Peer-to-Peer Energy Sharing for Enhancing Networked Microgrids Resilience Considering Threats to Data Availability

Milad Mehri Arsoon[1], and Seyed Masoud Moghaddas-Tafreshi[2]*

[1] Department of Electrical Engineering, Faculty of Engineering, University of Guilan, Rasht, Iran (e-mail: mmehri@webmail.guilan.ac.ir).

[2] Department of Electrical Engineering, Faculty of Engineering, University of Guilan, Rasht, Iran (e-mail: tafreshi@guilan.ac.ir).

*Corresponding Author

Received 10 Aug. 2022 Received in revised form 12 Nov. 2022 Accepted 28 Nov. 2022

Type of Article: Research paper

***Abstract*— This paper studies the simultaneous resilience enhancement of networked microgrids (NMGs) operation in a peer-to-peer way against extreme weather events and threats to data availability (DA). Applying the model predictive control (MPC) method and dynamic usage of energy storage helps microgrids (MGs) to mitigate the uncertainties of events impacts and increase their adaptation ability by rescheduling at each time step. However, despite the decentralized implementation, DA threats, like a denial of service attack or MGs' communication network damage due to the main event impact, cause communication network islanding and result in incorrect convergence of consensus values for energy sharing. Hence, MGs share the prespecified preamble vectors along with shared energy values using the same communication protocol to overcome the above problems. Furthermore, the impact of reducing the length of shared data by utilizing the MPC approach and the compressive sensing method for the large-scale communication network with low connectivity and bandwidth limitation is investigated. Numerical results show the more resilient operation of MGs against simultaneous threats to the cyber-physical infrastructures. In this case, although the system performance level decreases, this decrease is lower than the non-resilient case against these types of simultaneous threats.**

***Keywords*: Compressive sensing, data availability, networked microgrids, peer-to-peer energy sharing, resilience.**

NOMENCLATURE

Sets and Indices

$i/pr/j/t$	Index of MGs/MGs' priority/islands/time step
k/l	Iteration index for main problem/ACA
n/G_i	Index/set of microturbines
B_i	Set of ith MG's neighbors

Parameters

N	Number of MGs in the cyber layer
μ	Step size for ACA convergence
$\rho_i, \beta_i, \omega_i, \sigma_i$	Penalty coefficients
C_i^{ES}	Energy storage capacity (MWh)
Δt	Time step
$\bar{P}_i^{ch}/\bar{P}_i^{dch}$	Charging/discharging rate of energy storage (MW)
$S_{i,t}^l$, y_m^l	Iteration values in ACA
$P_n^{G,ru/rd}$	Ramp up and ramp down limits of microturbine (MW/Δt)
$\bar{P}_n^G$	Maximum output of microturbine (MW)
$P_{i,t}^{wind}$	Wind turbine output (MW)
$P_{i,t}^{ex}$	Maximum exchangeable power by MG i (MW)
$P_{i,t}^D$	Demand of ith MG (MW)

Variable

$P_{i,t}^s/P_{i,t}^b$	Sold/bought power from/to main grid (MW)
$P_{i,t}^{ch}/P_{i,t}^{dch}$	ESs' charging/discharging power (MW)
$P_{i,t}^{out}/P_{i,t,pr}^{in}$	Exported/imported power by MG i (MW)
$P_{i,t}^G$	Microturbine output (MW)
$SOC_{i,t}$	SOC level of energy storage
$P_{i,t}^{sh}$	load shedding (MW)
$\boldsymbol{x}$	Vector of MGs status in each island of communication network

[Downloaded from joc.kntu.ac.ir on 2026-11-11]

[DOI: 10.61186/joc.17.3.13]

$P_{i,t}^{Mout}/P_{i,t,pr}^{Min}$ Exported/imported power of other MGs from the ith MG's view point

I. Introduction

The increasing vulnerability of power systems to high-impact, low-frequency (HILF) events such as extreme weather events or deliberate attacks has made the resilience enhancement of these systems of great importance [1]. One aspect of enhancing power system resilience is taking preventive and corrective measures, categorized as planning-oriented and operation-oriented measures [1]. The first category, such as physical infrastructure hardening strategies [2], needs high investment. The second one, like resource scheduling [3], has a relatively lower cost. However, its effectiveness depends on the existence of sufficient facilities. Hence, regarding the rare nature of HILF events and the above limitations, the synergy of multiple energy systems resources can be adopted as an effective solution [4]. In this regard, microgrids' (MGs) important role in future energy networks has led to more attention being paid to resource integration of networked MGs (NMGs) for resilience purposes [5]-[10].

The study in [6] proposed an energy management strategy for the resilience enhancement of NMGs in coordination with distribution network operators (DNO). A market-based power trading for emergencies was presented in [7]. Also, [8] proposed an effort-based method for the fair allocation of unserved load in NMGs in a hierarchical way. However, the need for a central coordinator makes them vulnerable to the single point of failure in the cyber domain. In order to overcome this problem, [9] proposed the decentralized energy sharing model for increasing the self-healing ability of NMGs. Also, [10] presented an energy sharing model among MGs for emergencies, whereas MGs' individual objectives were not considered.

In most of the above studies, their top-down financial transactions may prohibit them from direct energy sharing among MGs [11] in emergencies. However, by introducing peer-to-peer (P2P) energy trading, local MGs can directly exchange energy with each other without intermediation by conventional service providers (SPs) [12]. P2P concept brings more opportunities for enhancing the power system performance by facilitating the implementation of consumer preferences [13] or cost minimization by local energy exchange [14] in normal operation mode. It is also intuitively understood that P2P energy sharing can be useful for the resilience enhancement of NMGs by locally compensating energy deficiency. The study in [11] proposed a proactive energy bartering method without needing financial agreement for NMGs' resilience enhancement without considering unpredicted contingencies during the HILF event. Also, a resilience-oriented P2P based multi-carrier energy swapping framework was proposed in [15] for networked energy hubs. Besides the energy resource integration, coordinated utilization of energy and communication resources were studied in [16] for the normal operation mode. The above studies in P2P energy sharing are the day-ahead operation models with economic or resilience goals, which proactively prepare MGs. In this regard, a robust model predictive control (MPC) based transactive energy framework was presented in [17] or islanded NMGs in normal situations. This method uses updated information about renewables generation at the current time step to cope with uncertainties of these resources and minimize energy imbalance for the following intervals.

It should be noted that the communication network and management system are important parts of a power system. Hence, some of the mentioned studies proposed a hierarchical or fully decentralized energy sharing model to increase cyber resilience. However, the higher intelligence level of smart grids like MGs increases the risk of cyber threats [18], [19]. Therefore, it can be expected that NMGs' communication network disturbance will result in the wrong decision about consensus on shared energy among MGs, which was not investigated in the above studies on NMGs' energy management. Cyber resilience is compromised by disrupting data availability (DA) corrupting integrity or confidentiality [20]. For example, attackers can affect data integrity by launching a false data injection (FDI) attack for system data manipulation and leading systems operators toward making wrong decisions [21]. In this regard, the study in [22] proposed the reputation-based neighborhood watch algorithm for reducing the impact of the different types of FDI attacks on the operation of a multiagent-based power system. Also, the impact of these types of attacks can be found in other power system contexts like state estimation [23]. However, launching these types of attacks requires intensive knowledge about system structure and massive resources to manipulate data. Whereas by launching a cheaper attack like denial of service (DoS) [23], [24], attackers can disrupt DA by overloading and disabling the network elements like energy management systems. Hence, [25] proposed a distributed DoS attack-resilient control scheme for frequency regulation and energy balancing in heterogeneous battery energy storage systems. In addition, cyber resilience against information packet loss was investigated in some studies. Ref. [26] studied the coordinated operation of electricity and gas systems over a lossy communication network. Similarly, the studies in [27] and [28] proposed the communication packet loss resilient models for coordinating district energy systems and multiple MGs with their upstream networks, which are still vulnerable to the single point of failure in the cyber domain due to their hierarchical structure. A resilient packet loss and decentralized energy sharing

[Downloaded from joc.kntu.ac.ir on 2026-11-11]

[DOI: 10.61186/joc.17.3.13]

model for a multiagent-based microgrid was proposed in [29]. The studies in [26]-[29] investigated the resilience of energy management models against randomly-occurred DA threats. While, the impact of deliberate activities has not been studied. On the other hand, it should be mentioned that these studies only focus on power systems' cyber resilience. Compared with a single physical or cyber threat, their combination can significantly impact the system's performance [20]. In this regard, the impact of limited communication bandwidth on frequency restoration in an emergency was investigated in [30]. Furthermore, the study in [31] studied the impact of a load redistribution attack in coordination with a deliberate physical attack for masking the network topology changing and misleading the system operator. In contrast to [31], with respect to the attackers' limitations on cost and information, the studies in [20], [32] assessed the impact of a DoS attack in coordination with a physical attack through the bi-level mathematical and attacker-defender game modeling, respectively.

These studies focus on the vulnerability assessment of centralized power systems at the transmission level against coordinated cyber-physical attacks. In contrast and with respect to the provided comparison of the related literature in Table 1, the resilient operation of NMGs in a decentralized P2P manner is studied here against coordinated threats. In this study, instead of designing a physical attack, which needs more resources, attackers wait for affecting NMGs by the main event impact like reduction in generation capacity. Then, by launching a relatively cheaper attack like DoS [24], they target vulnerable points in the resilient operation model of NMGs. Hence, the main goal is to deal with a class of HILF threats, which aims to limit the effect of resilience measures against extreme weather events by cyber threats. In other words, the energy sharing model is developed to be resilient against these coordinated threats. For a better resilience response, the MPC method [6], [17] is adopted to overcome errors in predicting events' impacts. In this method, MGs reschedule themselves at each time step by considering a short but more accurate operation window. Also, the charging levels of energy storages (ESs) are kept at higher values to mitigate the impact of unexpected events and considering the short operation window. However, the execution of the proposed method for each time step and the need for communication among MGs increases the risk of DA threats like DoS attack or communication network damage due to the main event impact, which also increases the vulnerabilities in the cyber domain. These cyber-threats can disable MGs for communication and disrupt negotiations to reach consensus. Therefore, they can cause incorrect convergence of consensus values. To overcome this problem, the preamble vector is shared along with the power information to verify the correctness of converged values. In this regard, the contributions of this study are: i) Applying the MPC method and dynamic usage of ESs for sequentially rescheduling for each time step to deal with uncertainties of HILF events impact and increasing resistance and adaptation abilities of NMGs by minimizing load shedding (LS) based on MGs' priority. ii) Detecting threats to DA and verifying the correctness of consensus values convergence by distributing pre-specified preamble vectors with the same power data sharing protocol. iii) In addition, besides considering a short operation window, the utilization of the compressive sensing (CS) approach [33], [34] causes reducing preamble vector length and needed bandwidth. Therefore, it causes more scalability for networks with numerous peers and more resilience in the case of alternative DoS attacks.

TABLE. 1
COMPARISON OF RELATED LITERATURE AND PROPOSED METHOD.

Refs	NMGs	P2P	Cyber domains resilience	Energy domains resilience	Decentralized energy management	Scheduling	
						Proactive	Corrective
[11]	✓	✓	×	✓	✓	✓	×
[15]	✓	✓	×	✓	✓	✓	×
[16]	✓	✓	×	×	✓	✓	×
[17]	✓	✓	×	×	✓	✓	✓
[20]	×	×	✓	✓	×	✓	×
[22]	×	✓	✓	×	✓	✓	×
[26]	×	×	✓	×	✓	✓	×
[28]	✓	×	✓	×	✓	✓	×
[31]	×	×	✓	✓	×	✓	×
This paper	✓	✓	✓	✓	✓	✓	✓

The remainder of this paper is organized as follows. Section II describes the problem. Section III proposes the formulations of resilience-oriented P2P energy sharing, which will be extended in section IV in resilient data broadcasting. In Section V, case studies are provided. Section VI concludes the paper.

II. PROBLEM DESCRIPTION

Fig. 1(a) shows the simplified representation of a typical power distribution network with multiple MGs. Each MG has multiple microturbines (MTs), a wind turbine, and an ES. In addition, due to the role of SPs in the restructured environment, it is assumed that each MG trades energy with its specific SP in the normal mode. Although other types of extreme natural events can be considered, it is assumed that MGs face extreme weather events like hurricanes, which can be predicted with moderate or well accuracy. After receiving an alert for these events, DNO and MGs prepare themselves. Here, the impact of these events on MGs is assumed to be disconnecting from the main grid and reducing generation capacities. Therefore, N electrically isolated MGs form NMGs for compensating power deficiency by

[Downloaded from joc.kntu.ac.ir on 2026-11-11]

[DOI: 10.61186/joc.17.3.13]

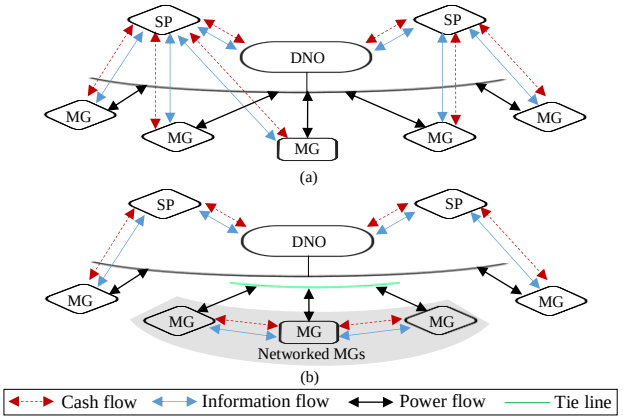


Fig. 1. The simplified NMGs formation in a typical distribution network. (a) General scheme for MGs operation. (b) NMGs formation in case of occurring an HILF event.

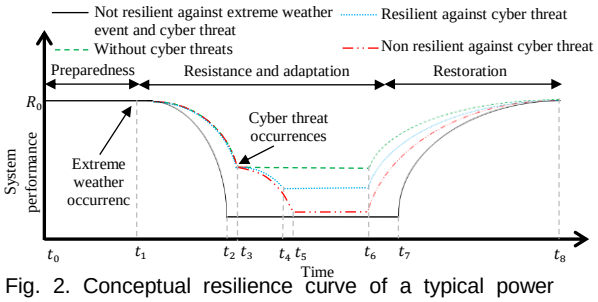


Fig. 2. Conceptual resilience curve of a typical power

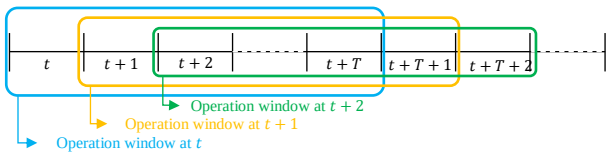


Fig. 3. MPC description.

closing tie-lines switches, as shown in Fig. 1(b). In this situation, SPs may not be responsible for these isolated MGs [11], and they must directly exchange energy with each other without the intermediation of a third party. To do so, first, each MG determines its exchangeable power values. By sharing these power values with other MGs, all of them are informed about the total exchangeable power. Then, the total power values are corrected to hold the power balance among MGs. Using these corrected values, MGs reschedule their resources and determine their new values of exchangeable power. This procedure is iteratively executed until the convergence. It is assumed that DNO is responsible for defensive islanding, similar to the method in [3], and informing MGs about communication and electrical networks topologies.

Fig. 2 shows the resilience curves of a typical power system. This curve can be divided into preparing, resistance, adaptation, and restoration intervals [35]. In a resilient system, after anticipating and receiving an alert for an extreme weather event, the proactive and preparedness scheduling period is started from t_0 to t_1 to reduce the event impact after t_1. In other words, due to preparedness scheduling and depending on the system hardening level, the performance curve degrades with a lower slope in a longer period t_1 to t_3 instead of a shorter interval t_1 to t_2. Hence, the performance curve is kept in the higher values compared with the non-resilient case. So, the power system has a higher resistance to performance curve degradation and better adaption ability to respond to event impact and prevent performance level decreasing. Finally, concerning the event impact, different system restoration strategies like physical infrastructure repairing will be employed after t_6 to restore the system to the targeted performance level. It should be mentioned that, due to the impact of event uncertainties, system performance may be more affected after t_1. Hence, in comparison with the studies like [9]-[11], where they cover one stage, the present study tries to cover the first three stages using the MPC method [6], [17] and dynamic usage of ESs to increase the resistance and adaptation abilities of NMGs. As shown in Fig. 3, each MG reschedules itself at each time step (e.g., time interval t) in the MPC method over a short operation window (e.g., considering T future time intervals), which is based on the more accurate prediction of system status. By solving the operation model, schedules are implemented only for the current time step (e.g., t). After passing the current time step and arriving next time step (e.g., $t+1$), the operation model is solved by updating the system status and parameters, such as available generation capacity and load consumption. This procedure is repeated for each time step in real-time implementation. It is worth mentioning that load and wind generation are assumed to be well predictable here for the current operation window. Nevertheless, some approaches like the scenario-based method [36] can be used to cope with their uncertainties.

Keeping ESs' state of charge (SOC) level at higher values compensates for ignoring a longer operation window and increases MGs' preparedness in the face of unexpected events. Also, considering a short operation window reduces the amount of exchanged power data and consensus time, which may be helpful when communication bandwidth is limited during a DA threat (e.g., by the lower value of the signal to interference plus noise ratio (SINR) [24], [37]). For reaching consensus, the communication protocol is initialized based on the Laplacian matrix L representing the communication network of NMGs. However, in contrast to the above studies focused on NMGs operation, it is assumed that some MGs cannot participate in data sharing by threatening DA. Therefore, matrix L is changed. DA can be threatened by malicious activities like DoS attacks or the main event impact on the communication network equipment, especially when the energy management procedure is executed for each time step. In deliberate cases, attackers eavesdrop on MGs' negotiations and wait for the falling of NMGs into a weak state. Then,

[Downloaded from joc.kntu.ac.ir on 2026-11-11]

[DOI: 10.61186/joc.17.3.13]

launching a DoS attack during data sharing and disabling some MGs for communication will result in the incorrect convergence of consensus values. Therefore, as shown in Fig. 2, MGs' performance level is decreased to the lower values in this case. So, a prespecified preamble vector along with the power values is shared by each MG with the same protocol. These measures help MGs to independently detect communication network islanding and verify the correctness of the converged values. After isolating disabled MGs by their neighbors, MGs of each island execute this framework again. Hence, as Fig. 2 illustrates, although some MGs cannot participate in energy sharing, other MGs can share power, which may cause a higher performance level in comparison with the non-resilient case against cyber threats. Also, the CS-based approach is utilized for more scalability and higher resilience by decreasing the length of the preamble vector in the face of alternative DoS attacks. It should be mentioned that DA threat occurrence may not be easily predictable. Hence, its occurrence is checked at each time step.

Here, the main goal is supplying MGs based on their priorities instead of gaining revenue. Also, this method must be simple for easy implementation. Here, the local power price (LPP) for P2P trading is considered as the fixed value and determined by DNO based on historical data. It should be sufficiently higher than the maximum generation cost. Therefore, it is expected to avoid imposing the extra cost on MGs when they use their more expensive generation units. Hence, their willingness is increased to participate in this method.

III. Resilience-Oriented P2P Energy Sharing Model

This section explains the energy sharing framework in two stages. First, the resource scheduling problem is presented. Then, the information sharing procedure is expressed, which will be extended for cyber resilience in the next section.

A. Networked Operation Model for Determining Exchangeable Power of Each MG

For resilience enhancement, MGs can exchange energy with each other without considering its origin. Therefore, as shown in Fig. 4 and similar to [11], from the ith MG's viewpoint with priority p and at time step $t \in \{t_p, \dots, t_p + T\}$, the total exchangeable power of other MGs (i.e., $P_{i,t}^{Mout}$ and $P_{i,t,pr}^{Min}$ with priority $pr \in \{1, \dots, p, \dots, \pi\}$) are written as follows and will be calculated in a decentralized way later.

$$P_{i,t}^{Mout} = \sum_{s=1}^{N} P_{s,t}^{out} - P_{i,t}^{out} = P_{t}^{Tout} - P_{i,t}^{out} \quad \forall i,t \quad (1a)$$

$$P_{i,t,pr}^{Min} = \sum_{s=1}^{N} P_{s,t,pr}^{in} - P_{i,t}^{in} = P_{t,pr}^{Tin} - P_{i,t}^{in} \quad \forall i,t,pr = p \quad (1b)$$

$$P_{i,t,pr}^{Min} = \sum_{s=1}^{N} P_{s,t,pr}^{in} = P_{t,pr}^{Tin} \quad \forall i,t,pr \neq p \quad (1c)$$

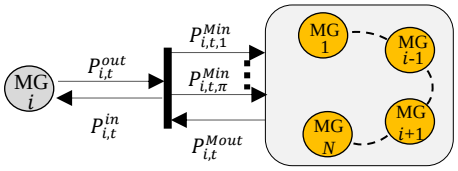


Fig. 4. Integration of other MGs as a black box from ith MG's view point.

$$P_{i,t}^{Min} = \sum_{pr=1}^{\pi} P_{i,t,pr}^{Min} \quad \forall i,t \quad (1d)$$

where P_t^{Tout} and $P_{t,pr}^{Tin}$ are the total exchangeable power of all MGs and $P_{i,t}^{out}$ and $P_{i,t}^{in}$ are the exported and imported power by ith MG. For MG i at time step t_p and kth iteration, MG's scheduling problem is written as follows:

$$\max \sum_{t=t_p}^{t_p+T} ((P_{i,t}^{out} - \rho_i P_{i,t}^{in} - \beta_i (mis_{i,t}^{out} + mis_{i,t}^{in}) - \omega_i P_{i,t}^{sh}) \Delta t + \sigma_i C_i^{ES} SOC_{i,t}) \quad (2)$$

$$s.t \quad P_{i,t}^{out} + P_{i,t}^{Mout} + mis_{i,t}^{out} = P_{i,t}^{in} + P_{i,t}^{Min} + mis_{i,t}^{in} \quad \forall t \quad (3)$$

$$P_{i,t}^{b} + P_{i,t}^{in} + \sum_{n \in G_i} P_{n,t}^{G} + P_{i,t}^{dch} + P_{i,t}^{wind} + P_{i,t}^{sh} = P_{i,t}^{D} + P_{i,t}^{ch} + P_{i,t}^{out} + P_{i,t}^{s} \quad \forall t \quad (4)$$

$$0 \le P_{i,t}^{out} \le u_{i,t}^{out} min(P_{i,t}^{ex}, P_{i,t}^{Min}) \quad \forall t \quad (5a)$$

$$0 \le P_{i,t}^{in} \le u_{i,t}^{in} min(P_{i,t}^{ex}, P_{i,t}^{Mout}) \quad \forall t \quad (5b)$$

$$u_{i,t}^{out} + u_{i,t}^{in} \le 1 \quad \forall t \quad (5c)$$

$$0 \le P_{i,t}^{b} \le v_{i,t}^{b} P_i^{ex} \quad \forall t \quad (6a)$$

$$0 \le P_{i,t}^{s} \le v_{i,t}^{s} P_i^{ex} \quad \forall t \quad (6b)$$

$$v_{i,t}^{b} + v_{i,t}^{s} \le 1 \quad \forall t \quad (6c)$$

$$0 \le P_{i,t}^{s} + P_{i,t}^{out} \le P_{i,t}^{ex} \quad \forall t \quad (7a)$$

$$0 \le P_{i,t}^{b} + P_{i,t}^{in} \le P_{i,t}^{ex} \quad \forall t \quad (7b)$$

$$0 \le mis_{i,t}^{out} \le x_{i,t}^{out} U \quad \forall t \quad (8a)$$

$$0 \le mis_{i,t}^{in} \le x_{i,t}^{in} U \quad \forall t \quad (8b)$$

$$x_{i,t}^{out} + x_{i,t}^{in} \le 1 \quad \forall t \quad (8c)$$

$$0 \le P_{i,t}^{ch} \le y_{i,t}^{ch} \bar{P}_i^{ch} \quad \forall t \quad (9a)$$

$$0 \le P_{i,t}^{dch} \le y_{i,t}^{dch} \bar{P}_i^{dch} \quad \forall t \quad (9b)$$

$$y_{i,t}^{ch} + y_{i,t}^{dch} \le 1 \quad \forall t \quad (9c)$$

$$SOC_{i,t} = SOC_{i,t-1} + (P_{i,t}^{ch} \eta_i^{ch} - P_{i,t}^{dch} / \eta_i^{dch}) \Delta t / C_i^{ES} \quad \forall t \quad (10a)$$

$$SOC_i^{min} \le SOC_{i,t} \le SOC_i^{max} \quad \forall t \quad (10b)$$

$$0 \le P_{n,t}^{G} \le \bar{P}_n^{G} \quad \forall n \in G_i, t \quad (11a)$$

$$-P_n^{G,rd} \le P_{n,t}^{G} - P_{n,t-1}^{G} \le P_n^{G,ru} \quad \forall n \in G_i, t \quad (11b)$$

$$0 \le P_{i,t}^{sh} \le P_{i,t}^{D} \quad \forall t \quad (12)$$

For the ith MG (the iteration index k is dropped for simplicity), the first and second terms of the objective function (2) maximizes exportable energy and minimizes imported energy except for the critical intervals. The third and fourth terms penalize power mismatches among

[Downloaded from joc.kntu.ac.ir on 2026-11-11]

[DOI: 10.61186/joc.17.3.13]

MGs and LS [11]. $mis_{i,t}^{out}$ and $mis_{i,t}^{in}$ are power balance mismatch variables, and must iteratively go to zero. Δt is the time step duration. ρ_i is set to be greater than the multiplier of $P_{i,t}^{out}$ (i.e., 1) and $\omega_i > \rho_i$ for forcing MGs to import power only when LS is inevitable. β_i is the penalty weight for minimizing power balance mismatch and is set to be higher than ω_i to prevent minimizing LS with increasing mismatch values. The fifth term in (2) controls the ES charging level. If $\sigma_i > 0$, ES is forced to keep its SOC at a higher level to deal with uncertainties and mitigate short operation horizon consideration in the MPC method. Also, the MPC method is adopted for dealing with unexpected events based on the short-term forecast. Each MG schedule itself for time step t_p by considering T future time steps, while schedules are implemented only for t_p. Power balance among MGs and inside each one is ensured by (3) and (4). $P_{i,t}^{Mout}$ and $P_{i,t}^{Min}$ are calculated from the previous iteration. At each iteration, MGs try to keep the power balance among MGs with minimum mismatch at the current iteration. In (4), $P_{i,t}^{wind}$ and $P_{n,t}^{G}$ are the power generation of wind turbine and MT, where n and G_i are the index and set of MTs in MG i. In addition, $P_{i,t}^{ch}$ and $P_{i,t}^{dch}$ are ES's charging and discharging power. Also, $P_{i,t}^{sh}$ and $P_{i,t}^{D}$ are the load shedding variable and total load at time t. The variables $P_{i,t}^{b}$ and $P_{i,t}^{s}$ are the bought/sold power from/to the main grid. Constraints (5a)-(5c) control P2P power exchange and binary variables $u_{i,t}^{out}$ and $u_{i,t}^{in}$ enforce MG i to exchange power in one direction. Constraints (6a)-(6c) control the amount of bought power and sold power from/to the main grid and its direction using binary variables $v_{i,t}^{b}$ and $v_{i,t}^{s}$ when MGs are connected to the main grid. Constraints (7a) and (7b) represent exchanging power with other MGs and the main grid, where $P_{i,t}^{ex}$ is its maximum limit. Constraints (8a)-(8b) limit $mis_{i,t}^{out}$ and $mis_{i,t}^{in}$ with upper value U, and binary variables $x_{i,t}^{out}$ and $x_{i,t}^{in}$ in (8c) guarantee that one of them can be non-zero [11]. Constraints (9a)-(9c) impose allowable ES's charging and discharging rate ($\bar{P}_i^{ch}$ and $\bar{P}_i^{dch}$) and its direction using binary variables $y_{i,t}^{ch}$ and $y_{i,t}^{dch}$. Constraints (10a) and (10b) calculate the stored energy in ES, where $SOC_{i,t}$ is the SOC level of it, C_i^{ES} is its capacity, and η_i^{ch} and η_i^{dch} are the charging and discharging efficiencies. The MTs' power output and ramp rate limits are represented by constraints (11a) and (11b) [6], where $\bar{P}_n^{G}$, $P_n^{G,ru}$ and $P_n^{G,rd}$ are the maximum and ramp up and ramp down limits of MT. Constraint (12) implies that the load shedding must be lower than the total load.

B. Calculating Total Exchanged Power Values

For calculating $P_{i,t}^{Mout}$ and $P_{i,t,pr}^{Min}$, ith MG iteratively updates its iteration value $S_{i,t}^{l}$ using average consensus algorithm (ACA) [10] as follows:

$$S_{i,t}^{l} = S_{i,t}^{l-1} + \mu \sum_{r\in B_i}\left(S_{r,t}^{l-1} - S_{i,t}^{l-1}\right) \qquad \forall i,t \quad (13)$$

where B_i is ith MG's neighbors, and l is the ACA iteration index. By initializing $S_{i,t}^{0}$ with $P_{i,t}^{out}$ and choosing proper step size μ, the value of $S_{i,t}^{l}$ will iteratively converge to the average of exported power, i.e., $S_{i,t}^{l} = S_{i,t}^{Pout} = (1/N)\sum_{i=1}^{N} P_{i,t}^{out}$ [10], [11]. From (1a), we have $P_t^{Tout} = \sum_{i=1}^{N} P_{i,t}^{out}$. Therefore:

$$P_t^{Tout} = N.S_{i,t}^{Pout} \qquad \forall t \quad (14)$$

Similarly, if $S_{i,t}^{0}$ is initialized with $P_{i,t}^{in}$ with priority pr, then:

$$P_{t,pr}^{Tin} = N.S_{i,t,pr}^{Pin} \qquad \forall t \quad (15)$$

Therefore, $P_{i,t}^{Mout}$ and $P_{i,t,pr}^{Min}$ can be obtained using (1).

C. Correcting Exchangeable Power Values for Holding Power Balance Among MGs

After determining $P_{i,t}^{out}$ and $P_{i,t}^{in}$ by solving (2)-(12), $P_{i,t}^{Mout}$ and $P_{i,t,pr}^{Min}$ are calculated using (1). Then, each MG solves (16)-(18) to correct its exchangeable power values based on MGs' priorities and hold the power balance among them. For the ith MG with pth priority:

$$\max \sum_{t=t_p}^{t_p+T} \left(n_{i,t}^{p}\alpha^{p}P_{i,t}^{in} + \sum_{pr=1}^{\pi} n_{i,t}^{pr}\alpha^{pr}P_{i,t,pr}^{Min}\right)\Delta t \quad (16)$$

$$\text{s.t. } m_{i,t}\left(P_{i,t}^{out} + P_{i,t}^{Mout}\right) = n_{i,t}^{p}P_{i,t}^{in} + \sum_{pr=1}^{\pi} n_{i,t}^{pr}\,P_{i,t,pr}^{Min} \qquad \forall t \quad (17)$$

$$0 \le m_{i,t}, n_{i,t}^{pr} \le 1 \qquad \forall t \quad (18)$$

The objective function (16) maximizes supplying MGs based on their priorities. α^{pr} is MGs' priority coefficient. MGs with higher priorities have greater coefficients. Also, the continuous variable $m_{i,t}$ is the portion of $P_{i,t}^{out}$ and $P_{i,t}^{Mout}$, and $n_{i,t}^{p}$ and $n_{i,t}^{pr}$ are the portion of $P_{i,t}^{in}$ and $P_{i,t,pr}^{Min}$ that hold power balance constraint (17) among MGs and maximizes (16). After solving (16)-(18), MG i corrects its $P_{i,t}^{Mout}$and $P_{i,t,pr}^{Min}$ as follows:

$$P_{i,t}^{Mout} \leftarrow m_{i,t}P_{i,t}^{Mout}, \quad P_{i,t,pr}^{Min} \leftarrow n_{i,t}^{pr}P_{i,t,pr}^{Min} \qquad \forall i,t \quad (19)$$

Then, each MG solves the problem (2)-(12) again for the next iteration without needing extra negotiation for informing other MGs about corrected values at the current iteration.

IV. Extending Resilience for Cyber Domain

A. DA Threats Model

Here, we consider two types of DA threats. First, it is assumed that some MGs are unavailable after a few ACA iterations until the end of the current time step. So, some islands may be formed in the communication network. Here, this threat is called a continuous threat and can occur by launching a DoS attack or damaging the communication equipment by the main event. In this

[Downloaded from joc.kntu.ac.ir on 2026-11-11]

[DOI: 10.61186/joc.17.3.13]

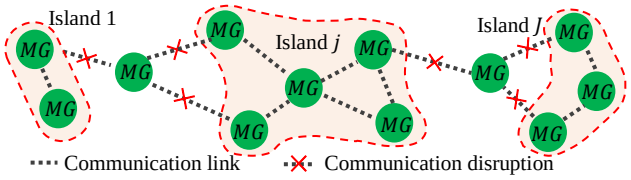


Fig. 5. Communication network islanding.

case, sharing the preamble vectors along with the power values helps MGs recognize island formation. However, it increases exchanged data length and ACA convergence time, which causes vulnerability against the temporary unavailability of MGs as the second type of threat. This threat is named the alternative threat and can be occurred due to a DoS attack [37], [38], which is launched for some random time intervals during running ACA. So, it needs more time for convergence, especially for a large network. Hence, in addition to considering the shorter operation window in the MPC method, the CS method is utilized to deal with this problem by reducing the exchanged data length.

B. Communication Network Islanding Detection in Case of Continuous Threats

In (13)-(15), knowing the accurate values of N and μ is essential. The studies focused on NMGs operation assumed the communication network is strongly connected, i.e., no island exists. While Fig. 5 shows that threats to DA may change network topology by forming J islands with N_j MGs on each island. So, for the jth island:

$$P_t^{Tout} = N_j . S_{i,t}^{Pout} \quad , \quad P_{t,pr}^{Tin} = N_j . S_{i,t,pr}^{Pin} \tag{20}$$

For the island detection and calculating N_j, the $N \times N$ invertible matrix Φ is defined and shared by DNO. Here, Φ is randomly generated from a Gaussian distribution. $\boldsymbol{\varphi}_m$ is the mth row of Φ and $1 \le m \le N$, and φ_m^i is its ith elements (corresponding to the ith MG's ID). For mth row, ith MG initializes y_m^l with φ_m^i and updates it using ACA as follows:

$$y_m^l = y_m^{l-1} + \mu \sum_{r \in B_i} (y_{m,r}^{l-1} - y_m^{l-1}) \tag{21}$$

Then y_m^l converges to the average of $\boldsymbol{\varphi}_m$ elements corresponding to MGs' ID in the jth island, i.e.:

$$y_m^l = (1/N_j) \sum_{i \in I_j} \varphi_m^i \tag{22}$$

where I_j is MGs ID set for jth island. By defining vector $\boldsymbol{y}^T = [y_1^l, y_2^l, \dots, y_N^l]$ and vector $\boldsymbol{x}$ with length N, vector $\boldsymbol{y}$ can be written as the following linear matrix form:

$$\boldsymbol{y} = \Phi \boldsymbol{x} \tag{23}$$

Since mth element of $\boldsymbol{y}$ is the average of elements in $\boldsymbol{\varphi}_m$ corresponding to the MGs' ID in the island j, elements of $\boldsymbol{x}$ must be $1/N_j$ for whose are correspond to MGs' ID in the island j; and zero for the others. In the island j, all MGs have vector $\boldsymbol{y}$. Therefore, they can obtain vector $\boldsymbol{x}$ as follows:

$$\boldsymbol{x} = \Phi^{-1} \boldsymbol{y} \tag{24}$$

Consequently, each MG can check the following properties:

$$All\ none\ zero\ values\ of\ \boldsymbol{x} = (N_j)^{-1} \tag{25a}$$

$$N_j = card(\boldsymbol{x}) \tag{25b}$$

where $card$ gives the number of nonzero elements. In brief, each MG sends its data vector at the beginning. This vector includes a column of Φ corresponding to its ID as the initial values of the preamble vector along with power data. After ACA convergence, they converge to the average values, i.e., $[\boldsymbol{y}, \boldsymbol{S_i^{Pout}}, \boldsymbol{S_i^{Pin}}]$, where $\boldsymbol{S_i^{Pout}}$ and $\boldsymbol{S_i^{Pin}}$ are vectors of $S_{i,t}^{Pout}$ and $S_{i,t,pr}^{Pin}$ for all $t \in \{t_p, t_p + T\}$ and pr. Then, $\boldsymbol{x}$ is calculated. By holding (25), MGs can verify the correctness of converged values. So, sharing the preamble vector along with the power values with the same protocol helps MGs to be informed about the incorrect convergence of ACA. If (25) does not hold, MGs with abnormal activities in the communication process, like absence in the last I iterations and deviation existence among average values of them and their neighbors, will be excluded by neighboring counterparts. Then, the proposed framework is executed again. I is the upper bound of the iteration number of ACA for the strongly connected communication network. ACA converges when $\mu \in (0, 2/\lambda_1)$ [39] or with the fastest rate when $\mu = 2/(\lambda_1 + \lambda_{N-1})$ [10]. λ_i is the ith largest eigenvalue of the matrix L. So:

$$I = \frac{ln(\theta_c/\theta_0)}{ln(1-\mu\lambda_{N-1})} \tag{26}$$

where θ_c and θ_0 are the converged and initial standard deviation of exchanged power values [39]. However, continuous or alternative DA threats change the network topology and increase the iterations number. So, it is set to be δI (where $\delta \ge 1$) with respect to the network constraints. Also, changing the communication network topology and, consequently, matrix L causes concern in choosing μ. The following proposition guarantees that ACA always converges for any arbitrary islanded topology.

Proposition: Let Ω be the Laplacian matrix representing any arbitrarily islanded part of the original communication network, and ω_1 be the largest eigenvalue of it. For this case, we have $\omega_1 \le \lambda_1$ [40]. In addition, for the islanded part, ACA converges if $\mu \in (0, 2/\omega_1)$. So, we can write $\omega_1 \le \lambda_1 \le \lambda_1 + \lambda_{N-1}$, and:

$$\frac{2}{\lambda_1 + \lambda_{N-1}} \le \frac{2}{\lambda_1} \le \frac{2}{\omega_1} \tag{27}$$

Consequently, by choosing $\mu = 2/(\lambda_1 + \lambda_{N-1})$ based on the original network, for any arbitrary islanded topology, we have $\mu \in (0, 2/\omega_1)$. Hence, ACA converges for any islanding scenario for continuous or alternative threats (when δI is large).

C. CS-Based Approach

For calculating vector $\boldsymbol{x}$, each MG shares its preamble

[Downloaded from joc.kntu.ac.ir on 2026-11-11]

[DOI: 10.61186/joc.17.3.13]

vector with length N. However, in the case of an alternative DoS attack, ACA convergence needs more iterations and time, particularly for communication networks with low connectivity and when N is large. Here, the CS approach is utilized to reduce the preamble vector length [33]. This approach is implemented using ACA with the same protocol for power data distribution. Based on the CS theory, vector $\boldsymbol{y}$ can be acquired from the M (instead of N, where $M < N$) inner product of $\boldsymbol{\varphi_m}$ and $\boldsymbol{x}$, or in linear matrix form $\boldsymbol{y} = \Phi\boldsymbol{x}$, where $1 \leq m \leq M$, and Φ is an $M \times N$ matrix. Hence, the length of the preamble vector (column of Φ) reduces from N to M. The CS problem is underdetermined and cannot be solved using (24). In this case, if Φ is randomly populated with entries drawn from a suitable distribution and $\boldsymbol{x}$ has the sparse representation over an appropriate $N \times N$ orthogonal basis Ψ such that $\boldsymbol{x} = \Psi\boldsymbol{\alpha}$ (where $\boldsymbol{\alpha}$ is the sparse representation of $\boldsymbol{x}$), it is possible to reconstruct $\boldsymbol{x}$ from $\boldsymbol{y}$ [33], [34] by solving the following problem:

$$\min_{\alpha} \|\boldsymbol{\alpha}\|_1 \tag{28}$$

$$\text{s.t.} \quad \boldsymbol{y} = \Phi\Psi\boldsymbol{\alpha} \tag{29}$$

where $\|.\|_1$ is the $l1$ norm. After finding $\boldsymbol{\alpha}$, $\boldsymbol{x}$ is calculated by $\boldsymbol{x} = \Psi\boldsymbol{\alpha}$. Here, CS theory is applied for the network with the ring topology.

D. Solving Procedure

The optimization problems (16)-(18) and (2)-(12) are linear programming and mixed integer linear programming problems, which can be solved by general optimization solvers of proper software like MATLAB. In addition, optimization problem (28)-(29) can be solved using the l1-magic package [41]. For more clarity, the sequence of implementation steps of the proposed framework is represented in the flowchart of Fig. 6. In this flowchart, the value of err^k is defined as $\sum_{t=t_p}^{t_p+T}\left|P_t^{Tout} - P_t^{Tin}\right|$ at the kth iteration of the main problem (MP). If $err^k < \epsilon_1$, then consensus is reached. If the difference of power imbalance between two consecutive iterations is lower than ϵ_2, the correcting phase is ignored for accelerating the MP convergence. After convergence, MGs reschedule themselves for optimal operation by fixing exchangeable power and ES's SOC values [11].

V. Numerical Results

The proposed method has been examined on a network with 14 MGs with six different types (denoted by A, B…, F), whose information is taken from [10], [11]. It is assumed that MGs disconnect from the main grid between 8:00-20:00, and wind units are shut off due to high wind speed from 5:00 to 18:00. Two priority levels ($\pi = 2$) are assumed. MGs types A and E have the higher priority with 10000 \$/MWh LS cost, and others have 4000 \$/MWh LS cost. The study horizon is assumed 24 hours. T is set to be 16 (4 hours with the 15-minute Δt). The values of ρ_i, β_i, ω_i, ϵ_1, ϵ_2 and k_{max} are set to be 10^2, 10^5, 10^6, 10^{-4}, 0.02 and 30. LPP is set to be 42 \$/MWh, which is almost 5% higher than MTs' maximum generation cost. Since $P_{i,t}^{xout}$ and $P_{i,t}^{xin}$ is assumed 2 MW, θ_0 is set to be 1 MW [39]. Also, $\theta_c = 10^{-4}$. As aforementioned, MGs communicate with each other through the ring topology. μ, I and δ are set to be 0.4764, 93 and 4. Φ is randomly generated from a Gaussian distribution for both non-CS and CS mode [33].

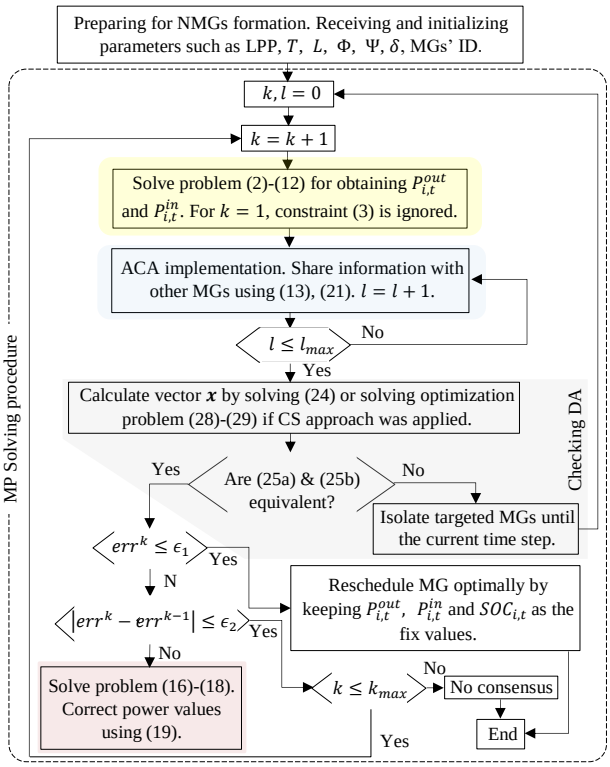


Fig. 6. Flowchart of the proposed method. It is executed by each MG at each time step.

A. The Impact of Physical Components Outages

Fig. 7(a) represents MGs' LS for independent mode. In this mode, MGs types D and F have no LS due to sufficient generation and ESs' capacities. After NMGs formation, MGs share energy with each other. Fig. 7(b) shows P2P energy sharing, where MGs types D, E and F generate supporting power. Due to the MGs' different load patterns (e.g., MGs type E), they support each other alternatively. Table 2 shows the operation costs and amount of unserved energy (UE), which is the ratio of LS to the total loads at the same time intervals. When $\sigma = 0$, MGs only maximize exporting power and minimize importing power and LS, which is roughly equivalent to the minimization of MGs operation cost. In this case, first, the higher priority MGs (i.e., A and E) are supplied. Hence, other MGs like type B must perform LS due to

[Downloaded from joc.kntu.ac.ir on 2026-11-11]

[DOI: 10.61186/joc.17.3.13]

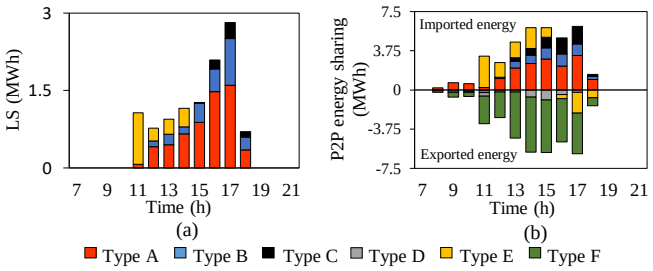


Fig. 7. (a) Hourly average of LS in the independent mode. (b) P2P energy exchange (P2PEE) (σ=0).

TABLE 2
OPERATION COST AND LS OF MGS.

MGs type		A	B	C	D	E	F	TP2PEE
$\sigma = 0$	Cost	4223	2696	3234	3631	1769	47	36.45
	LS	-	0.039	-	-	-	-	
	UE	-	1.6%	-	-	-	-	
$\sigma = 0.1$	Cost	4309	2592	3321	3696	1833	178	24.01
	LS	-	-	-	-	-	-	
	UE	-	-	-	-	-	-	
$\sigma = 200$	Cost	4310	3007	3635	3715	1830	48	43.45
	LS	-	0.1	0.079	-	-	-	
	UE	-	4.4%	4.5%	-	-	-	

LS: Load shedding (MWh). UE: Unserved energy ratio.

insufficient supporting power and stored energy in the ESs. If $\sigma > 0$, MGs keep the SOC level at higher values, which increases the operation cost for some MGs. Fig. 8(a) shows the mean of SOC for all MGs. If $\sigma \ll \rho$ (e.g., 0.1), MGs charge ESs to the maximum capacity and use them when they need power instead of importing it. So, total P2P exchanged energy (TP2PEE) decreases. If $\sigma \gg \rho$ (e.g., 200), MGs import power and charge ESs except when they have LS and cannot import power. So, TP2PEE increases.

For evaluating the impact of unpredicted contingency, it is assumed that 2 MW MTs in MG D.12 and all MTs in MGs F.8 and F.14 are interrupted from 15:00 to 19:00 due to damage to feeding gas pipelines. Table 3 shows MGs types A and E are mainly supplied. As expected, MGs operation costs were decreased when $\sigma > 0$, except for MG type A due to MTs ramp rate in MGs type E for generating supporting power. In the completion of Table 3, in Fig. 8(b), due to insufficient stored energy in ESs when $\sigma = 0$, some MGs experience more LS. If $\sigma = 200$, MGs compensate only their power deficiency by using ESs and return the SOC level to its maximum value as soon as possible. While, if $\sigma = 0.1$, MGs use their stored energy to supply other MGs. For $\sigma = 200$ (it will be used in the remainder of the paper), MGs are risk-averse and prepare themselves for the worst cases. For $\sigma = 0.1$, MGs are risk-taker and useful for cases with minimum errors in predictions. MGs can arbitrarily set σ based on their preferences.

In these experiments, due to maximizing exportable power, minimizing importable power, and correcting these values for holding power balance, the MP converges at two iterations for most of the time.

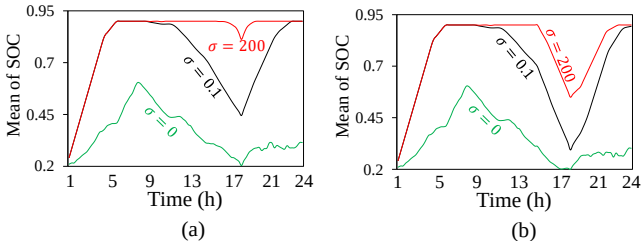


Fig. 8. Average SOC level of ESs. (a) Proactively scheduling. (b) Occurring unexpected outages.

TABLE 3
OPERATION COST AND LS IN THE CASE OF SOME MTS' OUTAGES

MGs type		A	B	C	D.4	D.12	E	F.6	F.8, F.14
$\sigma = 0$	Cost	7486	9227	11490	3604	50330	3050	33	65788
	LS	0.33	1.69	2.08	-	11.81	0.13	-	16.43
	UE	3.4%	10%	11.1%	-	43.6%	3%	-	79.8%
$\sigma = 0.1$	Cost	4310	6748	4979	3664	38119	1810	132	57897
	LS	-	1.05	0.418	-	8.7	-	-	14.62
	UE	-	6.6%	2.4%	-	34.6%	-	-	70.9%
$\sigma = 200$	Cost	8478	8129	5686	3675	43928	1771	17	64401
	LS	0.418	1.4	0.6	-	10.17	-	-	16.1
	UE	2.4%	8.9%	3.5%	-	40.4%	-	-	78%

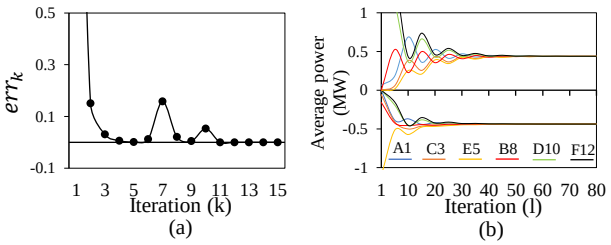


Fig. 9. (a) MP convergence. (b) ACA convergence. For the clarity, ACA convergence is shown in Fig. 9(b) for some MGs' and l. Negative/positive values represent average of exported/imported power.

However, for holding operational constraints like MTs ramp rate, more iterations are needed for a few time steps. Fig. 9(a) shows the MP convergence at t_p =70, which takes 11 iterations. Fig. 9(b) shows the ACA convergence to the average of total imported and exported power at the last iteration of the MP at this time step, which also shows balance among MGs.

B. *Resilience Against DA threat*

The performance of the proposed framework under DA threats is analyzed in the following two attack cases.

1) Continuous DoS attack: Fig. 10 shows island formation in the communication network when a DoS attack disables MGs type E for information sharing. This attack is launched at the ninth iteration ($l = 9$) of ACA at the second iteration of the MP ($k = 2$) at 15:00 and continues until the end of the current time step. We define non-resilience (NR) mode (without preamble sending) and resilient data broadcasting (RDB) mode (with preamble sending). Fig. 11(a) and (b) illustrate the ACA convergence of MG D.4 and MG B.10. These figures show that total exchangeable power converges to the

[Downloaded from joc.kntu.ac.ir on 2026-11-11]
[DOI: 10.61186/joc.17.3.13]

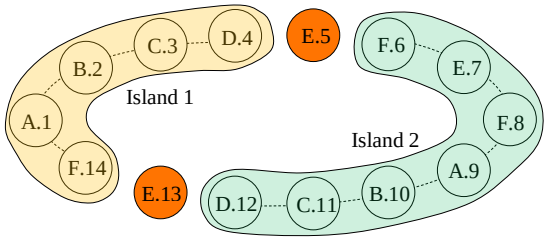


Fig. 10. NMGs' communication network topology with two islands.

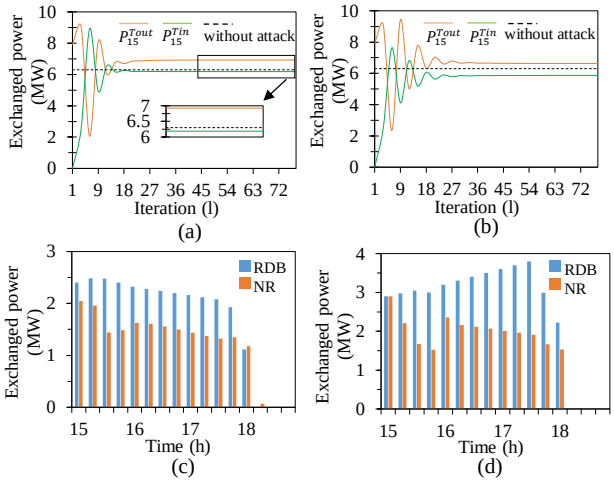


Fig. 11. Impact of continuous DoS attack on incorrect convergence of ACA and determining exchangeable power among MGs. (a) ACA convergence in the island 1. (b) ACA convergence in the island 2. (c) Exchanged power in the island 1. (d) Exchanged power in the island 2.

incorrect values in NR mode for all MGs. Since exported power is higher than imported power, MGs reduce it to hold the power balance among MGs in correcting phase. As shown in Fig. 11(c) and Fig.11(d), exchanged power in NR mode is reduced compared to RDB in the next iteration at 15:00. This issue is also observed when the attack is repeated for each time step from 15:00 to 19:00. So, a relatively simple and cheap DoS attack can affect the system data integrity like an FDI attack.

Fig. 12 shows the resilience curve of MG B.2. Here, the system performance is considered as the hourly average of the normalized supplied load. The resilience curve (RC) 1 shows the performance of MG B.2 against extreme weather events in the independent mode. However, this MG supplies most of its load by importing power from other MGs in networked mode. RC2 shows that the system performance is close to the targeted values (i.e., 1) in this case. On the other hand, after the cyber-attack from 15:00 to 19:00, more LS occurred, which can be verified by RC3 in Fig. 12. Because as shown in Fig. 11, exchangeable power decreases. In Fig. 12, RC4 shows this MG's performance with considering RDB. Due to islanding in the communication network, RC4 was expected to be lower than RC2. However, in comparison to RC3, RC4 has higher values.

Fig. 13 shows the islanding detection for fully

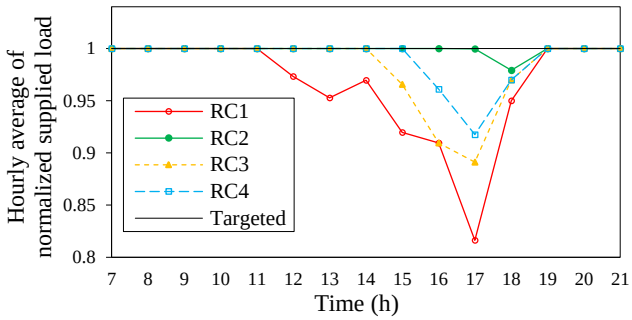


Fig. 12. Resilience curve of MG B.2 in different cases.

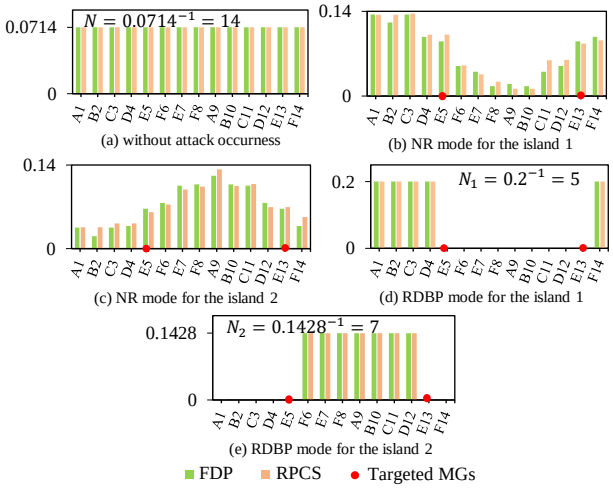


Fig. 13. Vector $\boldsymbol{x}$ after ACA convergence for the RDB. (a) without attack occurrences. (b) NR mode for the island 1. (c) NR mode for the island 2. (d) RDBP mode for the island 1. (e) RDBP mode for the island 2.

distributing preamble (FDP) vector and reduced preamble vector based on CS (RPCS) cases in RDB mode. The length of the preamble vector in FDP and RPCS is set to be 14 and 11. Regarding the ring topology of the communication network and assigning MGs' ID in serial form, Ψ is considered as the inverse of the corrected discrete derivative operator as follows:

$$\Psi^{-1} = \begin{bmatrix} 1 & -1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & -1 & \cdots & 0 & 0 & 0 \\ \vdots & & & \ddots & & & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 1 & -1 \\ 0 & 0 & 0 & \cdots & 0 & 0 & 0.01 \end{bmatrix} \quad (30)$$

Fig. 13(a) shows vector $\boldsymbol{x}$ without the attack occurring. Using (25), the number of MGs is obtained 14. After the attack, MGs on islands 1 and 2 calculate $\boldsymbol{x}$ as shown in Fig. 13(b), (c). By checking (25), each MG can detect the attack occurring. By isolating targeted MGs by their neighbors and repeating the MP, each MG calculates $\boldsymbol{x}$ as shown in Fig. 13(d), (e) and verifies the correctness of the converged power values using (25).

For more evaluation in a larger network (e.g., smart homes network [39]), Fig. 14 shows data broadcasting time for a network with different numbers of MGs. The data broadcasting time is calculated similarly to the

[Downloaded from joc.kntu.ac.ir on 2026-11-11]

[DOI: 10.61186/joc.17.3.13]

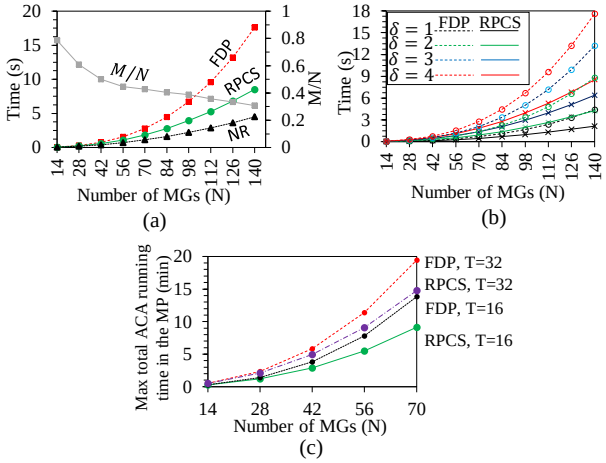


Fig. 14. Comparison of ACA convergence time. (a) ACA convergence time at each iteration of MP. (b) Comparison for different value of δ. (c) Comparison of two different values of T.

method in [42]. Here, 25Mbps communication bandwidth and double-precision floating-point numbering format are considered. Fig. 14(a) shows that the required time for ACA convergence increases like an exponential curve in FDP. In contrast, in RPCS mode, it is increased at a slower rate and relatively near NR. So, with equal iterations, RPCS converges faster. This feature appears due to CS's ability to reduce the needed data for sending. Also, it shows that for the large network, the ratio of preamble vector length in RPCS (M) is reduced more for RPCS. Fig. 14(b) shows the required iterations for ACA convergence at an iteration of MP for different values of δ. For the larger network in RPCS, ACA convergence time in the equal iterations number is almost twice FDP. When $\delta = 4$, in RPCS, ACA converges at 8.5s, while for FDP, it takes 17.6s for a network with 140 MGs. Fig. 14(c) shows the maximum total ACA running time for 30 iterations of the MP and two different values of T when bandwidth is reduced to ten times. For both cases in RCPS mode, MGs reach consensus within Δt. However, with a shorter window for MPC, this procedure takes less time, even in case of bandwidth limitation (e.g., decreasing of communication channel SINR [24]).

2) Alternative DoS attack: It is shown that the required time for ACA convergence reduces in RPCS. As shown in Fig. 15, it may be helpful for alternative DoS attacks, in which some transmission attempts fail at different times. This attack's parameters are extracted from [38]. This attack is assumed to be launched alternatively and targets all MGs in a network with 140 peers. However, in intervals without attack, MGs exchange data with each other. Also, it is assumed that half of MGs share zero values, and others share 2 (maximum value of $P_{i,t}^{ex}$). So, ACA converges to the average values (i.e., 1). In RPCS, ACA converges about twice faster than FDP due to the execution of more iterations at the same time. Therefore,

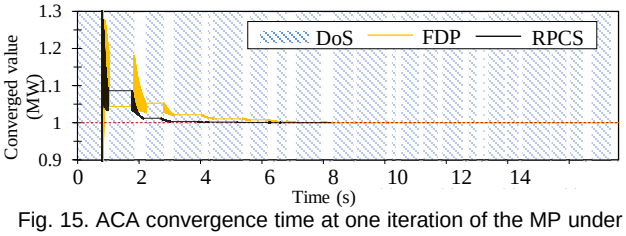


Fig. 15. ACA convergence time at one iteration of the MP under alternative DoS attack on NMGs. For the sake of clear representation, convergence of iteration value of one MG has been shown.

TABLE 4
CONVERGENCE TIME AND DIVERGING ERROR

δ	δI	FDP		RPCS	
		Time (s)	Max convergence error	Time (s)	Max convergence error
1	9147	4.4	0.0162	2.1	0.023
2	18294	8.8	0.0011	4.2	0.0015
3	27441	13.2	1.07×10^{-4}	6.4	1.52×10^{-4}
4	36588	17.6	1.35×10^{-5}	8.5	5.2×10^{-6}

compared with FDP, the value of δ can be increased in RPCS to have a chance for consensus, and more MGs will be present for energy sharing, which can be verified by Table 4 and Fig. 14. Hence, RPCS has more resilience in comparison with FDP, especially when time step duration Δt is short.

VI. CONCLUSION

This paper studied the simultaneous resilience enhancement of physical and cyber domains for NMGs. Results show that applying the MPC method and dynamic usage of ESs increased MGs' ability to withstand unpredicted events. By the communication network islanding detection, MGs could verify the correct convergence of the shared power values against DA threats like DoS attacks. In the case of cyber threat occurrence, it was shown that although the system performance level degraded, its decrease is lower than the non-resilient case against simultaneous cyber-physical threats. For instance, compared with the independent operation mode, the unsupplied load of MG B.2 decreased by 95% in the networked mode. However, with occurring a cyber threat, this value was reduced to 47%. While by considering cyber resiliency, this value is 69%. Also, the utilization of the CS method and MPC approach can cause more resilience in the case of alternative DoS attacks by reducing the required time for reaching consensus. So, this method can facilitate direct energy sharing in a network with numerous peers like smart homes with more resilience. Hence, by extending the CS approach for reducing the power data length and designing the sparse representation dictionary for any arbitrary communication topology, the need for having a large network with high connectivity and cost is removed. Therefore, the future outlooks of studies directions can contain these issues. Moreover, consideration of the power flow control constraints and

[Downloaded from joc.kntu.ac.ir on 2026-11-11]

[DOI: 10.61186/joc.17.3.13]

interaction with the network operator, along with the application of blockchain technology in this method, could be interesting for more investigation in future works.

REFERENCES

[1] A. Gholami, T. Shekari, M. H. Amirioun, F. Aminifar, M. H. Amini, and A. Sargolzaei, "Toward a consensus on the definition and taxonomy of power system resilience," *IEEE Access*, vol. 6, pp. 32035–32053, 2018.

[2] S. Ma, B. Chen and Z. Wang, "Resilience Enhancement Strategy for Distribution Systems Under Extreme Weather Events," *IEEE Transactions on Smart Grid*, vol. 9, no. 2, pp. 1442-1451, 2018.

[3] M. H. Amirioun, F. Aminifar and H. Lesani, "Resilience-Oriented Proactive Management of Microgrids Against Windstorms," *IEEE Transactions on Power Systems*, vol. 33, no. 4, pp. 4275-4284, 2018.

[4] H. A. Gabbar and A. Gabbar, "Risk Analysis and Self-Healing Approach for Resilient Interconnect Micro Energy Grids," *Sustainable Cities and Society*, vol. 32, pp. 638-653, 2017.

[5] B. Chen, J. Wang, X. Lu, C. Chen and S. Zhao, "Networked Microgrids for Grid Resilience, Robustness, and Efficiency: A Review," *IEEE Transactions on Smart Grid*, vol. 12, no. 1, pp. 18-32, 2021.

[6] H. Farzin, M. Fotuhi-Firuzabad, and M. Moeini-Aghtaie, "Enhancing power system resilience through hierarchical outage management in multi-microgrids", *IEEE Transactions on smart grid*, vol. 7, no. 6, pp. 2869-2879, 2016.

[7] H. Farzin, R. Ghorani, M. Fotuhi-Firuzabad, and M. Moeini-Aghtaie, "A market mechanism to quantify emergency energy transactions value in a multi-microgrid system," *IEEE Transactions on Sustainable Energy*, vol. 10, no. 1, pp. 426-437, 2019.

[8] A. Hussain, V. Bui and H. Kim, "An Effort-Based Reward Approach for Allocating Load Shedding Amount in Networked Microgrids Using Multiagent System," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 4, pp. 2268-2279, 2020.

[9] F. Shen, Q. Wu, J. Zhao, W. Wei, N. D. Hatziargyriou and F. Liu, "Distributed Risk-Limiting Load Restoration in Unbalanced Distribution Systems with Networked Microgrids," *IEEE Transactions on Smart Grid*, vol. 11, no. 6, pp. 4574-4586, 2020.

[10] Z. Wang, B. Chen, J. Wang, and C. Chen, "Networked microgrids for self-healing power systems," *IEEE Transactions on smart grid*, vol. 7, no. 1, pp. 310–319, 2016.

[11] M. Mehri Arsoon and S.M. Moghaddas-Tafreshi, "Peer-to-peer energy bartering for the resilience response enhancement of networked microgrids," *Applied Energy*, vol. 261, p. 114413, 2020.

[12] T. Sousa, T. Soares, P. Pinson, F. Moret, T. Baroche, and E. Sorin, "Peer -to-peer and community-based markets: A comprehensive review," *Renewable and Sustainable Energy Reviews*., vol.104, pp.367-378, 2019.

[13] T. Perger, L. Wachter, A. Fleischhacker and H. Auer, "PV sharing in local communities: Peer-to-peer trading under consideration of the prosumers' willingness-to-pay", *Sustainable Cities and Society*, vol. 66, pp. 102634, 2020.

[14] S. Xuanyue, X. Wang, X. Wu, Y. Wang, Z. Song, B. Wang, Z. Ma, "Peer-to-peer multi-energy distributed trading for interconnected microgrids: A general Nash bargaining approach," *International Journal of Electrical Power and Energy Systems*, vol. 138, pp. 107892, 2022.

[15] M. Mehri Arsoon and S.M. Moghaddas-Tafreshi, "Resilience-Oriented Proactive Peer to Peer Multiple Energy Carriers Swapping Framework for the Partial Networked Energy Hubs," *Sustainable Energy Technologies and Assessments*, vol. 53, no. 102576, 2022.

[16] D. Xu et al., "Peer-to-Peer Multienergy and Communication Resource Trading for Interconnected Microgrids," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 4, pp. 2522-2533, 2021.

[17] Z. Zhao et al., "Distributed Robust Model Predictive Control-Based Energy Management Strategy for Islanded Multi-Microgrids Considering Uncertainty," *IEEE Transactions on Smart Grid*, vol. 13, no. 3, pp. 2107-2120, 2022.

[18] M. N. Alam, S. Chakrabarti and A. Ghosh, "Networked Microgrids: State-of-the-Art and Future Perspectives," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 3, pp. 1238-1250, 2019.

[19] N. Li, W. Hou and S. E. Ghoreyshipour, "A secured transactive energy management framework for home AC/DC microgrids," *Sustainable Cities and Society*, vol. 74, 2021.

[20] J. Tian, B. Wang, T. Li, F. Shang and K. Cao, "Coordinated cyber-physical attacks considering DoS attacks in power systems," *International Journal of Robust and Nonlinear Control*, vol. 30, no. 11, pp. 4345-4358, 2020.

[21] M. M. Arsoon and S. M. Moghaddas-Tafreshi, "Modeling Data Intrusion Attacks on Energy Storage for Vulnerability Assessment of Smart Microgrid Operation," *2021 11th Smart Grid Conference (SGC)*, Tabriz, Iran, Islamic Republic of, 2021, pp. 1-5.

[22] J. Duan and M. Chow, "A Resilient Consensus-Based Distributed Energy Management Algorithm against Data Integrity Attacks," *IEEE Transactions on smart grid*, vol. 10, no. 5, pp. 4729-4740, 2019.

[23] K. Pan, A. Teixeira, M. Cvetkovic, and P. Palensky, "Cyber Risk Analysis of Combined Data Attacks Against Power System State Estimation," *IEEE*

[Downloaded from joc.kntu.ac.ir on 2026-11-11]

[DOI: 10.61186/joc.17.3.13]

Transactions on smart grid, vol. 10, no. 3, pp. 3044-3056, 2019.

[24] Q. Zhou, M. Shahidehpour, A. Paaso, S. Bahramirad, A. Alabdulwahab and A. Abusorrah, "Distributed Control and Communication Strategies in Networked Microgrids," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 4, pp. 2586-2633, 2020.

[25] L. Ding, Q. Han, B. Ning and D. Yue, "Distributed Resilient Finite-Time Secondary Control for Heterogeneous Battery Energy Storage Systems Under Denial-of-Service Attacks," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 7, pp. 4909-4919, 2020.

[26] T. Qian, X. Chen, Y. Xin, W. Tang, L. Wang, "Resilient decentralized optimization of chance constrained electricity-gas systems over lossy communication networks," *Energy*, vol. 239, pp. 122158, 2022.

[27] X. Liang, Z. Li, W. Huang, Q. H. Wu and H. Zhang, "Relaxed Alternating Direction Method of Multipliers for Hedging Communication Packet Loss in Integrated Electrical and Heating System," *Journal of Modern Power Systems and Clean Energy*, vol. 8, no. 5, pp. 874-883, 2020.

[28] C. Yuan, Z. Li and H. Xin, "Cyber-Resilient Distributed Operation of Active Distribution Networks Based on Relaxed Alternating Direction Method of Multipliers," 2021 4th International Conference on Energy, Electrical and Power Engineering (CEEPE), 2021, pp. 415-421.

[29] J. Duan and M. -Y. Chow, "Robust Consensus-Based Distributed Energy Management for Microgrids With Packet Losses Tolerance," *IEEE Transactions on Smart Grid*, vol. 11, no. 1, pp. 281-290, 2020.

[30] P. T. Mana, K. P. Schneider, W. Du, M. Mukherjee, T. Hardy and F. K. Tuffner, "Study of Microgrid Resilience Through Co-Simulation of Power System Dynamics and Communication Systems," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 3, pp. 1905-1915, 2021.

[31] Z. Wang, H. He, Z. Wan and Y. Sun, "Coordinated Topology Attacks in Smart Grid Using Deep Reinforcement Learning," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 2, pp. 1407-1415, 2021.

[32] L. Wei, A. I. Sarwat, W. Saad and S. Biswas, "Stochastic Games for Power Grid Protection Against Coordinated Cyber-Physical Attacks," *IEEE Transactions on Smart Grid*, vol. 9, no. 2, pp. 684-694, 2018.

[33] E. J. Candes and T. Tao, "Decoding by linear programming," *IEEE Transactions on Information Theory*, vol. 51, no.12, pp.4203-4215, 2005.

[34] K. Jia, B. Yang, T. Bi and L. Zheng, "An Improved Sparse-Measurement-Based Fault Location Technology for Distribution Networks," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 3, pp. 1712-1720, 2021.

[35] Z. Bie, Y. Lin, G. Li, F. Li, "Battling the extreme: a study on the power system resilience," *Proceedings of the IEEE*, vol. 105, no. 7, pp. 1253-1266, 2017.

[36] H. Ma, Z. Liu, M. Li, B. Wangd, Y. Si, Y. Yang, M. A. Mohamed, "A two-stage optimal scheduling method for active distribution networks considering uncertainty risk," *Energy Reports*, vol. 7, pp. 4633–4641, 2021.

[37] A. Cetinkaya, H. Ishii, and T. Hayakawa, "An Overview on Denial-of-Service Attacks in Control Systems: Attack Models and Security Analyses," *Entropy*, vol. 21, no. 2, p. 210, 2019.

[38] S. Feng and P. Tesi, "Resilient control under denial-of-service: Robust design", *Automatica*, vol. 79, pp. 42-51, 2017.

[39] C. Chen, J. Wang, and S. Kishore, "A Distributed Direct Load Control Approach for Large-Scale Residential Demand Response," *IEEE Transactions on Power Systems*, vol. 29, no. 5, pp. 2219-2228, 2014.

[40] E. Brouwer and W. H. Haemers, Spectra of Graphs, New York:Springer, 2012, pp. 37.

[41] E. Candes and J. Romberg. (2005). L1-Magic: Recovery of Sparse Signals Via Convex Programming. [Online]. Available: https://statweb.stanford.edu/~candes/software/l1magic/downloads/l1magic.pdf

[42] A. Sheikhi, M. Rayati, S. Bahrami, and A. Mohammad Ranjbar, "Integrated Demand Side Management Game in Smart Energy Hubs," *IEEE Transactions on Smart Grid*, vol. 6, no. 2, pp. 675-683, 2015.

[Downloaded from joc.kntu.ac.ir on 2026-11-11]

[DOI: 10.61186/joc.17.3.13]