Pacific Northwest
NATIONAL LABORATORY

PNNL-37009

Peer-to-peer communication control for resilient operations of networked cyberphysical systems

November 2024

Thanh Long Vu
Sayak Mukherjee
Kyung-Bin Kwon
Veronica Edetola

U.S. DEPARTMENT OF ENERGY

Prepared for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

DISCLAIMER

PACIFIC NORTHWEST NATIONAL LABORATORY
operated by
BATTELLE
for the
UNITED STATES DEPARTMENT OF ENERGY
under Contract DE-AC05-76RL01830

Printed in the United States of America

Available to DOE and DOE contractors from
the Office of Scientific and Technical Information,
P.O. Box 62, Oak Ridge, TN 37831-0062
www.osti.gov
ph: (865) 576-8401
fox: (865) 576-5728
email: reports@osti.gov

Available to the public from the National Technical Information Service
5301 Shawnee Rd., Alexandria, VA 22312
ph: (800) 553-NTIS (6847)
or (703) 605-6000
email: info@ntis.gov
Online ordering: http://www.ntis.gov

PNNL-37009

Peer-to-peer communication control for resilient operations of networked cyberphysical systems

November 2024

Thanh Long Vu
Sayak Mukherjee
Kyung-Bin Kwon
Veronica Edetola

Prepared for
the U.S. Department of Energy
under Contract DE-AC05-76RL01830

Pacific Northwest National Laboratory
Richland, Washington 99354

Abstract

This report includes two main accomplishments of the peer-to-peer communication control for resilient operation of networked microgrids project in FY24, which include a scheme for cyberattack-aware coordination of networked microgrids for supporting voltages of bulk power systems and a scheme for price signal-based operations of EV-rich networked microgrids with mixed ownership. The cyberattack-aware scheme enables networked microgrids to distributedly determine the amount of reactive power injection to support the voltage of bulk power system (BPS) in a fair manner. In this scheme, a risk-informed algorithm is presented to generate the peer-to- peer (P2P) communication graph with minimal risk of attack on communication links. To deal with cyberattacks on MG controllers, the resilient consensus algorithm (CA) is utilized for MG controllers to robustly estimate the total reactive power headroom, from which the MGs can accurately provide the needed amount of reactive power injection for supporting the voltage of BPS. The CA implementation and performance within the P2P communication framework are demonstrated on the IEEE 39-bus system with 6 microgrids contained in the distribution feeder under different cyberattack scenarios. On the other hand, the price-based scheme enables the usage of the real-time price signal for the operations of electric vehicle (EV)-rich networked-microgrids with mixed ownership, in which not all the microgrids can communicate with the distribution system operator (DSO). In this scheme, a max consensus is introduced to enable the real-time price signal to be propagated from the DSO to all the microgrids, from which each microgrid controller will manage the DERs to balance the load demand and the power injection from the EV charging stations within its microgrid. Numerical results over one day with 288 slots of 5-minute intervals on the modified 123-node test feeder including 3 microgrids with high penetration of EV are presented to evaluate how the price signal affects the operations of networked microgrids under different charging strategies of the EV charging stations. The result indicates that our proposed EVCS (dis)charging strategy, which leverages the flexibility of EVs to support the grid through discharging during peak demand, proves to be a cost-effective solution that reduces operational costs while improving the social welfare of EV charging.

Summary

This report includes two main accomplishments of the peer-to-peer communication control for resilient operation of networked microgrids project in FY24, which include a scheme for cyberattack-aware coordination of networked microgrids for supporting voltages of bulk power systems and a scheme for price signal-based operations of EV-rich networked microgrids with mixed ownership.

In the first accomplishment, the cyberattack-aware scheme enables networked microgrids to distributedly determine the amount of reactive power injection to support the voltage of bulk power system (BPS) in a fair manner. In this scheme, a risk-informed algorithm is presented to generate the peer-to- peer (P2P) communication graph with minimal risk of attack on communication links. To deal with cyberattacks on MG controllers, the resilient consensus algorithm (CA) is utilized for MG controllers to robustly estimate the total reactive power headroom, from which the MGs can accurately provide the needed amount of reactive power injection for supporting the voltage of BPS. The CA implementation and performance within the P2P communication framework are demonstrated on the IEEE 39-bus system with 6 microgrids contained in the distribution feeder under different cyberattack scenarios.

In the second accomplishment, the price-based scheme enables the usage of the real-time price signal for the operations of electric vehicle (EV)-rich networked-microgrids with mixed ownership, in which not all the microgrids can communicate with the distribution system operator (DSO). In this scheme, a max consensus is introduced to enable the real-time price signal to be propagated from the DSO to all the microgrids, from which each microgrid controller will manage the DERs to balance the load demand and the power injection from the EV charging stations within its microgrid. Numerical results over one day with 288 slots of 5-minute intervals on the modified 123-node test feeder including 3 microgrids with high penetration of EV are presented to evaluate how the price signal affects the operations of networked microgrids under different charging strategies of the EV charging stations. The result indicates that our proposed EVCS (dis)charging strategy, which leverages the flexibility of EVs to support the grid through discharging during peak demand, proves to be a cost-effective solution that reduces operational costs while improving the social welfare of EV charging.

Acknowledgments

This research was supported by the Resilience through Data-Driven intelligently-Designed Control (RD2C), under the Laboratory Directed Research and Development (LDRD) Program at Pacific Northwest National Laboratory (PNNL). PNNL is a multi-program national laboratory operated for the U.S. Department of Energy (DOE) by Battelle Memorial Institute under Contract No. DE-AC05-76RL01830.

1.0 Cyber Attack-aware Coordination of Networked Microgrids for Supporting Voltages of Bulk Power Systems

Distributed energy resources (DERs), such as rooftop solar panels and battery energy storage systems (BESS), are being increasingly integrated into electric distribution systems to enhance utility operations and benefit end-use customers. These resources can be aggregated to form microgrids [1] and networks of microgrids [2]. Recently, microgrids and networked microgrids have been utilized as a resiliency resource, supporting end-use loads outside the point of common coupling (PCC) [3]. As networked microgrids technology becomes more mature, it is natural to consider their support to the operations of transmission system [4].

Recently, it is demonstrated that networked microgrids can support the voltage at the PCC of distribution feeder and transmission system [5]. In this peer-to-peer (P2P) communication control scheme, each microgrid controller calculates local information including its reactive power headroom and receives the sensitivity $\Delta V/\Delta Q$ curve from the distribution management system (DMS) in normal condition. During a voltage event, the DMS asks the microgrids for support by broadcasting the voltage needed to recover and re-balance the system. The microgrid controllers will then exchange information to distributedly determine the fair amount of reactive power injections by using the average consensus algorithm (CA). Different schemes for the distributed support from networked microgrids to the voltage of BPS is also presented in [6].

While coordination of microgrids can provide the operational flexibility needed for supporting transmission system and end-use demand, the distributed communication among MG controllers is vulnerable to cyberattacks on the communication links among controllers, as well as on the MG controllers themselves. As such, it is necessary to design resilient control systems to support the operations of networked microgrids in the presence of cyberattacks. This project further extends the work in [5] by considering the risk of cyberattack on communication links and MG controllers when implementing the voltage support scheme.

In the broader context of cyber-physical systems, various types of cyberattacks have been classified in [7] based on factors such as the attacker's knowledge of the system model, resource disclosure, and resource disruption. Recent studies have identified different types of attacks, including denial- of-service attacks [8], false data injection attacks [9], replay attacks [10], and covert attacks [11]. Consequently, methods for detecting, identifying, and mitigating these attacks have been explored in [12]–[15]. However, there is still limited research on designing control systems of networked microgrids that can enhance their resilience to cyberattacks.

In this project, a risk-informed algorithm is presented to generate the P2P communication graph that have minimal risk of attack on communication links. To deal with cyberattacks on MG controllers, the cyberattack-aware scheme using resilient consensus al- gorithm is introduced for MG controllers to robustly estimate the total reactive power headroom, from which the MGs can accurately provide the needed amount of reactive power injection for supporting the voltage of BPS. Simulation results on the IEEE 39-bus system with 6 microgrids contained in the distribution feeder under different cyberattack scenarios are presented to demonstrate the advantages of this approach, in comparison with the baseline scheme in [5].

1.1 Communication architecture

Consider N microgrids, MG1 , ..., MGN , operating in grid- connected mode. Each microgrid is equipped with its own controller, as showed in Fig. 1. Each controller collects information from devices within that microgrid and per- forms different control functions. Moreover, the controllers can exchange information amongst each other and receive signals from the DMS. These controller functionalities can be implemented in commercially available controllers like ORNL CEISMIC microgrid controller [16].

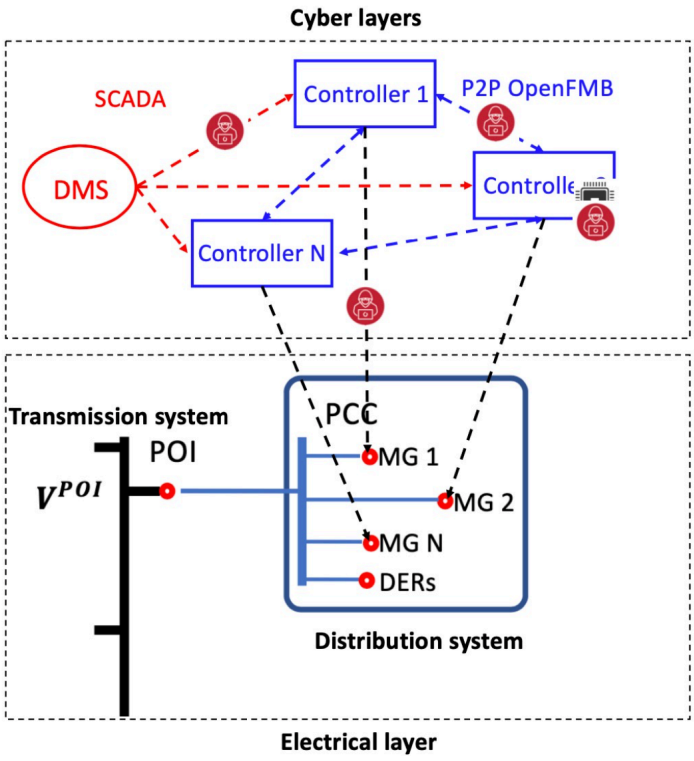

Fig. 1: Electrical and cyber architecture in operations of networked microgrids connected with the BPS.

For the operating infrastructure of networked microgrids connected to the BPS shown in Fig. 1, the following cyber layers are typically available:

- Layer 1 (red dashed lines): The communication at this level is between DMS and microgrid controllers. To limit information exchange in this communication level, it is considered unidirectional with the DMS allowed to broadcast signals to the microgrid controllers, but unable to receive information from them. In this paper, it is considered that DMS can send the dQ/dV curve, amount of voltage needed in abnormal events, and the risk-informed P2P communication graph to the MG controllers.

- Layer 2 (blue dashed lines): The communication at this level is realized among MG controllers through the P2P framework. The individual microgrid controllers exchange information, but not control signals. In this paper, the exchanged information is the

reactive power headroom of each microgrid. Interactions at this layer could be a traditional mapped Supervisory Control and Data Acquisition (SCADA) approach. But for scalabil- ity and for coping with authority in a mixed-ownership environment, the P2P communication approach is more appropriate.

- Layer 3 (black dashed lines): The communication at this level is realized within the microgrid. Here, the individual MG controller directly gets the information from and sends control signal to its constituent devices, such as generators, inverters, relays, and sensors. In this paper, the communication at this level is for each microgrid controller to send the reactive power setpoints to controllable devices in that microgrid to realize the reactive power injection determined by the resilient consensus algorithm in the cyber Layer 2.

In this communication architecture, there are risk of at- tacks on communication links between DMS and MG con- trollers, on the coommunication links among MG controllers, and on the MG controllers computation process. Since dis- tribution system operator can have its own process to harden the communication between DMS and MG controllers, this papers mainly focus on the risk of attacks on communication links among MG controllers and risk of attack on the MG controllers.

1.2 Voltage support decision process

The goal of the voltage support decision process is for microgrid controllers to distributedly determine the suitable amount of reactive power injection to support the voltage at the POI. This process is implemented in the following steps:

- Step 1: DMS generates the risk-minimal P2P commu- nication graph and broadcasts it to MG controllers.
- Step 2: DMS broadcasts global information to all mi- crogrid controllers, which includes the sensitivity curve $\Delta V/\Delta Q$ sent during normal operation and the needed voltage support sent after a voltage event.
- Step 3: Microgrid controllers calculate their local infor- mation, including the reactive power headroom based on its local data, and the total reactive power needed after a voltage event based on data received from DMS.
- Step 4: Microgrid controller exchanges reactive power headroom with other microgrid controllers via the risk- minimal P2P communication network.
- Step 5: Each MG controller estimates total reactive power headroom of all MGs by using the resilient consensus algorithm.
- Step 6: Microgrid controllers locally determine the suit- able local amount of additional reactive power injection within their headroom, and inject the additional reactive power into system.

It should be noted that Step 2, Step 3, and Step 6 involve local calculations and information broadcasting, which are not vulnerable to cyberattacks. The main risk of cyberattacks appear in Step 4 and Step 5 where MG controllers exchange information on the P2P communication graph and use the consensus algorithm (CA) to estimate the total reactive power headroom.

1.3 Reactive power injection determination

Note that after Step 3, each MG controller determines the amount of total reactive power needed to support the voltage of BPS, denoted as ΔQ. To fairly share this amount of reactive power support among MGs, the MG controllers will exchange the reactive power headroom with each other, via a P2P communication network, to estimate the total amount of reactive power headroom from all MGs in Step 5. Then, the fair amount of additional reactive power injection from each microgrid to support the BPS is determined as:

$$Q_i^{additional} = \frac{\tilde{Q}_i}{Est(\sum_{i=1}^{N} \tilde{Q}_i)} \Delta Q$$

where N is the number of MGs, $\tilde{Q}_i$ is the reactive power headroom of MG i, and Est($\sum_{i=1}^{N} \tilde{Q}_i$) is the estimation of total amount of reactive power headroom from all microgrids by the MG controller i. Consequently, the total additional reactive power injections from all MGs will closely equate the value expected by DMS to ensure the voltage support, as follows:

$$\begin{aligned} \sum_{i=1}^{N} Q_i^{additional} &= \sum_{i=1}^{N} \frac{\tilde{Q}_i}{Est(\sum_{i=1}^{N} \tilde{Q}_i)} \Delta Q \\ &\approx \sum_{i=1}^{N} \frac{\tilde{Q}_i}{\sum_{i=1}^{N} \tilde{Q}_i} \Delta Q = \Delta Q \end{aligned}$$

It should be noted that the ratio between the additional reactive power injection $Q_i^{additional}$ and the reactive power headroom $\tilde{Q}_i$ is approximately the same for all MGs as follows:

$$\frac{Q_i^{additional}}{\tilde{Q}_i} = \frac{\Delta Q}{Est(\sum_{i=1}^{N} \tilde{Q}_i)} \approx \frac{\Delta Q}{\sum_{i=1}^{N} \tilde{Q}_i}$$

1.4 Resilience to cyberattacks on communication links and controllers

When the risk of attack to communication links among MG controllers is deterministic (i.e., if there is an attack to the communication link among MG controllers then the DMS knows it), the DMS can just request MG controllers not use those attached links for the P2P information exchange. However, it is more typical that the DMS only knows that each communication link among MG controllers has a probability of getting attack. In this project, a risk-informed algorithm is presented for DMS to generate the P2P communication graph for the P2P information exchange among MG controllers that have minimal risk of attack on communication links.

Indeed, for each P2P communication graph ε among MG controllers, the risk of attack to the communication links of ε is calculated as follows as the total risk of cyberattacks from all its subgraphs, i.e.,

$$\mathbb{P}(\epsilon) = \sum_{\eta \subset \epsilon} \mathbb{P}(\eta)$$

where η is a subgraph of ε and $\mathbb{P}(\eta)$ is the risk of cyberattacks on the communication links of η. The risk of attack to η is calculated as

$$\mathbb{P}(\eta) = \prod_{c_{ij} \in \eta} \mathbb{P}(c_{ij})$$

where $\mathbb{P}(c_{ij})$ is the probability that the communication link c_{ij} between MG controller i and MG controller j gets attacked.

As showed in [17], to deal with the risk of cyberattacks on MG controllers, it is necessary that the P2P graph has sufficient connectivity, i.e., if there are k MG controllers got cyberattacks, then then P2P graph needs to have (2k+1) connectivity. As such, in this paper, we will only determine the P2P graph with minimal risk of attacks from the set of all P2P graphs with (2k+1) connectivity. Accordingly, the graph $\varepsilon*$ with minimal risk of getting attacks on the communication links is determined as

$$\epsilon^* = argmin_{\epsilon \in \mathcal{C}} \mathbb{P}(\epsilon)$$

where C is the set off all P2P communication graph with (2k+1) connectivity to enable the resilient consensus algorithm. The process to determine the P2P graph with minimal risk of attack to communication links is in Fig. 2. Generation of P2P graphs with (2k+1) connectivity follows graph generation algorithms in [17].

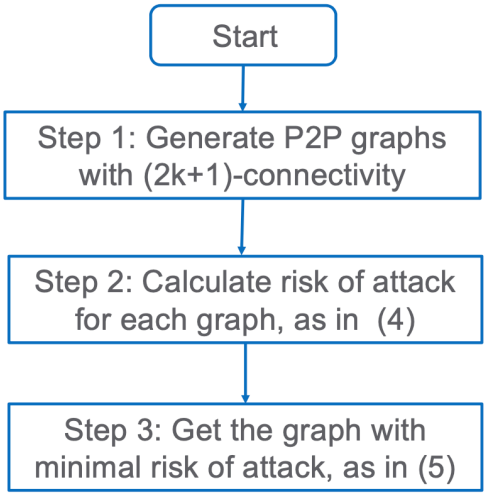

Fig. 2: Process for DMS to determine the P2P graph for information exchange among MG controllers with minimal risk of attack to communication links.

To deal with the cyberattack to k MG controllers, each MG controller uses the resilient consensus algorithm (Algorithm 1) in [17] and the generated risk-informed P2P graph with

(2k+1) connectivity to determine the total reactive power headroom in the presence of cyberattacks on the MG controllers. Note that The Algorithm 1 in [17] was used to resiliently determine the total supply of all MGs headroom in the presence of cyberattacks on the MG controllers, but here it is used to resiliently determine the total reactive power headroom in the presence of cyberattacks on the MG controllers in the same manner.

1.5 Demonstration

This section demonstrates the effectiveness of the pro- posed resilience scheme through an example how the CA can be applied to coordinate a network of microgrids to inject reactive power to support voltage of the BPS in the presence of cyberattacks. For this purpose, the IEEE 39-bus testcase is used to represent the BPS, while 6 microgrids will be placed at one distribution system connected at one bus, as showed in Fig. 3.

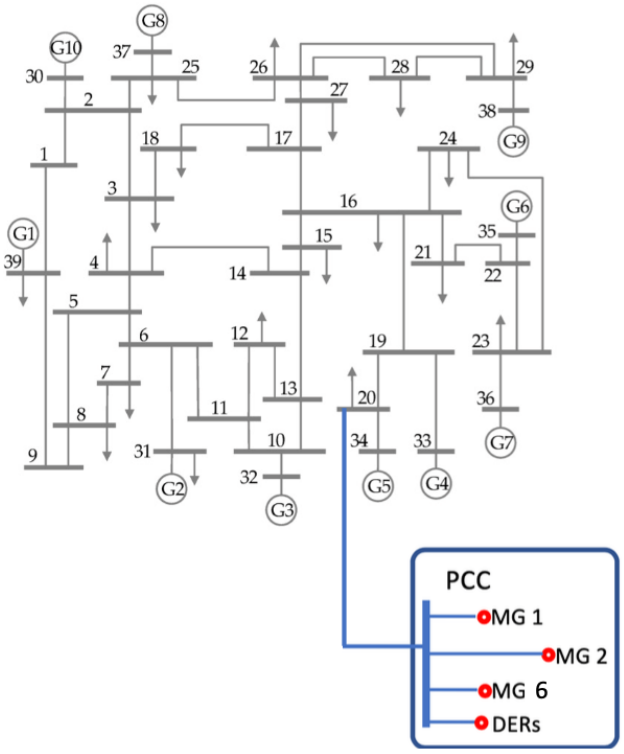

Fig. 3: IEEE 39-bus testcase with 6 microgrids connected to one distribution feeder at bus 20.

The rated reactive power and the reactive power injection before the voltage event of each microgrid are given in Table I, based on which microgrid controllers can calculate the reactive power headroom accordingly. It is note that the total reactive power headroom of all MGs is 451.44 MVAr.

Microgrid	Q_i	$\bar{Q}_i$	$\tilde{Q}_i$
1	75.83	200	124.17
2	25.69	150	124.31
3	60.81	100	39.19
4	15.57	50	34.43
5	30.35	80	49.65
6	20.31	100	79.69

TABLE I: Microgrid controllers local calculations [MVAr]

In the following scenario, it is assumed that the DMS acknowledges a need for ΔQ = 400 MVAr to support the voltage at the BPS POI after a voltage event. For a comparison, the baseline scheme is chosen as the average CA in [5] to enable MG controllers distributedly determine the amount of reactive power injection from each MG in order to provide 400 MVAr support to BPS.

Two usecases are considered to examine the effectiveness of both algorithms: (i) attacks on communication links and (ii) attack on MG controllers. In usecase (i), it is assumed that all the communication links between MG controller 1 and other MG controllers have a positive probability of getting attack. The scheme in [5] only consider the deterministic risk of attack, and hence, the DMS requests MG controllers not to use the communication links between MG controller 1 and other MG controllers. Accordingly, the P2P communication graph, generated by the DMS in [5], is not connected and the average consensus algorithm in [5] does not converge. The risk-minimal P2P graph, generated as in Section III, is still connected since it only considers the probabilistic nature of the cyberattacks on the communication links. Accordingly, the risk-minimal P2P graph for information exchange among MG controllers is generated as in Fig. 4.

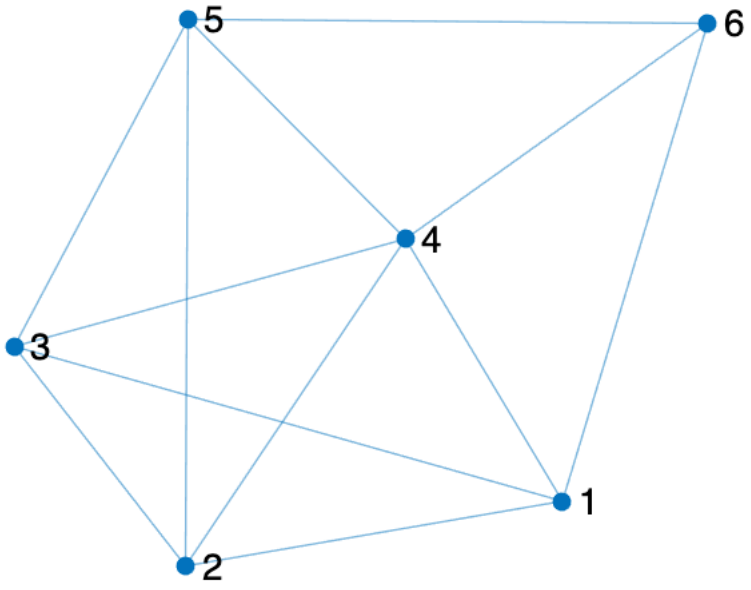

Fig. 4: Risk-minimal P2P graph for information exchange among MG controllers.

In usecase (ii), it is assumed that there is a data injection attack to MG controller 4 in a short time period resulting in data injection of [20 30 40] MVAr in three updating steps of MG controller 4 when it performs the resilient CA and the average CA in the baseline. This data injection will eventually propagate to other MG controllers when they exchange information to implement the algorithms. For a fair comparison, both algorithms in this usecase will utilize the P2P communication graph as in Fig. 4.

Using the average CA in the baseline and resilient CA, the estimations of total reactive power headroom and the additional reactive power injections from MGs are determined in Table II. It can be seen that the average CA in the baseline fails to accurately estimate the total reactive power headroom due to the data injection attack to MG controller 4, while the resilient CA allows all the MG controllers to successfully estimate the total reactive power headroom off all MGs, which is 451.44MVAr.

	Baseline with average CA		resilient CA	
MG	$Est(\sum_{i=1}^{N} \tilde{Q}_i)$	$Q_i^{additional}$	$Est(\sum_{i=1}^{N} \tilde{Q}_i)$	$Q_i^{additional}$
1	532.6734	93.2429	451.4400	110.0213
2	532.6734	93.3480	451.4400	110.1453
3	532.6734	29.4289	451.4400	34.7244
4	532.6734	25.8545	451.4400	30.5068
5	532.6734	37.2837	451.4400	43.9926
6	532.6734	59.8418	451.4400	70.6096

TABLE II: Comparison of reactive power headroom estimations and additional reactive power injections estimated using average CA and resilient CA [MVAr].

Based on the estimation of total reactive power headroom, the MG controllers calculate the total reactive power injections as in Table III. It can be seen that the resilient CA allows MG controllers to successfully support the requested amount of reactive power 400 MVAr to bring up the voltage of BPS at POI, while the average CA in the baseline does not inject enough reactive power to support the voltage of BPS.

MVAr needed	MVAr by Baseline	MVAr by resilient CA
400	338.9999	400.0000

TABLE III: Total reactive power injection from all MGs [MVAr]

2.0 Price signal-based operations of EV-rich networked microgrids with mixed ownership

Various distributed energy resources (DER), such as rooftop PV and battery energy storage systems (BESS), have been integrated into distribution systems, providing greater flexibility to support utility operations and end-use customers [18]. Furthermore, electric vehicles (EV) are going to be one of the most predominant flexibility sources in the distribution systems [19]. It is estimated that 62% of all vehicles on the US roads will be electric or plug-in electric vehicles by 2050 [20], [21]. As a point of aggregation for collections of DERs, microgrids will have to adopt large penetration of EV, and hence, operating microgrids and networked microgrids with rich EV is an important problem. In this paper, a framework using real-time price signals for the operations of electric vehicle (EV)-rich networked-microgrids with mixed ownership will be presented.

There are several works pursued on the operations of microgrids in electricity market. An optimal bidding strategy was proposed for a microgrid to engage in day-ahead electricity market [22]. In [23], a bidding model was developed for a microgrid to take part in day-ahead and real-time electricity markets considering microgrid reconfiguration and flexible energy sources under a hybrid stochastic and information gap decision theory (IGDT) method. A strategic bidding model was presented for a hybrid ACDC microgrid to participate in day-ahead and real-time markets with a chance-constrained two-stage stochastic programming approach [24]. A peer-to-peer bidding strategy was also introduced for energy transactions between networked microgrids, considering the uncertainties of renewable energy sources under cartel game [25]. Furthermore, a novel blockchain-based transactive model was developed for energy exchange between multiple microgrids [26]. Similarly, a distributed framework was developed to facilitate energy exchange between several NMs, wherein the each microgrid self-schedules internal generation units to satisfy domestic demand while sharing its surplus production with other microgrids [27].

In addition, electric vehicle charging stations (EVCS) in microgrids can be a crucial resource for cost-effective operation [28]. The power consumption of EVCS can be flexible by adjusting the EV charging schedule, with the objective of meeting the demand of EV owners before their departure [29]. Moreover, EVCS can contribute to the microgrid by discharging stored energy when electricity prices are high, thereby enhancing cost-effectiveness [30], [31]. While EVCS provide economic benefits similar to utility-scale batteries in microgrid operations, a key distinction is that EVCS must also consider the power consumption required to meet EV demand, which adds additional constraints compared to batteries. This highlights the need to develop effective (dis)charging scheduling strategies for EVCS that balance their contribution to both the grid and EV owners.

In this project, real-time price signal will be used for managing the operations of networked microgrids, in which the power balance in each microgrid is performed locally with the engagement of DERs, the load demand and the power injection from the EV charging stations. In particular, the real-time price signal from DSO will be sent to microgrid controllers and then distributed to EV charging stations within each microgrid. When all the microgrids belong to an owner, it is possible to control all these microgrids by a centralized controller [32]. However, in a mixed ownership environment where microgrids can belong to either utility or non-utility owner, and hence, not all microgrids can communicate with the DSO. Accordingly, a max consensus algorithm is utilized to propagate the real-time price signal from DSO to all microgrid controllers. Given the real- time price signal, EV charging stations can utilize different charging strategies to

charge and discharge the EVs to satisfy the EV demand. Eventually, the MG controller manages the power output of DERs to balance the load demand and the power injection from the EV charging stations. While the price signal can only used in a monthly basis in the current practice, the proposed framework utilizes the real-time price signal directly at the EV charging stations, which enables much faster response by the EV charging station to get benefits.

In this project, a price signal-based framework is introduced for the operations of networked microgrids in mixed ownership environment. Also, a max consensus algorithm is introduced to propagate the real-time price signal among microgrid controllers. Demonstration on the 123-node test feeder with 3 microgrids is provided to evaluate the social welfare (SW) of the NMGs under different charging strategies of the EV charging stations.

2.1 Communication architecture

Consider a number of microgrids Si,i = 1,...,N, that are operating in the grid-connected mode, each of which has one controller, as showed in Fig. 5. Each microgrid controller can collect information from devices in that microgrid and perform different controlling objectives. Each microgrid can contain generation resources, load, and/or EV charging station.

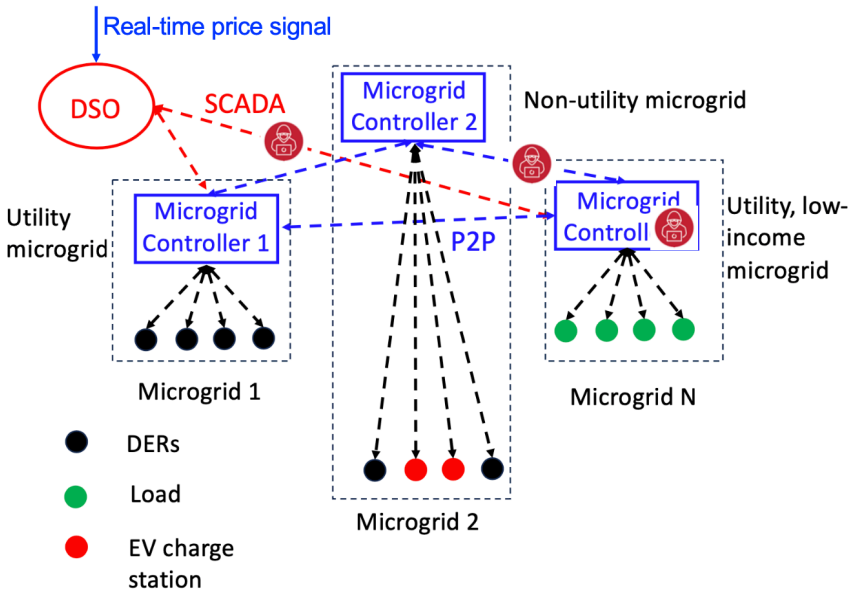

Fig. 5: Communication architecture to support the price signal-based operations of EV-rich networked microgrids with mixed ownership

In the operations of networked microgrids connected to the BPS, the following communication layers are typically available:

- Layer 1: Communication between microgrid con- troller and individual devices within a microgrid. The individual microgrid controller will directly get the information from and send control signal to individual devices which include generators, inverters, relays, and sensors.

- Layer 2: Peer-to-peer communication among micro- grid controllers. The individual microgrid controllers exchange information, but not control signals. Inter- actions at this layer could be a traditional mapped Supervisory Control and Data Acquisition (SCADA) approach. But for scalability and for coping with authority in a mixed-ownership environment, a peer-to-peer communication approach is more appropriate. In this paper, peer-to-peer communication among microgrid controllers will be applied.

- Layer 3: Communication between microgrid controllers and DSO. The utility's centralized DSO communicates with the microgrid controllers. In a mixed ownership environment, it is considered that DSO can only communicate with utility microgrid controllers, but cannot communicate with non-utility MG controllers.

2.2 Price signal-based framework for operating networked microgrids

Leveraging the communication architecture in the previous section, the following framework is utilized for using the real-time price signal in the operation of networked micro- grids with mixed ownership.

- Step 1: DSO gets the price from wholesale market in every 5 minute and sends to utility MG controllers using the SCADA network

- Step 2: The price signal is propagated from utility MG controllers to non-utility MG controllers via the P2P communication network among MG controllers

- Step 3: Charging station in each MG decides the charg- ing strategy based on the received price signal, while meeting the EV demand

- Step 4: Each MG controller manages the DERs within that MG to balance the supply-demand locally in the MG.

2.3 Propagation of real-time price signal via SCADA and P2P communication networks

When all the microgrids belong to an owner, it is possible to control all these microgrids by a centralized controller [15]. However, in a mixed ownership environment where microgrids can belong to either utility or non-utility owner, and hence, not all microgrids can communicate with the DSO. Using SCADA network the real-time price signal can be sent from DSO to utility MG controllers. Thanks to the P2P communication network among MG controllers, it is possible to propagate the real-time price signal from utility MG controllers to non-utility MG controllers.

Denote $\mathcal{N}_i$ as the set of MG controllers that can communicate with MG controllers i via the P2P communication network. Accordingly, the max consensus algorithm is utilized to propagate the real-time price signal from DSO to all microgrids controllers:

$$\lambda_{t,i}^{(m+1)} = \max_{j \in \{\mathcal{N}_i, i\}} \lambda_{t,j}^{(m)}, m = 0, 1, 2..$$

where $\lambda_{t,i}^{(m)}$ is the estimation of the real-time marginal price at the time period t by the MG i and updating step m of the consensus algorithm. Note that $\lambda_{t,i}^{(0)}$ is the real-time marginal price at the time period t received by the MG i if MG i is utility MG. $\lambda_{t,i}^{(0)}$ = 0 if MG i if MG i is non-utility MG. It should t,i be noted that if the P2P communication network among MG controllers is connected, then the max consensus algorithm quickly converges and all the MG controllers get the same value of the real-time marginal price at the time period t.

2.4 Operations of EV-rich Networked Microgrids

We consider a system of multiple microgrids (MGs) with DERs and EVCS resulting into a mixed ownership structure, as depicted in Fig. 6. In each microgrid k over time t, the load must be met at each time t with the interval Δt. To meet the load, DER generation can be utilized, which is controllable. Here, $Q_{t,k}(p_{t,k})$indicates the cumulative generation in descending order of bids $p_{t,k}$Additionally, the system includes EVCS, which can be considered as a set of EV batteries. The overall capacity is $r_{t,k}$, which changes by the amount of $D_{t,k}$and $A_{t,k}$, indicating the battery capacity of departed and arrived EVs at time t, respectively. The total charging power of EVCS from/ to the MG is denoted as $e_{t,k}$, which can be either positive or negative. If EVs are charged using power from DERs, $e_{t,k}$, is positive. Conversely, if EVCS contributes to satisfying the demand by using the power stored in the EV batteries, $e_{t,k}$, becomes negative.

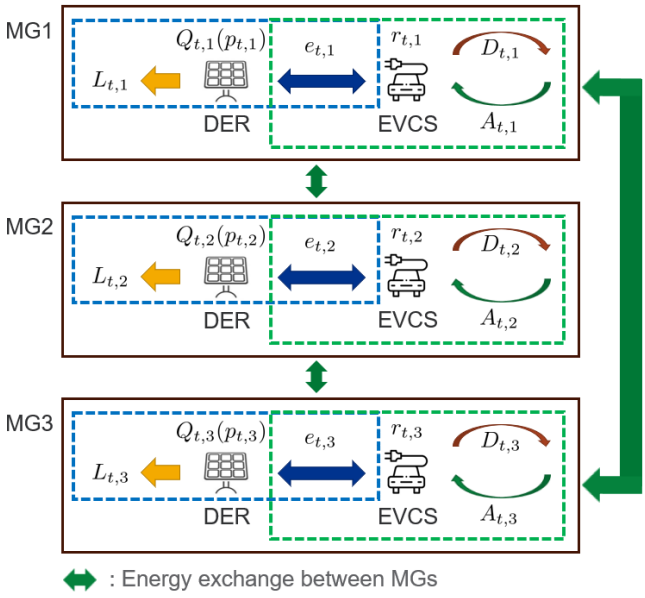

Fig. 6: System Description

Specifically, the power balance must be maintained at each time t, i.e.,

$$\sum_{k \in \mathcal{K}} \left[Q_{t,k}(p_{t,k}) - L_{t,k} - e_{t,k} \right] = 0,$$

along with the minimum/maximum boundaries of the DER generations for each MG k. Moreover, the participation of EVCS introduces additional constraints to the problem:

$$
\begin{aligned}
r_{t,k} &= r_{t-1,k} + e_{t,k}\Delta t + A_{t,k} - D_{t,k}, \\
R_{t,k}^{\min} &\le r_{t,k} \le R_{t,k}^{\max}, \\
R_{t,k}^{\min} &= R_{t-1,k}^{\min} + A_{t,k} - D_{t,k}, \\
R_{t,k}^{\max} &= r_{t-1,k} + A_{t,k} - D_{t,k} + \Delta R_k.
\end{aligned}
$$

Here, the first equation indicates the changes in the aggregated capacity of the EV batteries in MG k at time t. The capacity $r_{t-1,k}$ changes by the charging or discharging energy $e_{t,k}\Delta$t, and the aggregated battery capacity of arriving and departing EVs $A_{t,k}$ and $D_{t,k}$, respectively. Consequently, $r_{t,k}$ is bounded by $R_{t,k}^{min}$ and $R_{t,k}^{max}$. Here, $R_{t,k}^{min}$ represents the minimum EVCS capacity needed to satisfy the overall EV demand, ensuring that all EVs can depart with their demand met. The maximum $R_{t,k}^{max}$ implies the maximum charging limit of EVCS in MG k.

Note that $A_{t,k}$ and $D_{t,k}$ can be considered random variables. In our numerical experimentation, we utilized a uniform distribution followed by scaling with time-dependent arrival/departure ratios. Here, $R_{t,k}^{min}$ is determined based on the estimated values of $A_{t,k}$ and $D_{t,k}$.

2.5 EVCS Operation Strategy

the demand L is constant at each time t, which leaves the term $\sum_{k\in\mathcal{K}} Q_{t,k}(p_{t,k}) - e_{t,k}$ constant. This implies that we can reduce the cumulative generation by reducing the EV charging power when the marginal price is high. This helps in reducing the generation cost. Moreover, we can even set $e_{t,k}$ to be negative, implying discharging power from the EV batteries if the EVs already have enough charge. This will help reduce the generation cost dramatically and increase the total SW.

Based on this observation, we consider three EV charging strategies: *Strategies 'Min', 'Max',* and *'Flex'*:

- *Strategy 'Min'*: We charge as little as possible while satisfying the EVCS constraints. As a result, $e_{t,k}$ can be represented as

$$e_{t,k} = \min(\max(R_{t-1,k}^{\min} - r_{t-1,k}, \Delta R_k^{\min}), \Delta R_k)/\Delta t$$

- *Strategy 'Max'*: Contrary to *Strategy 'Min'*, we charge as much as possible while satisfying the EVCS constraints. Consequently, $e_{t,k} = \Delta R_k/\Delta$t by following (8).

- *Strategy 'Flex'*: This strategy is flexible between charging maximum and minimum based on the marginal price while satisfying EVCS constraints. Once the price threshold is determined, we will charge to the maximum if the marginal price is less than this thresthold. Otherwise, we charge to the minimum or even discharge, which can be represented as

$$
\begin{aligned}
e_{t,k} = &\min(\max(Q_t^{\min} - L_{t,k}, -\Delta R_k, R_{t-1,k}^{\min} - r_{t-1,k}) \\
&, \Delta R_k)/\Delta t.
\end{aligned}
$$

2.6 Evaluation Metrics

To evaluate the operations of networked microgrids when the EV charging stations use different charging strategies, the social welfare (SW) of the system will be analyzed and compared. Here, the SW is defined as

$$\mathrm{SW} = \sum_{t\in\mathcal{T}} \sum_{k\in\mathcal{K}} [U_{t,k}(L_{t,k}) + W_{t,k}(e_{t,k}) - C_k(Q_{t,k}(p_{t,k}))]$$

with $U_{t,k}$ and $W_{t,k}$ indicate the SW of the customer represented as load demand and EV charging, and C($Q_{t,k}(p_{t,k})$) represents the generation cost

$$U_{t,k}(L_{t,k}) = \theta_{t,k} \log(1 + L_{t,k})$$

$$W_{t,k}(e_{t,k}) = \begin{cases} \phi_{t,k} \log(1 + e_{t,k}) & \text{if } e_{t,k} \geq 0, \\ a_{t,k}\{\mathrm{sign}(e_{t,k})\}(e_{t,k})^2 + b_{t,k} e_{t,k} \end{cases}$$

$$C(Q_{t,k}(p_{t,k})) = \lambda_{t,k} Q_{t,k}(p_{t,k}),$$

2.7 Demonstration

To show the effectiveness of the proposed method, we conducted a numerical test on a simple three-microgrid system as in Fig. 6 based on IEEE 123-bus feeder [33]. We considered a time horizon of one day with EVCS participating in the real-time market, which leads us to consider a total of 288- time slots with 5-minute intervals. To simplify the problem, we assume that the price signal and the total load of each MG are given as shown in Fig. 9, based on adjusted ERCOT data [34].

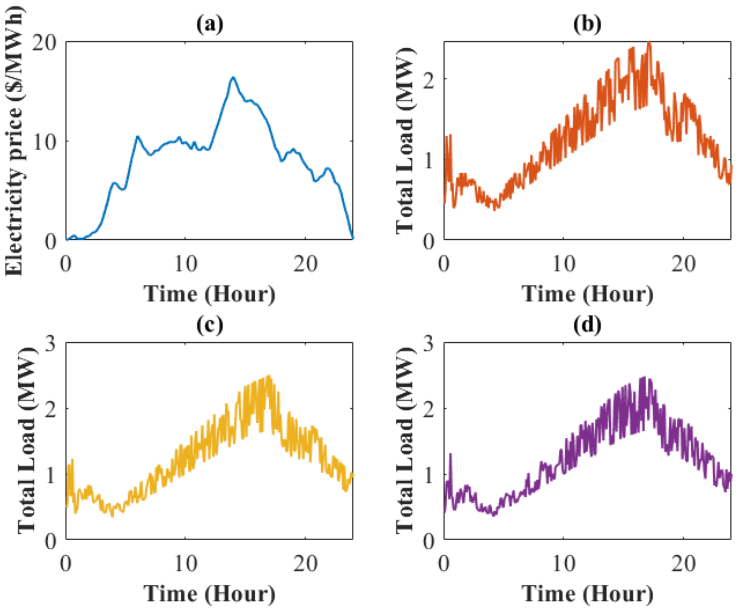

Fig. 9: (a) Electricity price and a total load of (b) MG1, (c) MG2 and (d) MG3 in one day

In the scenario without an attack on the price signal, we assume that all MGs have accurate knowledge of the price. Lastly, R^{min}, D, and A are depicted in Fig. 10, considering the trend that EV departure and arrival occur most frequently during the afternoon, with the minimum capacity requirement R meeting the EV charging demand. Here, the number of arriving EVs at the EVCS is greater than the number of departing EVs in hour 12, causing the A to be bigger than D and in turn raises the minimum capacity requirement R^{min}. Conversely, after hour 12, more EVs depart than arrive, leading to a decrease in R^{min} value with D being bigger than A.

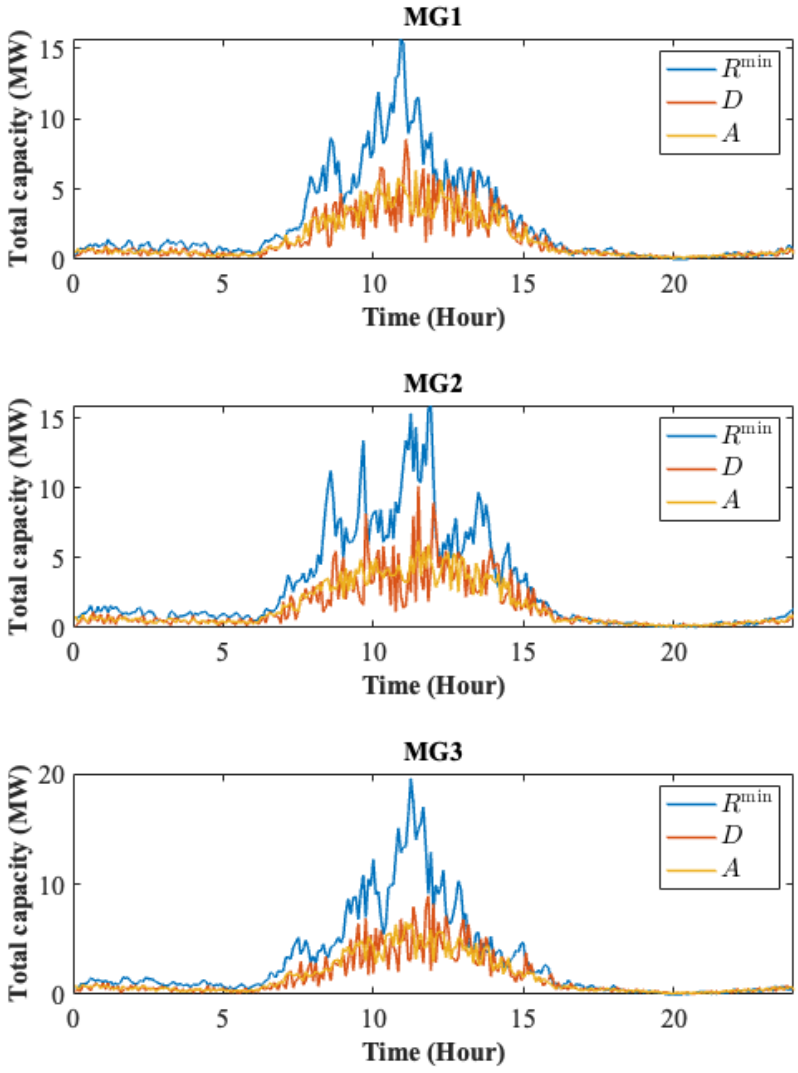

Fig. 10: Minimum required EVCS charging capacity (Rmin), capacity of EV arrival (A) and EV departure (D) of three MGs in one day

As we discussed, three strategies have been considered: *'Min', 'Max',* and *'Flex'*. In the *Flex* strategy, the price threshold is set at 1.15 times the average marginal price over one day. The numerical results using these three strategies are shown in Table IV. We observe that *Flex* shows the best total SW compared to the other two strategies.

	Min	Max	Flex
Total SW ($)	20356	21390	22188
Load SW ($)	46866	46866	46866
Generation cost ($)	28394	29779	27494
EV SW ($)	1883	4303	2817

TABLE IV: Numerical test comparisons between three strategies

This improvement in SW is due to better SW for EVs than *Min* and *Max*, while also reducing generation costs compared to other strategies. The *Flex* strategy leverages the flexibility of EVs to adapt to electricity prices. Specifically, when electricity prices are high, EVs discharge to the maximum extent possible without causing an EV charging shortfall, similar to *Min*. Conversely, when electricity prices are low, EVs charge to the maximum, similar to *Max*. This behavior is reflected in Fig. 11, where the total capacity for *Flex* is between those of the other two strategies. Initially, *Flex* follows *Max* due to low electricity prices, but as prices increase, the charging/discharging strategy shifts closer to *Min*, reducing the total capacity. These differences are also visible in Fig. 12, which shows the EVCS charging/discharging power over each time period for the three strategies. *Min* maintains a steady minimum charge that can prevent EV charging shortfalls. *Max* charges significantly more than *Min* to maximize the charge at each interval, but it does not utilize the flexibility of EV charging, resulting in constant power charges at each time. In contrast, *Flex* leverages EV flexibility and frequently adjusts charging/discharging to enhance SW. Unlike *Max*, *Flex* alternates between charging and discharging, resulting in higher SW. Note that although there are frequent fluctuations in EV charging/discharging in *Flex*, there would be no degradation issues with the EV batteries because the time interval is 15 minutes.

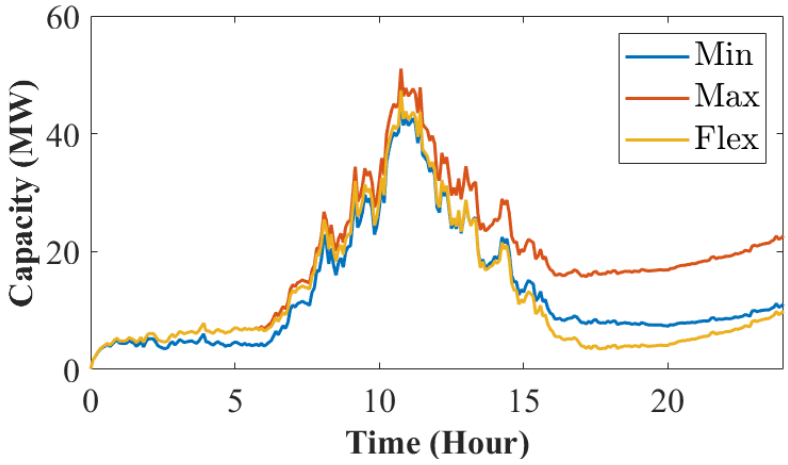

Fig. 11. Comparison of total EV capacity between three strategies

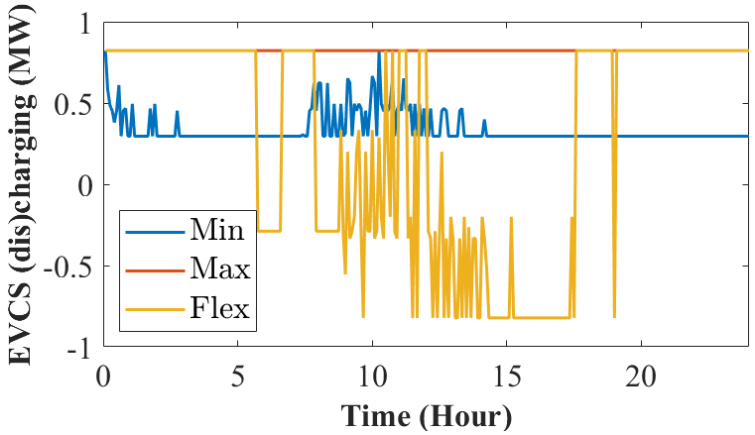

Fig. 12: Comparison of total EV capacity between three strategies

Finally, we consider the scenario where an attack occurs on the price signal. Specifically, we assume that MG1 is a utility MG, while MG2 and MG3 are non- utility MGs. In this setup, MG1 directly receives the real-time price signal from the DSO, while the other two MGs estimate the price signal using a consensus algorithm. We assume that MG2 estimates the price based on information shared by MG1, and MG3 estimates the price based on information shared by MG2. During this estimation process, an attack is assumed to reduce the price, leading to the MGs underestimating the price. Fig. 10 shows an example of the (estimated) price signals for each MG under attack.

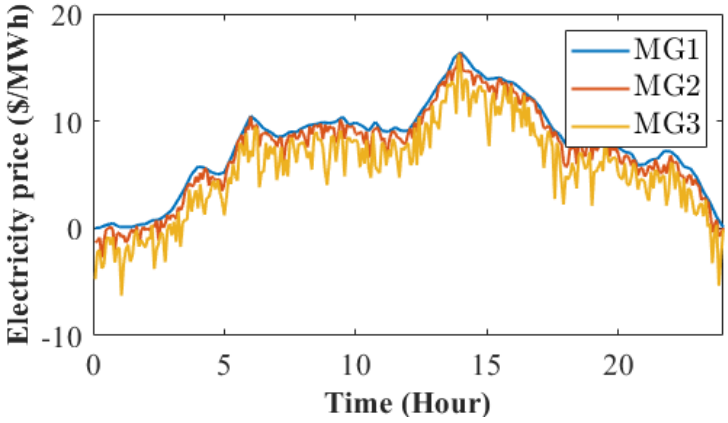

Fig. 13: (Estimated) price signals for each MG under attack

Similar to the previous sections, we compare the EV charging strategies *Flex* and *'FlexAtt'*. Here, *FlexAtt* uses the estimated price signals shown in Fig. 13, assuming that an attack exists. This differs from *Flex*, which assumes no attack and perfect price signal estimation by all MGs.

Table V compares the total SW, load SW, generation cost, and EV SW between *Flex* and *FlexAtt*. As we can see, the attack causes MG2 and MG3 to have less accurate price estimates, leading to a decrease in the total SW. Here, we emphasize the impact of the attack, which degrades both load SW and EV SW while increasing the generation cost. This implies that the attack undermines the economic efficiency of the system and prevents the agent from determining the proper actions for each circumstance. Notably, despite the attack, the total SW is still better than the *Min* and *Max* strategies shown in Table IV, demonstrating the effectiveness of the *Flex* strategy.

	Flex	FlexAtt
Total SW ($)	22188	21172
Load SW ($)	46866	46866
Generation cost ($)	27494	27899
EV SW ($)	2817	2205

TABLE V: Numerical comparison between *'Flex'* and *'FlexAtt'*

Next, Fig. 14 compares the total EV capacity between *Flex* and *FlexAtt*. Consistent with the previous results, the attack and the resulting inaccurate price estimations lead to a slight decrease in total EV capacity. This is closely related to the EVCS (dis)charging patterns, which are shown in Fig. 15. As seen in the figure, *FlexAtt* underestimates the price due to the attack, thereby reducing discharging, as indicated by the values below zero in the plot. Consequently, the flexibility of EVs is not fully utilized, leading to a decrease in both EV SW and total SW. Nevertheless, the results still show that the *Flex* strategy is more effective compared to others even in the presence of an attack, implying the robustness of our proposed strategy.

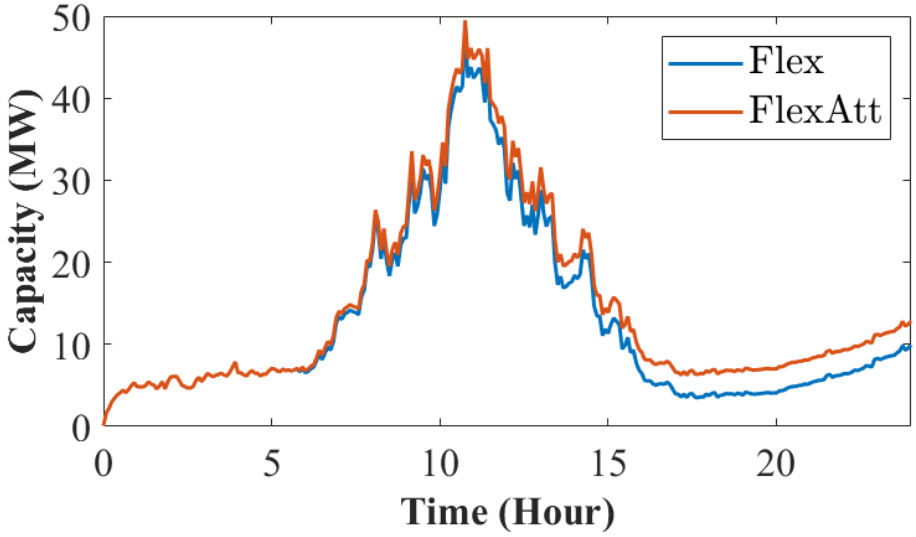

Fig. 14: Comparison of total EV capacity between *Flex* and *FlexAtt*.

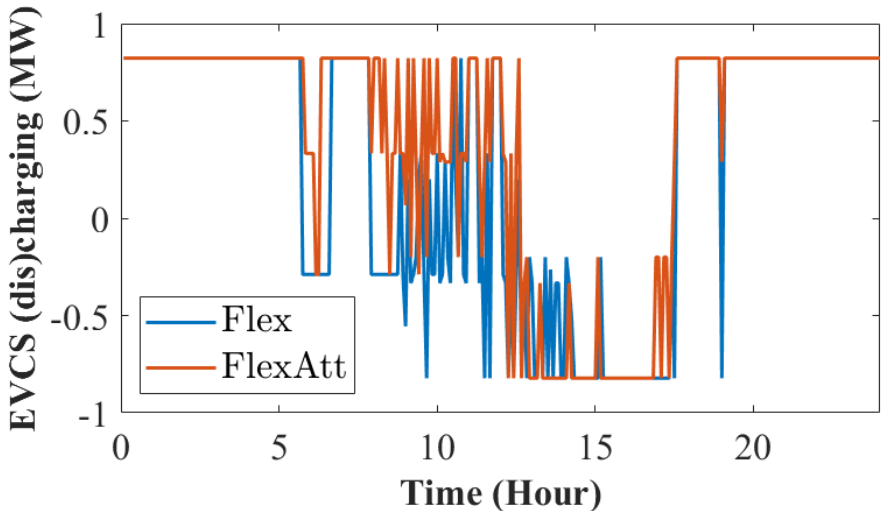

Fig. 15: Comparison of EVCS (dis)charging for the three MGs between *Flex* and *FlexAtt*.

3.0 References

[1] R. Lasseter, “Microgrids,” in *2002 IEEE Power Engineering Soci- ety Winter Meeting. Conference Proceedings (Cat. No.02CH37309)*, vol. 1, 2002, pp. 305–308 vol.1.

[2] Z. Li, M. Shahidehpour, F. Aminifar, A. Alabdulwahab, and Y. Al- Turki, “Networked microgrids for enhancing the power system re- silience,” *Proc. IEEE*, vol. 105, no. 7, pp. 1289–1310, 2017.

[3] K. P. Schneider, F. K. Tuffner, M. A. Elizondo, C.-C. Liu, Y. Xu, and D. Ton, “Evaluating the feasibility to use microgrids as a resiliency resource,” *IEEE Trans. Smart Grid*, vol. 8, no. 2, pp. 687–696, 2017.

[4] K. P. Schneider, J. Glass, C. Klauber, B. Ollis, M. J. Reno, M. Burck, L. Muhidin, A. Dubey, W. Du, L. Vu, J. Xie, D. Nordy, W. Dawson, J. Hernandez-Alvidrez, A. Bose, D. Ton, and G. Yuan, “A framework for coordinated self-assembly of networked microgrids using consen- sus algorithms,” *IEEE Access*, vol. 10, pp. 3864–3878, 2022.

[5] T. L. Vu, L. Marinovici, K. Schneider, J. Xie, C. Klauber, and A. Dubey, “Coordination of networked microgrids for supporting voltages of bulk power systems,” in *2023 IEEE Power Energy Society General Meeting (PESGM)*, 2023, pp. 1–5.

[6] N. Gray, R. Sadnan, A. Bose, A. Dubey, T. L. Vu, J. Xie, L. D. Marinovici, K. P. Schneider, C. Klauber, and W. Trinh, “Distributed coordination of networked microgrids for voltage support in bulk power grids,” *IEEE Transactions on Industry Applications*, pp. 1–11, 2024.

[7] M.S.Chong,H.Sandberg,andA.M.Teixeira,“Atutorialintroduction to security and privacy for cyber-physical systems,” in *2019 18th European Control Conference (ECC)*. IEEE, 2019, pp. 968–978.

[8] Y. Yuan, Q. Zhu, F. Sun, Q. Wang, and T. Bas ̧ar, “Resilient control of cyber-physical systems against denial-of-service attacks,” in *2013 6th International Symposium on Resilient Control Systems (ISRCS)*. IEEE, 2013, pp. 54–59.

[9] C.-Z. Bai, F. Pasqualetti, and V. Gupta, “Data-injection attacks in stochastic control systems: Detectability and performance tradeoffs,” *Automatica*, vol. 82, pp. 251–260, 2017.

[10] M. Zhu and S. Martinez, “On the performance analysis of resilient networked control systems under replay attacks,” IEEE Transactions on Automatic Control, vol. 59, no. 3, pp. 804–808, 2013.

[11] A. Barboni, H. Rezaee, F. Boem, and T. Parisini, “Detection of covert cyber-attacks in interconnected systems: A distributed model-based approach,” IEEE Transactions on Automatic Control, 2020.

[12] E. Mousavinejad, F. Yang, Q.-L. Han, and L. Vlacic, “A novel cyber attack detection method in networked control systems,” IEEE transactions on cybernetics, vol. 48, no. 11, pp. 3254–3264, 2018.

[13] B. Satchidanandan and P. R. Kumar, “Dynamic watermarking: Active defense of networked cyber–physical systems,” Proceedings of the IEEE, vol. 105, no. 2, pp. 219–240, 2016.

[14] C.SchellenbergerandP.Zhang,“Detectionofcovertattacksoncyber- physical systems by extending the system dynamics with an auxiliary system,” in 2017 IEEE 56th Annual Conference on Decision and Control (CDC). IEEE, 2017, pp. 1374–1379.

[15] P.Griffioen,S.Weerakkody,andB.Sinopoli,“Amovingtargetdefense for securing cyber-physical systems,” IEEE Transactions on Automatic Control, 2020.

[16] M. Starke, B. Xiao, G. Liu, B. Ollis, P. Irminger, D. King, A. Herron, and Y. Xue, “Architecture and implementation of microgrid controller,” in 2016 IEEE Power & Energy Society Innovative Smart Grid Tech- nologies Conference (ISGT), 2016, pp. 1–5.

[17] T. L. Vu, S. Mukherjee and V. Adetola, "Resilient Communication Scheme for Distributed Decision of Interconnecting Networks of Microgrids," *2023 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, Washington, DC, USA, 2023, pp. 1-5, doi: 10.1109/ISGT51731.2023.10066341.

[18] S.RiazandP.Mancarella,“Modellingandcharacterisationofflexibil- ity from distributed energy resources,” *IEEE Transactions on Power Systems*, vol. 37, no. 1, pp. 38–50, 2022.

[19] M.vanderKamandR.Bekkers,“Mobilityinthesmartgrid:Roaming protocols for ev charging,” *IEEE Transactions on Smart Grid*, vol. 14, no. 1, pp. 810–822, 2023.

[20] Mullen USA, “The U.S. Electric Vehicle Market: Exploring Ownership,” https://news.mullenusa.com/the-u.s.-electric-vehicle- market-exploring-ownership, 2024, accessed: 2024-09-23.

[21] The New York Times, “Electric vehicle fleet turnover,” https://www.nytimes.com/interactive/2021/03/10/climate/electric- vehicle-fleet-turnover.html, 2021, accessed: 2024-09-23.

[22] G. Liu, Y. Xu, and K. Tomsovic, “Bidding strategy for microgrid in day-ahead market based on hybrid stochastic/robust optimization,” *IEEE Transactions on Smart Grid*, vol. 7, no. 1, pp. 227–237, 2016.

[23] M. A. Mirzaei, M. Hemmati, K. Zare, M. Abapour, B. Mohammadi-Ivatloo, M. Marzband, and A. Anvari-Moghaddam, “A novel hybrid two-stage framework for flexible bidding strategy of reconfigurable micro-grid in day-ahead and real- time markets,” *International Journal of Electrical Power and Energy Systems*, vol. 123, p. 106293, 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0142061520302052

[24] T. Zhao, X. Pan, S. Yao, C. Ju, and L. Li, “Strategic bidding of hybrid ac/dc microgrid embedded energy hubs: A two-stage chance constrained stochastic programming approach,” *IEEE Transactions on Sustainable Energy*, vol. 11, no. 1, pp. 116–125, 2020.

[25] L. Wang, Y. Zhang, W. Song, and Q. Li, “Stochastic cooperative bidding strategy for multiple microgrids with peer-to-peer energy trading,” *IEEE Transactions on Industrial Informatics*, vol. 18, no. 3, pp. 1447–1457, 2022.

[26] M. R. Hamouda, M. E. Nassar, and M. M. A. Salama, “Centralized blockchain-based energy trading platform for interconnected micro- grids,” *IEEE Access*, vol. 9, pp. 95 539–95 550, 2021.

[27] H. Wang and J. Huang, “Incentivizing energy trading for intercon- nected microgrids,” *IEEE Transactions on Smart Grid*, vol. 9, no. 4, pp. 2647–2657, 2018.

[28] M. A. Beyazıt, A. Tas ̧cıkaraog ̆lu, and J. P. Catala ̃o, “Cost optimization of a microgrid considering vehicle-to-grid technology and demand response,” *Sustainable Energy, Grids and Networks*, vol. 32, p. 100924, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2352467722001692

[29] K.-b. Kwon and H. Zhu, “Efficient representation for electric vehicle charging station operations using reinforcement learning,” in *Pro- ceedings of the Hawaii International Conference on System Sciences*. ScholarSpace, 2022.

[30] H. Yue, Q. Zhang, X. Zeng, W. Huang, L. Zhang, and J. Wang, “Optimal scheduling strategy of electric vehicle cluster based on index evaluation system,” *IEEE Transactions on Industry Applications*, vol. 59, no. 1, pp. 1212–1221, 2023.

[31] J. Zhong, X. Lei, Z. Shao, and L. Jian, “A reliable evaluation metric for electrical load forecasts in v2g scheduling considering statistical features of ev charging,” IEEE Transactions on Smart Grid, vol. 15, no. 5, pp. 4917–4931, 2024.

[32] Z. Li, M. Shahidehpour, F. Aminifar, A. Alabdulwahab, and Y. Al- Turki, “Networked microgrids for enhancing the power system re- silience,” Proceedings of the IEEE, vol. 105, no. 7, pp. 1289–1310, 2017.

[33] Y. Dong, “Ieee 123 bus system,” 2022. [Online]. Available: https://dx.doi.org/10.21227/j0fm-5d70

[34] ElectricReliabilityCouncilofTexas(ERCOT),“Ercotmarketprices,” Available: https://www.ercot.com/mktinfo/prices, Accessed: Septem- ber 16, 2024.

Pacific Northwest National Laboratory

902 Battelle Boulevard
P.O. Box 999
Richland, WA 99354

1-888-375-PNNL (7665)

www.pnnl.gov