Impact of Cyber Attacks on Cost Oriented Power Routing Schemes in Microgrids

Kirti Gupta[1], Subham Sahoo[2], Bijaya Ketan Panigrahi[1], and Frede Blaabjerg[2]

[1]Department of Electrical Engineering, Indian Institute of Technology, Delhi, 110016, India
Email: {Kirti.Gupta, Bijaya.Ketan.Panigrahi}@ee.iitd.ac.in
[2]Department of Energy, Aalborg University, Aalborg, 9220, Denmark
Email: {sssa, fbl}@energy.aau.dk

Keywords

≪Cooperative energy management (CEM)≫, ≪economic dispatch (ED)≫, ≪real- time (RT) simulation≫, ≪microgrid (MG)≫, ≪cyber attack≫.

Abstract

The distributed economic dispatch (ED) algorithm carried out in an AC microgrid (MG) is a promising solution which guarantees flexibility, scalability and reliability over single point failure as compared to the centralized approach. Not to mention, the integration of communication infrastructure for information exchanges on one hand adds feasibility for the distributed operation but at the same time, is a threat to the smart grid. The attackers can penetrate in the communication links and inject malicious data in order to gain economical benefits, disrupt the proper functioning of the system etc. Hence, the investigation of the effect of cyber attacks on cooperative energy management (CEM) is an important concern both theoretically and practically. This paper analyses the impact of cyber attacks on a CEM, optimizing ED to a sub-optimal value in an islanded AC MG. The response of the system over false data injection (FDI) and hijacking attacks is further demonstrated on a real-time (RT) co-simulation platform.

Introduction

With the increase in environmental pollution and energy crisis globally, the shift towards cleaner and greener energy solutions have been escalating. Such a shift leads to the development of a smart grid, integrated with advanced control technologies, communication infrastructures, etc. MG plays a major role in integrating these future energy sources which are environmental-friendly. MGs with the hierarchical control structure consists of primary, secondary and tertiary control layers. The later being slowest of all with a time-scale of operation seconds to minutes [1] is responsible for cost-oriented power routing schemes i.e, ED and unit commitment. However, in future with large integration of inverter based distributed generations (DGs), with intermittent nature would degrade the economic efficiency if ED is a part of tertiary control. In order to reduce the time gap of operation and increase the economic efficiency, ED is integrated in the secondary control layer with a time-scale of operation between 100 ms and 1 s.

Further, with integration of information and communication technologies (ICT), distributed control and optimization is preferred to enhance the flexibility, scalability and reliability with respect to its traditional counterpart. Hence, distributed algorithms are promising solutions for ED problem in a MG. The CEM allocates multiple DG units to meet the demand to minimize the total generation cost in a distributed manner [2]. The RT cooperative control plays a vital role in achieving the objectives of frequency restoration, proportional reactive power sharing and ED at the same time [3]. Moreover, the communication cost is also reduced as the information regarding loads are not required.

The information exchanges makes the system vulnerable to cyber attacks. The cyber attacks can disrupt the data confidentiality, integrity and availability [4]. with the increase in integration of DGs and hence the communication links between them has deepened the problem further. An attacker can penetrate in the communication link and malicious attack the information being exchanged. This can cause a chain reaction and affect the normal operation of the system. Hence, this work is dedicated to investigate the impact of cyber attacks on CEM system in an AC MG. Among data integrity and data availability attacks [5, 6], this paper primarily focuses on the later one [7, 8, 9], which can be either FDI and hijacking attacks [10, 11, 12]. These attacks may lead to instability, uneconomic operation, or even shut down of the system. Hence, exploring the impact of various cyber attacks is of a practical value. The paper investigates the impact of cyber attacks on ED optimization problem, affecting the generation cost of a DG to settle at a sub-optimal value. Further, a RT simulation has been performed on a co-simulation testbed. The analysis has been carried out on a four bus test MG system integrated with DGs.

The main contributions of this paper are summarized as follows:

- investigating the impact of cyber attacks on information exchanged, optimizing the generation cost of a DG to a sub-optimal value;
- demonstrating FDI and hijacking attacks and its effect on cost of generation, and the objectives of frequency restoration, proportional reactive power sharing and ED;
- RT testing of a CEM of an islanded AC MG on a co-simulation platform.

The remainder of the paper is organized as: preliminaries on graph theory, control of MG in islanded mode of operation and CEM is presented at first. Various cyber vulnerabilities like FDI, hijacking attacks and variation of cost parameters are discussed further followed by the experimental results. Finally, the work is concluded.

Preliminaries

This section presents some useful preliminaries required for analysis. Various notations used in the further sections are illustrated in this section.

Graph Theory

Let us consider an islanded MG with 'N' DGs connected via communication links. The communication topology of the system can be expressed as a graph with nodes (V) being the DGs and the edges (E) representing the communication links. The graph can be expressed as $G = (V, E, A)$, where $V = 1, 2, ..., N$; $E \subset V \times V$; adjacency matrix, $A = (a_{ij})_{N \times N}$ where (i,j $\in$ V). The graph considered in this work is bidirectional. Each entry (a_{ij} of the adjacency matrix (A) represents the communication weight. The weight $a_{ij} > 0$ if $(i, j) \in E$, otherwise $a_{ij} = 0$. Further, N_i is denoted as a set of neighbouring DGs to i^{th} DG expressed as, $N_i = \{j \in V | (j, i) \in E\}$. The laplacian matrix ($L$) can be expressed in terms of A and in-degree matrix (D) as $L = D - A$. Here, D can be expressed as $diag(d_1, d_2, ...d_N) \in R^{N \times N}$ where, $d_i = \sum_{j \in N_i} a_{ij}$ is known as weighted in-degree of node i [13].

Primary and Secondary Control of Microgrid

The basic control structure of an islanded MG consisting of primary and secondary controllers is presented in the Fig. 1a. The primary control comprises of three control loops namely, droop control, voltage control and current control. As primary control is not sufficient to drive the system to zero steady state error, hence secondary control is integrated to generate frequency and voltage correction terms to achieve this objective.

The droop control for i^{th} DG can be expressed as:

$$\omega^i = \omega_{ref} - m_p^i . P^i \tag{1}$$

$$V_d^i = V_{ref} - n_q^i . Q^i \tag{2}$$

$$V_q^i = 0 \tag{3}$$

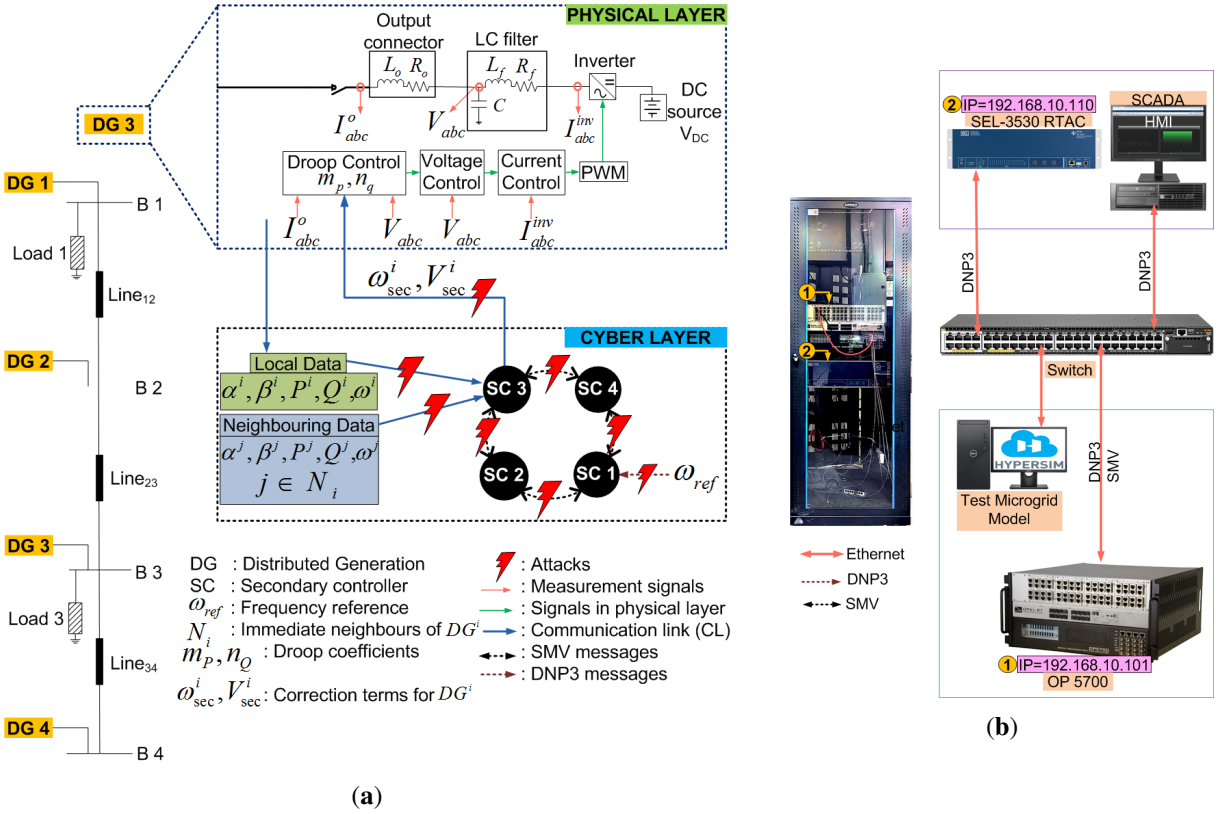

Fig. 1: RT co-simulation platform **(a)** Test MG model with four DGs, **(b)** Testbed setup.

where, ω_{ref} and V_{ref} are the reference frequency and voltage of the system. Further,m_p and n_q are the constant active and reactive power droop coefficients; P and Q are the active and reactive power; V_d and V_q are the d-axis and q-axis voltages; ω is the frequency. Moreover, superscript 'i' denotes the corresponding quantities of an i^{th} DG.

The secondary control is integrated to compensate for the frequency and voltage deviations caused by the primary control. Conventionally, centralized framework was incorporated but with the advancement of ICT, distributed control architecture is preferred. It is scalable, flexible, relieves computational burden, support plug and play functionalities [14]. The overall equation consisting of both primary and secondary control can be expressed as:

$$\omega^i = \omega_{ref} - m_p^i.P^i + \omega_{sec}^i \tag{4}$$

$$V_d^i = V_{ref} - n_q^i.Q^i + V_{sec}^i \tag{5}$$

where, ω_{sec} and V_{sec} are the frequency and voltage correction terms generated by the secondary controller. Such a distributed secondary control architecture helps to restore frequency to the reference values, to proportionally share active/reactive power among the DGs.

Cooperative Energy Management

The term ED refers to allocating the resources (say DGs) to meet the demand in a most economic way. To estimate the total cost of the output power provided by the DGs, cost function is used. Assuming the cost of generation for i^{th} DG (C^i) be expressed as a quadratic function [15, 16], represented by (6)

$$C^i(P^i) = \alpha^i(P^i)^2 + \beta^i P^i + \gamma^i \tag{6}$$

where, P^i denotes the power generated by i^{th} DG; and α^i, β^i and γ^i are the cost coefficients. In order to

minimize the total generation cost while maintaining the balance of supply and demand, it is mandatory to equalize the incremental cost of each DG. Upon differentiating (6) with respect to P^i, we obtain incremental cost function expressed by (7)

$$\eta^i(P^i) = 2\alpha^i P^i + \beta^i \tag{7}$$

The overall system can be regarded as a multiagent system, with each DG as an agent. The agents exchange the information related to active power, incremental cost to achieve the objective of economic dispatch and at the same time balancing the generation and load demand through distributed algorithm. Furthermore, incorporating this objective in the secondary controller of an islanded MG, the objectives of frequency restoration, ED and proportional reactive power sharing are achieved at the same time.

The overall frequency control equation comprising of primary and secondary controllers can be expressed by (8), and the frequency correction term generated by is represented by (9), with $K^i_{p\omega}$ and $K^i_{i\omega}$ being the proportional and integral gains [17]. The error term is further represented by (10). Similarly, the equations corresponding to cooperative voltage controller can be derived.

$$\omega^i = \omega_{ref} - \eta^i(P^i) + \omega^i_{sec} \tag{8}$$

$$\omega^i_{sec} = K^i_{p\omega}\dot{e}^i_{\omega} + K^i_{i\omega}e^i_{\omega} \tag{9}$$

$$\dot{e}^i_{\omega} = -\sum_{j\in N_i} a_{ij}\left(\eta^i(P^i) - \eta^j(P^j)\right) - \sum_{j\in N_i} a_{ij}\left(\omega^i - \omega^j\right) - \sum_{j\in N_i} g_i\left(\omega^i - \omega_{ref}\right) \tag{10}$$

The objectives of this control architecture can be mathematically expressed as:

1. To restore the frequency of each DG (ω^i) to the reference value (ω_{ref}):

$$\lim_{t\to\infty} \omega_i(t) = \omega_{ref} \tag{11}$$

2. To achieve the optimal active power sharing:

$$\lim_{t\to\infty} [\eta^j(P^j) - \eta^i(P^i)] = 0 \tag{12}$$

3. To realize the proportional reactive power sharing:

$$\lim_{t\to\infty} [n^j_q Q^j(t) - n^i_q Q^(t)] = 0 \tag{13}$$

where j$\in N_i$. i.e., all the immediate neighbors of i^{th} DG.

Cyber Vulnerabilities

The adversaries can target either the nodes of communication links in the cyber-physical model of MG [18]. Depending on the target, attack can be classified in two categories which can be described as:

- The attacks targetted by adversaries on the communication links can be grouped under false data injection (FDI) attacks;
- The attack targetting the controllers to generate the unfair commands can be agrregated as hijacking attacks.

Based on these definitions, the attacked entities and the attack equations can be formulated as described in the section further.

False-Data Injection Attacks:

The well-crafted FDI attack can hide its presence, commonly termed as *deception (or stealth)* attacks. The attacker can later on inject unfair attack value, commonly termed as *destablization* attacks, to disrupt the control functionality leading to system instability. Assuming the information exchange vector be $x^i(t)$=[$\alpha^i(t)$, $\beta^i(t)$, $P^i(t)$, $Q^i(t)$, $\omega^i(t)$] and constant attack element be x^{iA}, then FDI attack is expressed as:

$$x^{iF}(t) = x^i(t) + x^{iA}(t) \tag{14}$$

Hijacking Attacks:

The hijacking attacks can be represented by:

$$x^{iH}(t) = (1-\varphi^H)x^i(t) + \varphi^H x^{iA}(t) \tag{15}$$

where, φ^H is a binary number, indicating hijacking attack if 1, otherwise no attack. It poses difficulty in detecting the attacked agent as such an attack causes all the agents to behave in an abnormal way.

The characteristic feature of FDIA is that, the attack value is added to the existing signal, this may although allow to reach a consensus but the converged value may be incorrect. On the contrary, the hijacking attacks are carried out by completely replacing the existing signal. This disrupts the update process of consensus algorithm. To address the formulation of such attacks and response of CEM system under such attacks, a four bus islanded AC MG is studied on a RT co-simulation testbed.

Variation in Cost of Generation:

As discussed, the third-party adversary can attack on any of the variables being exchanged, deviating the optimal solution to a sub-optimal value. Substituting (6), (7), (9) and (10) in (8), we get

$$\eta^i(P^i) = \left[1 + K^i_{p\omega}\sum_{j\in N_i} a_{ij}\right]^{-1} \begin{bmatrix} \omega_{ref} - \omega^i + K^i_{p\omega}\sum_{j\in N_i} a_{ij}\eta^j - K^i_{p\omega}\omega^i \sum_{j\in N_i} a_{ij} + K^i_{p\omega}\sum_{j\in N_i} a_{ij}\omega^j - \\ K^i_{p\omega}\omega^i \sum_{j\in N_i} g_i + K^i_{p\omega}\omega_{ref}\sum_{j\in N_i} g_i + K^i_{i\omega}e^i_\omega \end{bmatrix} \tag{16}$$

From (16), (7) and (6), we can further find the deviation of cost of generation of a DG in terms of the attacked variables. The variation of cost of generation is further analyzed with attack on cost parameter (α^1, α^2) and active power (P^1) in the next section.

Experimental Results

The co-simulation testbed with a dedicated Ethernet-based network integrated via switch is shown in the Fig.1b. The testbed comprises of OP-5700, which is a RT simulator to emulate the MG test system; SEL-3530 Real-Time Automation Controller (RTAC) hardware integrated with ACSELERATOR RTAC SEL-5033 software for monitoring application. The cyber-physical layer of MG comprising of the primary and secondary control layers are modelled in HYPERSIM software and integrated with OP-5700. A human machine interface (HMI) is developed in ACSELERATOR Diagram Builder SEL-5035 software monitoring and controlling functionalities (locally/remotely). The cyber layer of the MG is linked through various communication protocols such as, sampled message values (SMV) and distributed network protocol (DNP3). The information of frequency, active/reactive power, cost parameters are exchanged via SMV to achieve the objectives of frequency restoration, proportional active/reactive power, ED through CEM architecture. Further, DNP3 protocol is used to monitor the network parameters [9].

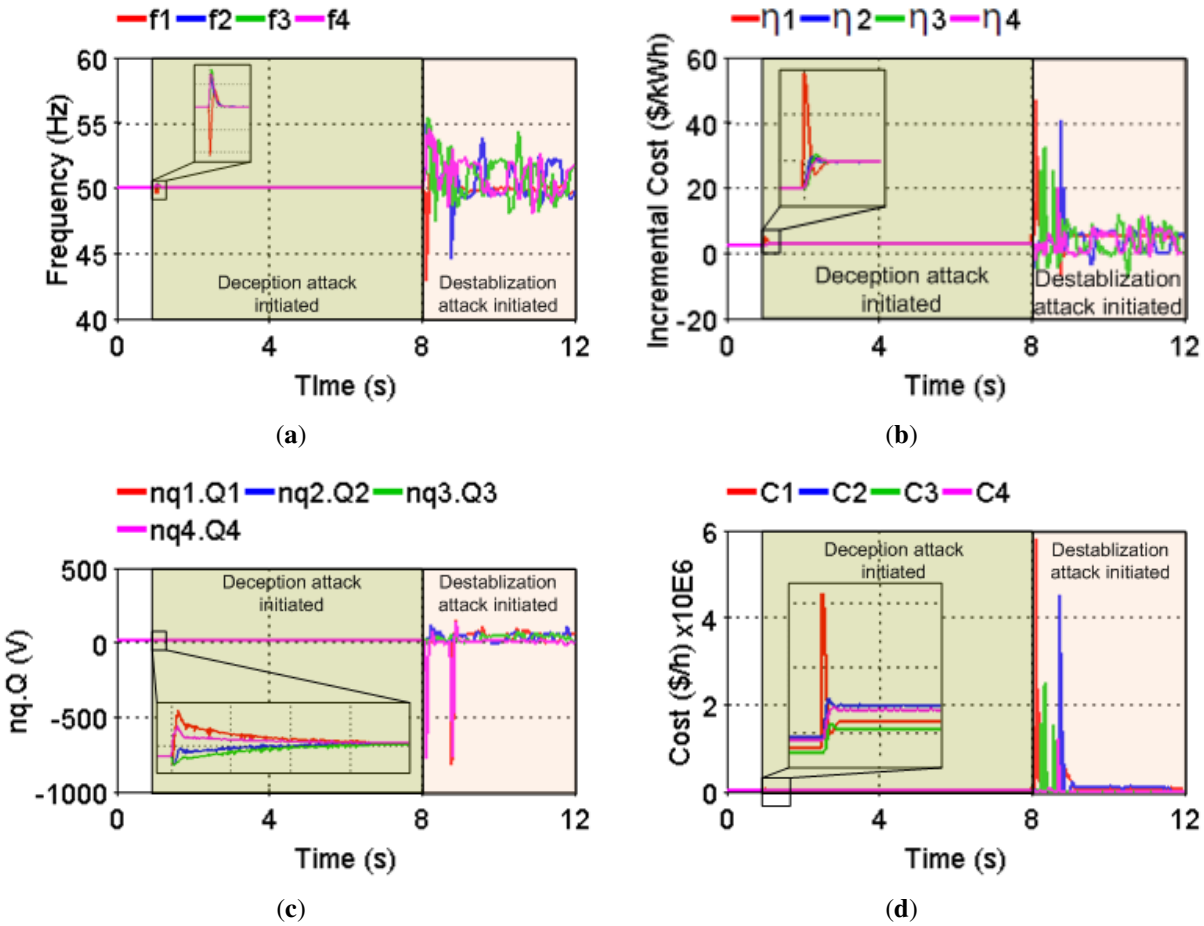

Fig. 2: RT simulation results on HYPERSIM with FDIA initiated at 1 s with small value and increased to unfair value at 8 s (**a**) frequency restoration; (**b**) ED; (**c**) proportional reactive power sharing; and (**d**) generation cost.

In Fig.1a, a 400 V/50 Hz islanded AC MG is considered composed of four DGs each of 40 kVA rating. The DG parameters are given in Table I. The various vulnerable points are also highlighted. The attacker can target these vulnerable entities to launch cyber attacks. The system response to FDI and hijacking attacks on DG 1 are further demonstrated. in this section.

The variations of system objectives and cost of generation on launching FDI attacks are first presented. Each of the simulation results are divided in two shaded portions. The green shaded section represents the system under stealthy FDI attack and the orange section represents the system under destablization attack. It can be observed in Fig. 2 that prior to FDI attack, system was operating normally satisfying all the objectives. Later deception attack was initiated at 1 s (appearing similar to a load change) and destablization attacks was further initiated at 8 s. Although the system objectives were satisfied during deception attack but it became unstable on initiating destablization attack.

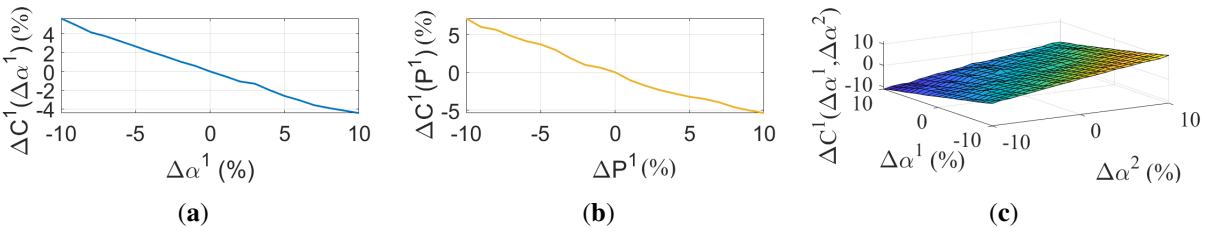

Fig. 3: Variation of cost of generation (**a**) α^1 attacked; (**b**) P^1 attacked; (**c**) α^1 and α^2 attacked.

Table I: DG PARAMETERS

Active power droop coefficient	m_p	9.4 x 10-5 rad/Ws	
Reactive power droop coefficient	n_q	1.3 x 10-3 V/VAr	
Voltage controller proportional gain	K_{pv}	0.2	
Voltage controller integral gain	K_{iv}	1	
Current controller proportional gain	K_{pc}	5	
Current controller integral gain	K_{ic}	100	
Line parameters	$Line_{12}$	R_{12}= 0.23 Ω	L_{12}= 318 μH
	$Line_{23}$	R_{23}= 0.35 Ω	L_{23}= 1847μH
	$Line_{34}$	R_{34}= 0.23 Ω	L_{34}= 318 μH
Load parameters	Load 1	P1= 36 kW	Q1= 36 kVAr
	Load3	P3=45.9 kW	Q3=22.8 kVAr
Cost parameters	α^1= 0.094 $\$/kW^2h$	β^1= 1.22 $\$/kWh$	γ^1= 51 $\$/h$
	α^2= 0.078 $\$/kW^2h$	β^2= 3.41 $\$/kWh$	γ^2= 31 $\$/h$
	α^3 =0.105 $\$/kW^2h$	β^3= 2.53 $\$/kWh$	γ^3= 78 $\$/h$
	α^4 =0.082 $\$/kW^2h$	β^4= 4.02 $\$/kWh$	γ^4= 42 $\$/h$

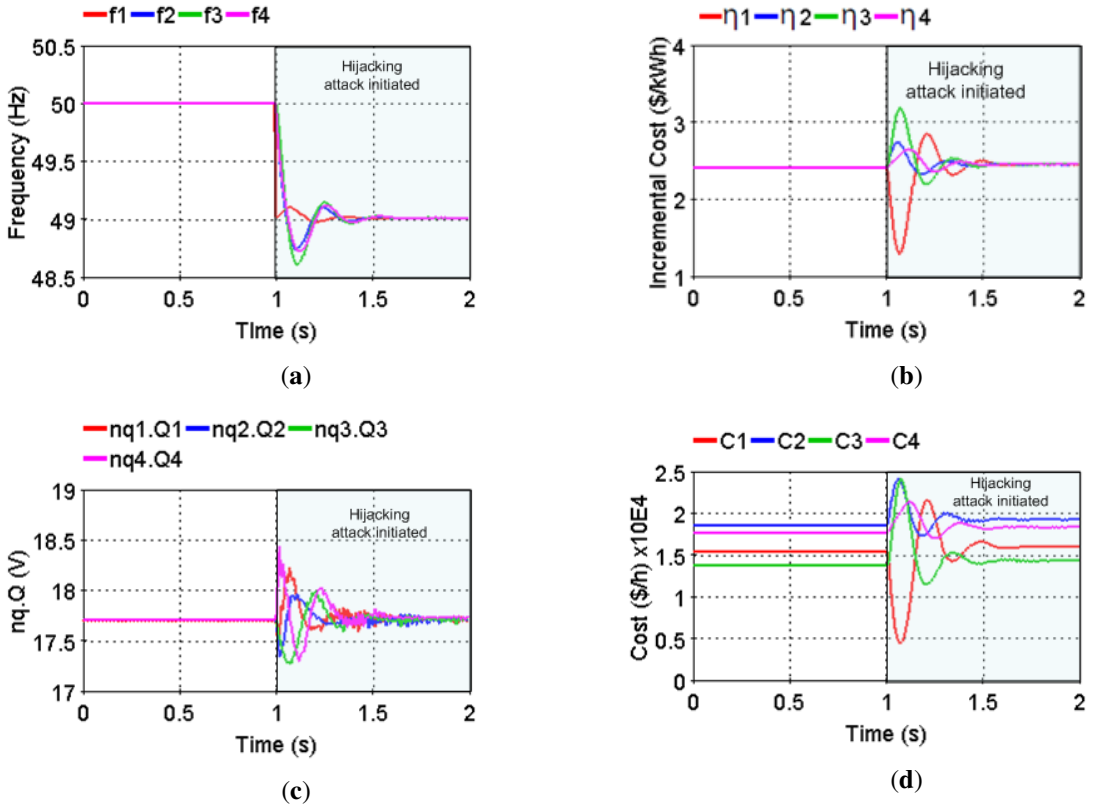

Fig. 4: RT simulation results on HYPERSIM with hijacking attack initiated at 1 s with a small value (**a**) frequency restoration; (**b**) ED; (**c**) proportional reactive power sharing; and (**d**) generation cost.

Assuming $\Delta C^i(x) = C^{Ai}(x) - C^i(x)$ for DG^i, where $\Delta C^i(x)$ is deviation in cost of generation when $C^i(x)$ is attacked by x to get the new value of $C^{Ai}(x)$. Fig. 3 reflects the variation in cost of generation for DG^1, with individual attack on α^1 and P^1 and combined attack by α^1 and α^2. Each attack vector (α^1, α^2, P^1) are deviated in range of $\pm 10\%$. The maximum deviation in cost, $\Delta C^1(\Delta\alpha^1) = 5.66\%$ and $\Delta C^1(\Delta P^1) = 7.10\%$ was observed for $\Delta\alpha^1 = -10\%$, $\Delta P^1 = -10\%$, as shown in Fig. 3a and Fig. 3b, respectively. It was further observed that a larger deviation in cost, $\Delta C^1 = 11.34\%$ was obtained when attack was done in a combined manner ($\Delta\alpha^1 = -10\%$, $\Delta\alpha^1 = 10\%$) as shown in Fig. 3c.

Further, the variations of system objectives and cost of generation on launching hijack attack at 1 s are presented in the Fig. 4. The system objectives converges to a new attacked value presented in the blue shaded portion. Similar to FDI attacks, the effect of variations of different attack elements can be plotted in case of hijack attacks as well.

Conclusion

This paper analyzes the impact of cyber risks on generation cost in a CEM system. It has been observed that combined attack on the cost parameters (α^1, α^2) affected the generation cost to a larger extent than the individually, for the same deviation in the attack parameters. The influence of the attack on P^1 was further investigated. RT testing of the CEM under FDI and hijacking attacks has also been demonstrated.

References

[1] Z. Li, Z. Cheng, J. Liang, J. Si, L. Dong and S. Li, "Distributed Event-Triggered Secondary Control for Economic Dispatch and Frequency Restoration Control of Droop-Controlled AC Microgrids," in *IEEE Trans. Sustain. Energy*, vol. 11, no. 3, pp. 1938-1950, July 2020, doi: 10.1109/TSTE.2019.2946740.

[2] Y. Han, K. Zhang, H. Li, E. A. A. Coelho and J. M. Guerrero, "MAS-Based Distributed Coordinated Control and Optimization in Microgrid and Microgrid Clusters: A Comprehensive Overview," *IEEE Trans. Power Electron.*, vol. 33, no. 8, pp. 6488-6508, Aug. 2018, doi: 10.1109/TPEL.2017.2761438.

[3] S. Sahoo, T. Dragičević and F. Blaabjerg, "Resilient Operation of Heterogeneous Sources in Cooperative DC Microgrids," *IEEE Trans. Power Electron.*, vol. 35, no. 12, pp. 12601-12605, Dec. 2020, doi: 10.1109/TPEL.2020.2991055.

[4] X. Fu, G. Chen and D. Yang, "Local False Data Injection Attack Theory Considering Isolation Physical-Protection in Power Systems," *IEEE Access*, vol. 8, pp. 103285-103290, 2020, doi: 10.1109/ACCESS.2020.2999585.

[5] P. Li, Y. Liu, H. Xin and X. Jiang, "A Robust Distributed Economic Dispatch Strategy of Virtual Power Plant Under Cyber-Attacks," *IEEE Trans. Ind. Informat.*, vol. 14, no. 10, pp. 4343-4352, Oct. 2018, doi: 10.1109/TII.2017.2788868.

[6] G. Chen and Z. Guo, "Distributed Secondary and Optimal Active Power Sharing Control for Islanded Microgrids With Communication Delays," *IEEE Trans. Smart Grid*, vol. 10, no. 2, pp. 2002-2014, March 2019, doi: 10.1109/TSG.2017.2785811.

[7] J. Duan and M. Y. Chow, "A Novel Data Integrity Attack on Consensus-Based Distributed Energy Management Algorithm Using Local Information," *IEEE Trans. Ind. Informat.*, vol. 15, no. 3, pp. 1544-1553, March 2019, doi: 10.1109/TII.2018.2851248.

[8] H. Pourbabak, J. Luo, T. Chen and W. Su, "A Novel Consensus-Based Distributed Algorithm for Economic Dispatch Based on Local Estimation of Power Mismatch," *IEEE Trans. Smart Grid*, vol. 9, no. 6, pp. 5930-5942, Nov. 2018, doi: 10.1109/TSG.2017.2699084.

[9] G. D. Torre and T. Yucelen, "Adaptive architectures for resilient control of networked multiagent systems in the presence of misbehaving agents," *Int. J. Control*, vol. 91, no. 3, pp. 495-507, 2018.

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

[11] S. Sahoo and J. C. -H. Peng, "A Localized Event-Driven Resilient Mechanism for Cooperative Microgrid Against Data Integrity Attacks," *IEEE Trans. Cybernetics*, vol. 51, no. 7, pp. 3687-3698, July 2021, doi: 10.1109/TCYB.2020.2989225.

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

[13] B. Huang, Y. Li, F. Zhan, Q. Sun and H. Zhang, "A Distributed Robust Economic Dispatch Strategy for Integrated Energy System Considering Cyber-Attacks," *IEEE Trans. Ind. Informat.*, vol. 18, no. 2, pp. 880-890, Feb. 2022, doi: 10.1109/TII.2021.3077509.

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

[15] W. Zeng, Y. Zhang and M. -Y. Chow, "Resilient Distributed Energy Management Subject to Unexpected Misbehaving Generation Units," *IEEE Trans. Ind. Informat.*, vol. 13, no. 1, pp. 208-216, Feb. 2017, doi: 10.1109/TII.2015.2496228.

[16] Z. Cheng and M. -Y. Chow, "Resilient Collaborative Distributed Energy Management System Framework for Cyber-Physical DC Microgrids," *IEEE Trans. Smart Grid*, vol. 11, no. 6, pp. 4637-4649, Nov. 2020, doi: 10.1109/TSG.2020.3001059.

[17] M. S. Sadabadi, S. Sahoo and F. Blaabjerg, "A Fully Resilient Cyber-Secure Synchronization Strategy for AC Microgrids," *IEEE Trans. Power Electron.*, vol. 36, no. 12, pp. 13372-13378, Dec. 2021, doi: 10.1109/TPEL.2021.3091587.

[18] S. K. Mazumder et al., "A Review of Current Research Trends in Power-Electronic Innovations in Cyber–Physical Systems," *IEEE J. Emerg. Sel. Topics Power Electron.*, vol. 9, no. 5, pp. 5146-5163, Oct. 2021, doi: 10.1109/JESTPE.2021.3051876.