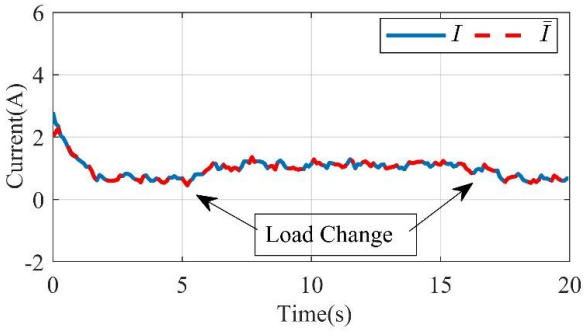
Fig. 2 Cyber-attack detection block diagram

Assuming, among states voltage measurement has encountered stealthy FDI attack during communication. Then, UIO estimates the states based on system dynamics and estimated states are utilized to compute estimated measurements. As voltage contains false data, the estimated states will vary and generate residual and based on this residual this proposed framework will detect attack. For accurate detection and reduce false positives due to measurement noise, proposed method incorporates a threshold where, it computes L_2 norm of residual ||r(t)||. Finally, ||r(t)|| is compared with threshold and flags F_{fdi} in case of it cross the threshold.

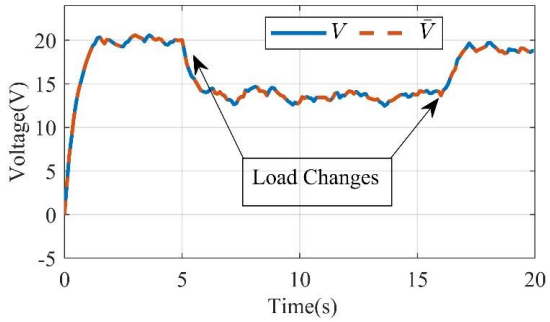
3. Results

3.1 Simulated results

To evaluate the effectiveness of the proposed DUIO-based framework, a DC microgrid cluster comprising four units is modelled in MATLAB Simulink, as shown in Fig. 1. Each microgrid (consists of grid forming converter and load) is integrated with its own DUIO and interconnected with others via line impedance. The cluster is subjected to controlled stealth FDI attacks to assess the performance of the detection framework.



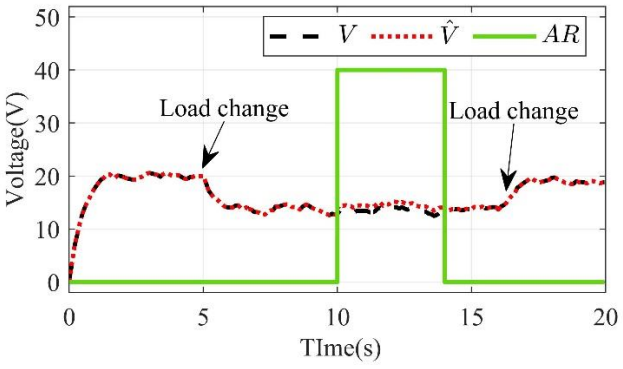
a



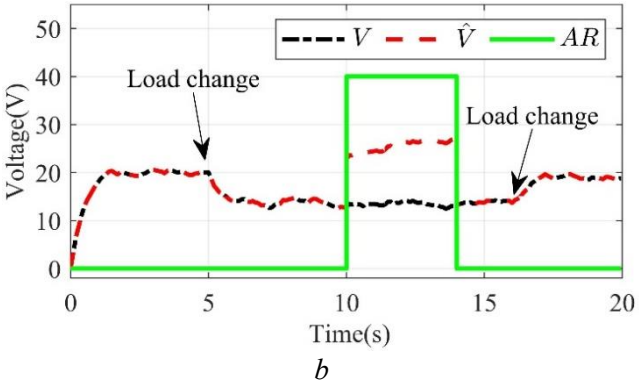
b

Fig. 3 Estimation performance of DUIO framework (a) Authentic current (blue solid line) and DUIO estimated current (red dash line) (b) Authentic voltage (blue solid line) and DUIO estimated voltage (red dash line)

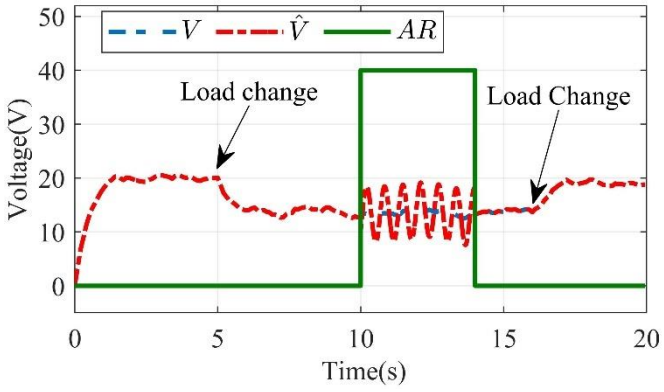
The parameters used in the simulated environment for this study are summarized in Table 2. To demonstrate the effectiveness, proposed methodology has passed through different cyber-attack conditions and three types of False Data Injection (FDI) attacks are introduced during the simulation: DC gain bias, time-varying sinusoidal, and ramp attacks, all occurring within the time window of 10 to 14 seconds. To evaluate the dynamic state estimation capability of the proposed DUIO framework, the estimated voltage and current of grid i are presented in Fig. 3. A comparison between the estimated and actual state values demonstrates that the DUIO provides accurate estimation. Furthermore, these estimation performance under load changing condition and disturbances. The Fig. 3 depicts minimal estimation error in both cases. This accuracy is attributed to the DUIO's ability to effectively reject unknown inputs.



a



b



c

Fig. 4 Detection performance (a) DC gain bias attack with (parrot green solid), attacked voltage (red dotted) and original voltage (black dashed) lines, (b) Ramp attack with (parrot green solid), attacked voltage (red dotted) and original voltage (black dashed) lines, (c) Sinusoidal attack with (green solid), attacked voltage (red dotted) and original voltage (blue dashed) lines.

Table 2. Simulated environment parameters

Module	Parameter	Value
DC Microgrid	Nominal Voltage	20 V
	Switching frequency	8 kHz
LC filter	Inductor resistance	0.10 Ω
	Inductor inductance	1.8 mH
	DC bus capacitance	2.2 mF

Furthermore, the detection performance is demonstrated in Fig. 4, where the DUIO-based framework is evaluated against three types of FDI attacks. The results confirm the robustness of the proposed method in identifying severe FDI threats. In addition, the framework exhibits reliable detection capabilities under varying load conditions and in the presence of unknown disturbances. To assess its sensitivity, a low-magnitude FDI attack was introduced, and the framework successfully detected even this minimal intrusion, highlighting its effectiveness in identifying subtle attack scenarios.

4. Conclusion

In this study, vulnerability of DC microgrid cluster against FDI attack during communication has investigated. The impact of three types of FDI from attacker perspective has discussed and applied into the cluster. To construct a defend mechanism, a distributed unknown input observer-based attack detection framework has proposed. This proposed method utilizes residual generation technique which is formulated to detect stealthy FDIs by generating higher residual value. Higher residual value triggers attack presence alarm which can be to construct mitigation scheme. Detection methodology has been tested against stealthy FDIs. Additionally, load changing conditions and disturbances have also feed into system to demonstrate the efficacy of this proposed method.

Acknowledgements

This research was supported by the Australian Research Council (ARC) Linkage Project LP200100056 and the 4th Cycle of MME Grant No. MME04-0607-230060, from the Qatar Research, Development and Innovation (QRDI) Council, in collaboration with the Ministry of Municipality, Qatar. The authors would like to thank Dr. G. Yao for his contribution and support.

5. References

[1] A. O. Aluko, R. P. Carpanen, D. G. Dorrell, and E. E. Ojo, "Real-Time Cyber Attack Detection Scheme for Standalone Microgrids," IEEE Internet Things J, vol. 9, no. 21, pp. 21481–21492, 2022, doi: 10.1109/JIOT.2022.3180939.

[2] S. Li and W. Wu, "Adaptive Voltage Control to Coordinate Multiple PV Inverters as a Cluster," IEEE Trans Smart Grid, vol. 15, no. 6, pp. 5526–5538, 2024, doi: 10.1109/TSG.2024.3422381.

[3] L. Wang et al., "Grid Resilience Enhancement and Stability Improvement of an Autonomous DC Microgrid Using a Supercapacitor-Based Energy Storage System," IEEE Trans Ind Appl, vol. 60, no. 2, pp. 1975–1985, 2024, doi: 10.1109/TIA.2023.3330455.

[4] N. Mosaad, O. Abdel-Rahim, W. Rohouma, and S. M. Abdelkader, "Identification and Alleviation of False Data Injection Within the Cyber Layer of an Enhanced Distributed Secondary Control in DC Islanded Microgrids," IEEE Access, vol. 13, pp. 48605–48624, 2025, doi: 10.1109/ACCESS.2025.3547724.

[5] H. Shafei, L. Li, and R. P. Aguilera, "A comprehensive review on cyber-attack detection and control of microgrid systems," Power Systems Cybersecurity: Methods, Concepts, and Best Practices, pp. 1–45, 2023.

[6] H. Shafei, L. Li, and R. P. Aguilera, "A Comprehensive Review on Cyber-Attack Detection and Control of Microgrid Systems," in Power Systems Cybersecurity: Methods, Concepts, and Best Practices, H. Haes Alhelou, N. Hatziargyriou, and Z. Y. Dong, Eds., Cham: Springer International Publishing, 2023, pp. 1–45. doi: 10.1007/978-3-031-20360-2_1.

[7] S. Tan, P. Xie, J. M. Guerrero, and J. C. Vasquez, "False Data Injection Cyber-Attacks Detection for Multiple DC Microgrid Clusters," Appl Energy, vol. 310, p. 118425, 2022, doi: https://doi.org/10.1016/j.apenergy.2021.118425.

[8] X. Wang, X. Luo, M. Zhang, Z. Jiang, and X. Guan, "Detection and Isolation of False Data Injection Attacks in Smart Grid via Unknown Input Interval Observer," IEEE Internet Things J, vol. 7, no. 4, pp.

3214–3229, 2020, doi: 10.1109/JIOT.2020.2966221.

[9] T. N. Pham, H. Trinh, and L. V Hien, “Load Frequency Control of Power Systems With Electric Vehicles and Diverse Transmission Links Using Distributed Functional Observers,” IEEE Trans Smart Grid, vol. 7, no. 1, pp. 238–252, 2016, doi: 10.1109/TSG.2015.2449877.

[10] H. H. Alhelou and P. Cuffe, “A Dynamic-State-Estimator-Based Tolerance Control Method Against Cyberattack and Erroneous Measured Data for Power Systems,” IEEE Trans Industr Inform, vol. 18, no. 7, pp. 4990–4999, 2022, doi: 10.1109/TII.2021.3093836.