By Robert Mieth, Samrat Acharya, Ali Hassan, and Yury Dvorkin

Learning-Enabled Residential Demand Response

Automation and security of cyberphysical demand response systems.

RESIDENTIAL DEMAND RESPONSE (DR) PROgrams have been validated as a viable technology to improve energy efficiency and the reliability of electric power distribution. However, various technical and organizational challenges hinder their full techno-economic potential. In practice, these challenges are related to the small-scale, distributed, heterogeneous, and stochastic nature of residential DR resources. This article investigates state-of-the-art online and reinforcement learning methods that are capable of overcoming these challenges in the context of DR pricing, scheduling, and cybersecurity.

Digital Object Identifier 10.1109/MELE.2020.3047470
Date of current version: 4 March 2021

2325-5897/21©2021IEEE

The Case of Residential DR

Distribution grids are undergoing a rapid overhaul due to the massive deployment and expansion of distributed energy resources (DERs), e.g., photovoltaic arrays, energy storage units, electric vehicles (EVs), cogeneration plants, and microgrids. The main factors fueling this expansion are significant decreases in the capital costs of DER technologies and incentives for DER installations offered by local electric power utilities as well as by state and federal authorities. For example, the state of California aims to reduce greenhouse gas emissions (GHG) by 40% below its 1990 levels in 2030 by means of increasing the share of electricity produced by renewable generation to 50%, doubling energy efficiency targets, and encouraging transportation electrification. Similarly, the state of New York set a target of having a zero-carbon power sector by 2040 and has a goal of reducing the 1990 levels of GHG emissions by 85% in 2050.

Distribution grids are undergoing a rapid overhaul due to the massive deployment and expansion of distributed energy resources.

However, the rollout of DERs in distribution grids also imposes additional operational challenges, e.g., bidirectional power flows, voltage fluctuations, and, as a result, additional wear-and-tear on electric power equipment. Dealing with such challenges is crucial to ensuring economic and reliable distribution grid operations and necessitates more flexibility. DR is a technology that can provide this additional flexibility by organizing adaptable residential, industrial, and commercial loads to provide a broad range of distribution-level ancillary services (e.g., energy arbitrage, peak shaving, balancing regulation, congestion relief, capacity deferral, and voltage support). The U.S. Federal Energy Regulatory Commission reports continuously increasing DR participation rates in wholesale electricity markets, with the growth of 8% from 2017 to 2018 and the total capacity of 29,674 MW. However, as the result of their wholesale focus, established DR programs mainly target commercial and industrial loads that are relatively homogeneous in size and technical capabilities. Thus, they provide economy-of-scale benefits, which in turn allow for intuitive pricing and standardized interfacing with energy-managements systems used by utilities.

On the contrary, residential-scale DR resources may have a significant potential of providing system-beneficial services, but they are challenging to employ in DR programs due to their heterogeneous characteristics and electricity usage patterns and preferences. For example, in 2018, New York City's Consolidated Edison (ConEd) launched the SmartAC program that allowed for a reduction of the power consumption of residential air-conditioners (ACs) during peak hours in exchange for retail gift cards. This program used a custom Internet of Things (IoT) device with a smartphone app to deliver control signals to participating AC units and provide an opportunity for DR customers to override this signal. However, despite its initial success, the SmartAC program was discontinued in 2020 for officially undisclosed reasons. Public materials indicate that the reasons may include overly intrusive control actions, unreliable IoT devices and smartphone apps from third-party providers, and gaming opportunities to receive incentive payments without providing any effective load reduction.

This article discusses current residential DR systems in the context of the existing infrastructure and their realistically envisioned future development. The ongoing massive rollout of smart meters (SMs) and the recent advances in (open source) communication protocols tailored toward DR systems pave a way to aggregating residential DR resources into more efficient and more homogeneous controllable ensembles. Emerging data mining and machine learning (ML) techniques further support the decision-making processes of the utility or third-party aggregators to determine optimal DR incentive schemes and to control actions that trade off between the utility and DR customer perspectives. At the same time, while novel ML approaches can reduce data and communication requirements, coupling power system operation with a broad spectrum of new communication and control infrastructure requires a critical cybersecurity assessment.

The Cyberphysical DR System

With advances in communication technologies and artificial intelligence, power utilities and third-party aggregators have been increasingly automating DR routines. This automation extends the cyberspace of electricity consumers and connects it with the cyberspace of the utility. This section provides an overview of cyberphysical nexus among customers, third-party aggregators, and utilities.

The DR Process

Figure 1 summarizes a typical architecture of U.S. residential DR programs. Power utilities communicate with DR resources, such as thermostatically controlled loads (TCLs) and EVs, either directly or via third-party aggregators. In either mechanism, the utility employs a DR automated server (DRAS), which functions in three stages:

1) *Data acquisition stage*: In this stage, the server acquires the operation schedules of the ISO market, captured by a centralized SCADA system via wide-area network (WAN) technologies, e.g., cellular networks or power line communication. Furthermore, the server acquires the real-time energy usage of DR resources logged by distributed SMs via WAN technologies, e.g., WiMAX and cellular networks.
2) *DR scheduling stage*: In this stage, the server determines the time, duration, and incentives to procure a

needed amount of DR, based on the acquired data from the ISO and DR resources. With advances in artificial intelligence technologies, power grid utilities and aggregators have started employing ML techniques to schedule DR. For example, there are more than 20 aggregators in California that use artificial intelligence techniques to optimize their DR profit. After scheduling the DR, the server broadcasts the DR incentives and schedules to the customers enrolled in the DR program via user interfaces, such as smartphone applications and in-home BEMS. In turn, the customers accept (opt-in) or reject (opt-out) the offered DR schedules and send their selected choices back to the DRAS. Customers can make their opt-in/out decision either automatically, using BEMS, or manually, via smartphone applications.

3) *DR monitoring and control stage:* Once the DR schedule is accepted by the customers, the DRAS monitors and controls the operation of the participating DR resources. Notably, due to the remote control features of IoT enabled by smart home appliances, e.g., Alexa, Google Nest, EVs, and HVAC loads, the customers can disengage its DR resources at any time, even during the DR event.

Aggregation

An important component of an effective residential DR program is aggregation. Aggregating individual residential DR resources based on their physical (location, type of appliance) or organizational (incentive scheme, timing) attributes as well as tuning necessary DR infrastructure makes it possible to design DR ensembles that allow for taking advantage of both the economy of scope and the economy of scale. Additionally, aggregation can be offered to the utility as a service from third-party providers, thus reducing utility-side organizational overhead and exposure to technical and financial risks. In turn, aggregators can either aggregate customers to facilitate communication with the DRAS or to schedule, monitor, and control the DR resources by means of their own DRAS server, thus replacing the utility-end DRAS server. Therefore, we present utility- and aggregator-end DRAS at the same level in the control hierarchy of Figure 1.

However, the aggregators may not employ the same communication protocol as the utility-end DRAS. For instance, most utilities communicate with DR resources or aggregators via the OpenADR 2.0 specification, whereas the aggregators may use proprietary communication protocols to communicate with DR resources. The OpenADR 2.0 communication protocol is a nonproprietary, open-standard information exchange model for DR applications, recently recognized as the International Electrotechnical Commission Standard 62746-10-1 for the interface between DR participants and a utility or aggregator. In the model, the utility DRAS is a virtual top node (VTN), the aggregator DRAS is a VTN or a virtual end node (VEN), and DR participants are VENs. The VTN schedules DR and broadcasts the schedules to VEN via an encrypted and digitally certified channel. In turn, VENs respond to the DR schedules sent by VTN and send back their response via the same communication channel.

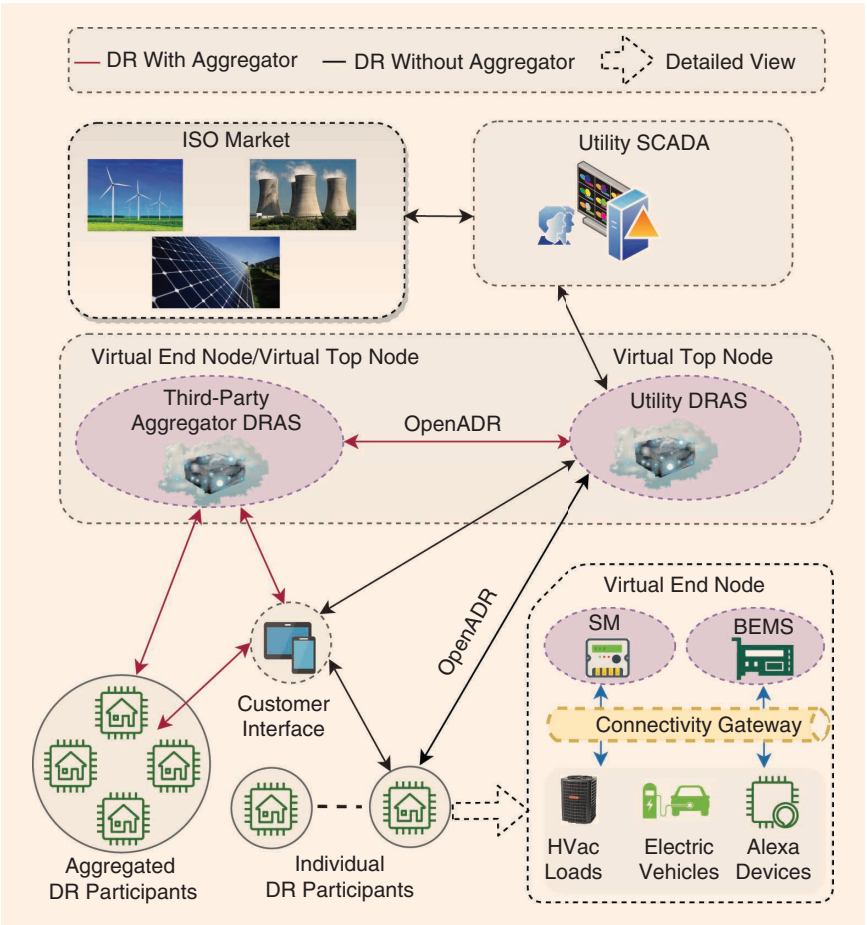

Figure 1. A schematic representation of a typical residential DR program. DRAS: DR automated server; SCADA: supervisory control and data acquisition; ISO: independent system operator; BEMS: building energy-management system; HVAC: heating, ventilation, and air-conditioning; ADR: automated DR.

Challenges

As residential DR programs gradually become more widespread, there are several common challenges and obstacles associated with them. Figure 2 summarizes the challenges discussed next:

- *Small-scale*: An individual contribution of residential-scale loads is determined by typically low-wattage consumer appliances, with EVs being a notable exception. As a result, effective DR programs require a large number of enrolled DR participants. This, however, implies that any profits from deploying DR resources must also be shared among a large number of participants. This profit, partially distributed in the form of monetary incentives, might not be sufficient to engage and retain DR participants. However, some nonfinancial incentives, e.g., an awareness of environmental impacts and the potential to mitigate climate change, may convince more customers to enroll in DR programs.
- *Distributed connectivity*: Distributed DR participants have various means of connectivity (e.g., cellular network, Wi-Fi, and Bluetooth) and levels of cyberhygiene. This diversity in cyberawareness incurs dealing with both the explored and novel (zero-day) vulnerabilities. Furthermore, due to the distributed nature of DR customers, utilities may need to uneconomically expand their infrastructure and scope to capture a small DR flexibility.
- *Stochasticity*: Residential DR is subject to systemic and behavioral uncertainty. First, residential DR participants are not obliged to follow DR call signals. Even if the operator is able to directly control appliances, customers are always able to manually interfere and override the DR control signals. Additionally, even if some preferences have been communicated or even somehow committed, some aspects of real-time preferences might be unknown to DR participants themselves due to limited rationality and changing environmental circumstances (e.g., weather).
- *Heterogeneity*: Residential DR participants are heterogeneous in nature, with unique load profiles and different preferences and behaviors that complicate the implementation and standardization of residential DR programs.

Learning Optimal DR Decisions

The goal of the DR program is to produce DR control or incentive signals to achieve a desirable change in the observed system demand. The ability to meet this goal depends on three attributes that characterize each DR resource but are not exactly known to the DR operator:

- *Available capacity*: Commit and dispatch DR resources with respect to their spatio-temporal restrictions and for particular applications, e.g., peak-load shaving, mitigation of intermittent injections from wind and solar, or other ancillary services.
- *Cost*: Determine the short- and long-term costs of dispatching and enrolling DR resources, respectively, and weigh them against other dispatchable resources available to the system.
- *Reliability*: Evaluate the projected real-time effectiveness of the scheduled DR dispatch decisions and account for uncertainty caused by the random, intentional or unintentional, interference of DR customers.

The available DR capacity depends on the physical characteristics of DR resources and the individual preferences of their users. For example, the DR participation of an EV requires the DR operator to know or estimate its state of charge, the desirable time of readiness, and battery-specific characteristics (e.g., degradation curves and charging history). Similarly, the thermal inertia of cooling and heating systems can be exploited to temporally shift power-consumption patterns. However, estimating the kW-capacity that can be extracted from this thermal inertia requires information about the technical characteristics of these systems and the temperature preferences of their users. While some system settings can be obtained using a two-way communication infrastructure and digitized appliance interfaces, individual preferences or comfort zones are rarely observable. Furthermore, acquiring, processing, and storing behavioral data involves effort for both the DR operator and participants, which may outweigh the benefits of the DR program.

DR participants expect some remuneration in return for their participation in DR programs as a compensation for lost utility due to the need to depart from their regular consumption patterns during DR events and also as an incentive to purchase new controllable appliances or necessary periphery. Therefore, DR operators aim to establish a remuneration scheme that incentivizes sufficient DR enrollment and systematic participation. At the same time, the overall cost of the total remuneration must be kept at a reasonable level to ensure a long-term profitability of the DR program.

The reliability of real-time DR deployments depends on the accuracy of DR capacity estimates and the sufficiency of the offered incentives. Scheduled load reductions may be insufficient if the called appliances are not operated as estimated, they fail to communicate with the DRAS, or DR participants suddenly opt out from the DR event. Such uncertain behaviors are difficult to predict ahead of time, which can reduce the effectiveness of DR programs.

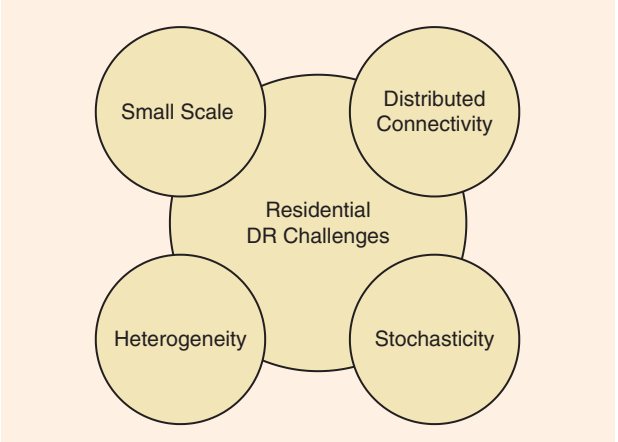

Figure 2. The challenges of residential DR programs.

Virtual DR Resource

Summarizing the characteristics of available DR resources as a virtual DR resource model that describes a functional relationship among capacity, cost, and reliability allows the DR operator to optimize scheduling decisions without two-way communication between DR participants and the DRAS server. Instead of establishing infrastructure to enable real-time negotiations or auctions, which is prohibitively expensive and obstructed by low customer engagement as well as by data security and privacy considerations, scheduling and incentive decisions should be derived locally without immediate customer feedback and then broadcasted as passive one-way signals. Here, as outlined in Figure 1, DR operators must rely on partial information available through SMs, SCADA, and limited app- or message-based customer interactions that comply with relevant cybersecurity requirements. From this information, the DR operator must identify or estimate DR resource characteristics and compile virtual ensembles of these resources that can be described in terms of abstract model formulations. As a result, data mining and ML methods play a pivotal role in the construction of decision-support tools that enable DR operators to efficiently maintain a reliable pool of DR resources.

Figure 3 outlines the process to design a virtual DR resource model that can be used to plan a residential DR program and inform DR scheduling and incentive decisions. A data mining process collects the available data from customer SMs and SCADA and external information, such as weather, temperature, day of the week, and holidays. Notably, the set of available measurements may be imperfect or incomplete, and the resulting data uncertainty must be accounted for. Using the processed data and additional historical data sets, suitable ML algorithms can estimate the available aggregated DR capacity, cost, and reliability, while abstracting attributes of individual DR resources and computing schedules and incentive signals that are optimal for an objective of the DR operator.

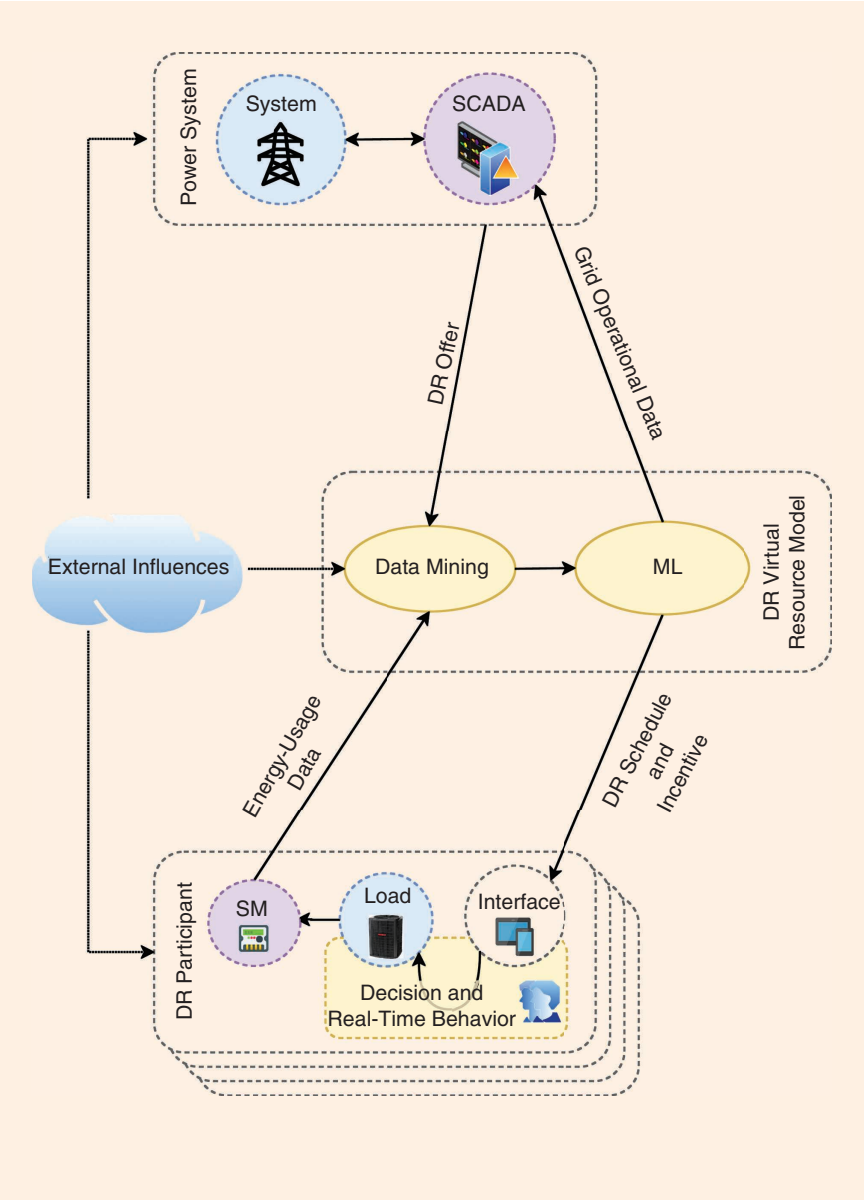

Figure 3. An ML-enabled DR program.

The objective of the DR operator will significantly influence the requirements on the virtual DR resource model and, thus, on the choice of ML methods. For example, a utility-operated DR program is mainly driven by reliability and efficiency considerations, and the utility is primarily interested in mapping incentive and control signals for reliable load reductions. On one hand, in the absence of a two-way communication infrastructure, optimal DR pricing can be achieved via online learning (also called *dynamic pricing*) approaches. An example of the online learning process is presented in Figure 4 and further described in the "Online Learning Processes" section. On the other hand, the DR programs operated by commercial third-party DR aggregators that sell flexibility-related ancillary services to utilities require a more profound understanding of flexibility sources and customer preferences. To reduce their financial risk and to enroll DR customers, they must develop long-term incentive strategies that

motivate reliable DR participation and broadcast control signals that fit customer preferences and ensure commitment to the program. In this context, ML methods based on Markov decision processes (MDPs) can attain a physics-informed state estimation of the DR resource and estimate the flexibility range compatible with the individual comfort zones of DR customers. An example of the MDP process for the aggregation of smart TCLs is displayed in Figure 5 and further described in the "MDPs" section.

Online Learning Processes

The online learning approach, as displayed in Figure 4, seeks to continuously improve incentive (price) signals for DR participation by tuning the pricing policy based on the observed responses. Such a dynamic pricing process models the available DR capacity (i.e., willingness of participants to deviate from their demand pattern) as a function of the broadcast price signal. At each DR period t, the DR operator broadcasts pricing signal $\lambda_{i,t}$, which is customized for each DR participant indexed as i, to all DR resources. Based on this pricing signal, every DR participant i will decide on their real-time electricity usage, $x_{i,t}$, by means of using an automated energy-management system or manual adjustments. The operator then observes usage, $x_{i,t}$, and uses the new price-quantity data-point, $\{\lambda_{i,t}, x_{i,t}\}$, to update the set of historical observations, $H_{i,t}$, obtained from each participant i. An ML algorithm then extracts parameters $\beta_{i,t}$ from $H_{i,t}$, which define a functional relationship, $x = f(\lambda, \beta_{i,t})$, between price signal λ and the load reduction x of customer i. Function $f(\lambda, \beta_{i,t})$ then informs the DR operator's optimal pricing decision, $\lambda_{i,t+1}$, at the next DR period, $t+1$.

Notably, there is no commitment or negotiation in the online learning process in Figure 4, and the learning process resembles a closed-loop feedback process. Due to the idiosyncratic behavior of DR participants, (linear) regression approaches have been shown to capture the price sensitivity of DR participants with a relatively high accuracy. However, such methods must be adapted to avoid the incomplete learning caused by the closed-loop feedback. Incomplete learning can occur if the decision-making process neglects its own influence on future parameter learning. For example, if the price signals broadcasted to a customer are all very similar, the price-sensitivity estimation will only be accurate in the limited interval of previous pricing signals. This might lead to a systematic error in

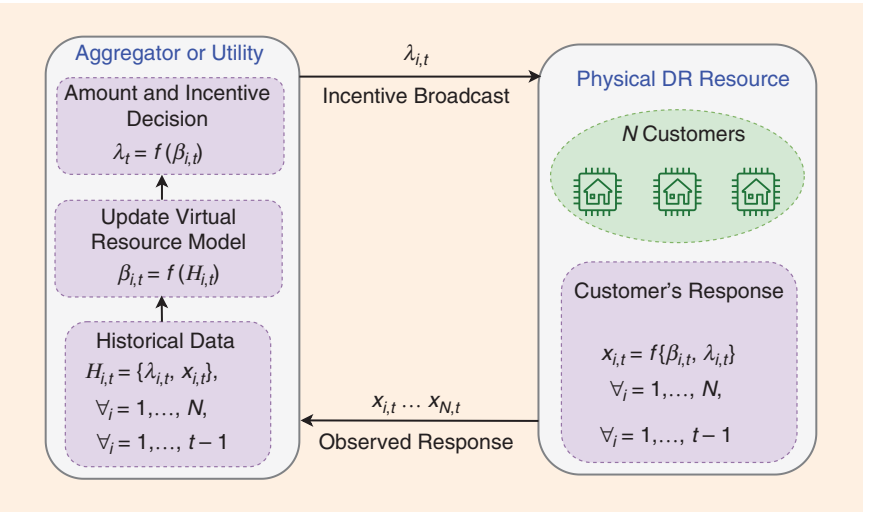

Figure 4. An online learning process for a virtual DR resource.

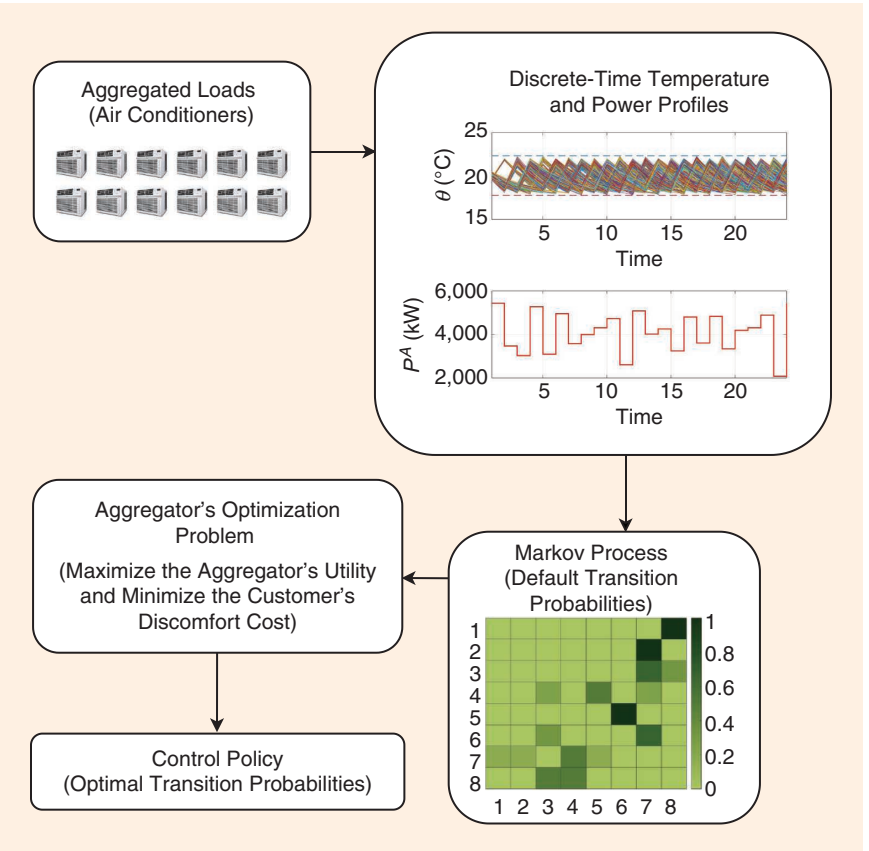

Figure 5. A summary of the MDP approach.

estimating the DR capacity of a given DR resource over a larger interval and, in turn, cause the algorithm to avoid sending more diverse pricing signals. This example illustrates that an efficient ML algorithm for DR scheduling must not only be cognizant of the immediate value of the DR program but must also internalize the value of a more-accurately trained model in the future.

Weighing an immediate present value against a future value from improved models is known as the tradeoff between exploitation and exploration. The rationale behind exploration strategies is to sacrifice some optimality in the decision-making process of the current DR period to gather information on newly enrolled DR participants or to probe the reactions of DR participants to increase or lower incentive signals. Carefully tuned explorative disturbances in the pricing policy will improve the diversity and quality of the gathered data and, thus, its future exploitation. Necessary deviations from the optimal "here-and-now" pricing can be 1) purely random disturbances with a decreasing magnitude as the learning progresses (perturbation policy), 2) drawn from prior distributions that are adjusted based on the observed ex-post statistics (bandit or sampling heuristics), or 3) related to marginal values obtained from optimizing a physical system to determine the cost of suboptimal decisions.

MDPs

The successful real-world implementation of residential DR programs in distribution grids requires effective modeling techniques to control aggregated DR resources in a network-constrained environment. The MDP methodology provides an efficient framework capable of providing such solution techniques. MDP methods are suitable for modeling decision making processes in situations where outcomes are partly random (e.g., weather, appliances operated by residents) and partly under the control of a decision maker (e.g., change HVAC settings, switch on/off lights). To assess the flexibility of the aggregated DR resources, a Markov process (MP) is developed to represent their aggregated energy consumption or temperature levels. Based on the developed MP, an MDP is formulated that can, in turn, be used to optimally control DR resources, either by the local utility or third-party aggregators. The MDP approach is summarized in Figure 5, where continuous-time measurements (temperature and power) of aggregated loads are considered. These measurements are then discretized into predefined states that form a default transition matrix representing an MP. The aggregators or local utilities then solve their optimization problem to maximize their utility and minimize any discomfort costs to which DR participants are subjected. This optimization problem results in optimal transition probabilities defining the optimal-control policy for the DR program.

The MDP theory is also well-suited to account for model and parameter uncertainty arising from the inability to accurately estimate the transition probabilities of the MP observed by utilities, third-party providers, and customers. This uncertainty arising from the inability to accurately estimate the transition probabilities of the MP can significantly distort MDP solutions and, hence, the optimal-control policy. One possible way to account for the uncertain dynamics is to parametrize them using stochastic and robust optimization methods. The MDP framework internalizes the parameter uncertainty and provides uncertainty-aware stochastic and robust optimal-control policies. Another approach to deal with uncertain customer dynamics is to utilize model-free reinforcement-learning techniques, such as Q- and Z-learning methods, to learn the default transition probabilities. This learning process is robust against the uncertainty that arises from estimating the dynamics of the aggregated DR resources and helps bridge the gap between the real environment and its model.

Security Assessment

This section outlines the cybersecurity issues arising in DR programs, as presented in Figures 1 and 3. We discuss the security of DR programs in terms of the following features:

1) *Confidentiality*: This refers to the unauthorized acquisition and dissemination of information. The acquisition of granular data on customer-end energy usage via SMs is an integral part of the DR program (see Figures 1 and 3). The energy-usage data can be leveraged by adversaries to reveal customer-end sensitive information and routines, e.g., house occupancy and well-being. Also, the energy-usage data can be breached at various stages of the DR. For example, adversaries can exploit vulnerabilities in the SMs, communication channel between the utility/aggregator and customers, and DRAS server.

   Similarly, DR schedules sent by the utility/aggregator and the response of the customers to DR calls extends the attack surfaces of smartphones used for communication. For example, adversaries can compromise a smartphone application for DR programs and enable remote attacks. Smartphones have been increasingly used for remotely controlling residential IoT devices (e.g., controlling the room temperature via smart thermostats when not at home). This feature also increases an attack surface as smartphones, SMs, and other home IoT devices share the same trusted connectivity.
2) *Integrity*: This indicates the unauthorized alteration or destruction of data or a process. The core of the DR program is a consensual exchange of DR schedules, SM data, and customer-end response to DR calls between the utility/aggregator and customers. As explained in "The DR Process" section, DR schedules include DR incentives, time, duration, and capacity. Similarly, customer-end responses include accepting/

rejecting DR calls or committing the DR capacity. Tampering with this information can have severe effects on the effectiveness of the DR program and power grid operation. For example, false data injection attacks (FDIAs) on the information sent to customers inherently forces them to make suboptimal decisions on how to use their appliances. Similarly, FDIAs on the information sent to the utility/aggregator (e.g., accepting/rejecting the DR calls, SMs data) misinforms them and, hence, forces their DR scheduling routines and algorithm to produce erroneous dispatch decisions. These attacks are considered as causative attacks on decision-support and learning schemes employed by the utility/aggregator. Such false DR schedules and customer-end responses can incur operational challenges, such as frequency and voltage excursions, and increase the system operating cost due to a mismatch between the committed DR capacity and the DR capacity provided in real time.

3) *Availability*: This implies that any authorized entity is deprived of reliable and timely access to services and information. The effectiveness of DR programs relies on the uninterrupted and timely exchange of information between the utility/aggregator and customers. In turn, disrupting this information exchange by exploiting customer-end devices (such as SMs and smartphones), the communication channel between the utility/aggregator and customers, and the DRAS server can damage the efficacy of the DR program. For example, denial-of-service (DoS) attacks on SM data or on the responses of customers to DR calls can inject erroneous values into the training data used by the learning algorithm deployed by the utility/aggregator. This attack misleads the algorithm to design suboptimal DR schedules. Similarly, DoS attacks on DR schedules, DRAS servers, or VENs preclude DR customers from participating in DR calls. This may, in turn, undermine the trustworthiness of the DR program deployed by the utility/aggregator.

The ability of adversaries to compromise customer-end devices, such as SMs and smartphones, utility/aggregator DRAS, and DR communication channels, has been greatly aided by the automation of DR programs and by a lack of standardization of these programs across the industry. For example, there is no internationally (or, in the case of the United States, interstate) accepted DR communication protocol. Although some protocols (e.g., OpenADR 2.0) have recently gained acceptance, they are still not recognized at the regulatory level. The OpenADR 2.0 protocol authenticates, encrypts, and digitally signs the DR information exchanged between the two parties. Although utilities use the OpenADR protocol, the aggregator may use a proprietary communication protocol whose security remains undetermined.

Recently, blockchain techniques have been validated as promising solutions to avoiding centralized authentication and data storage. The use of blockchain schemes inherently increases the security and privacy of DR customers by means of: 1) a trustless decentralized network, 2) immutability, and 3) network consensus. Unlike the centralized security authority, each blockchain is managed by an anonymized decentralized node (SMs or VENs in DR) that verifies the authenticity of new nodes and data using network consensus. Furthermore, blockchains maintain a timestamped and hashed list of data. For example, SM data can be saved and communicated in blocks with a hash that depends on previous blocks. This hashing increases the difficulty for an attacker to tamper with data. This feature will allow SMs to authenticate themselves and encrypt data without the use of DRAS. Although blockchains have more-robust security features compared to centralized security mechanisms, they suffer from cryptojacking—where adversaries can access unauthorized computations across blockchain nodes—thwarting genuine transactions and leading to system failures.

Even with standard security mechanisms, such as OpenADR and decentralized blockchain deployed by the utility and aggregator, DR security ultimately hinges on the cyberhygiene of DR customers. This is particularly concerning as many customers are either unaware of the needed security measures (e.g., strong passwords and multifactor authentication for their IoT devices and applications) or cannot afford these security measures (e.g., SMs and BEMS with a high computation power for industry-grade encryption).

Given these cyber vulnerabilities and proven attack mechanisms, ML algorithms, such as online or the Q/Z-learning discussed in the "Online Learning Processes" and "MDPs" sections, respectively, can improve the security of DR programs. For example, the online learning algorithm executed on the DRAS updates the incentive signals sent to DR participants during a real-time DR event. Unlike an offline approach, where all of the historical data are used to analyze the sensitivity of the DR customer to a price signal during a given DR event, the online counterpart only uses current DR event data. This bounds the effect of integrity attacks on training data. Similarly, Q/Z-learning can return probabilistic estimates on the DR participant's power curtailment, given historical DR incentives and operating conditions, such as the temperature for ACs, without necessarily monitoring SM data in every DR event. Unlike conventional DR approaches, where SM data are the backbone, ML algorithms, such as conditional kernel density forecast, learn the customer-end energy usage without requiring (or at least reducing) the SM measurement, which reduces data dependency and, thus, an attack surface. Furthermore, customer-end responses sent to the utility/aggregator can also be estimated based on their historical responses. Although these techniques decrease the attack surface arising from a lack of customer-end cyberhygiene, they are not a panacea.

Conclusion

Recent advances in communication and information technologies enable new ways and means of enrolling residential resources into DR programs. However, real-world deployments of these technologies are still limited due to their relatively high capital costs, cybersecurity concerns, and inability to continuously and seamlessly engage with a large number of customers. Thus, DR programs must overcome these limitations, which hinges on designing incentive mechanisms and scheduling routines that account for these limitations while co-optimizing available DR capacity, cost, and reliability. Commonly, the small-scale, distributed, stochastic, and heterogeneous nature of residential DR resources complicates these routines.

However, data mining and ML methods make it possible for DR operators to abstract out specific features of individual DR resources by means of creating virtual DR resources that describe a functional relationship among the characteristics of individual DR resources and their ensembles, which streamlines decision making. In turn, the usefulness of various data mining and ML approaches depends on the objective of the DR program and the structure of the ensemble.

Thus, on one hand, utility-operated DR programs seek to establish a reliable relationship between passive control (e.g., price signals) and the resulting aggregated behavior of the DR ensemble. Online learning methods based on Bayesian statistics or regression models can, therefore, be used to tune price signals, using historical and real-time observations to achieve the desirable behavior of DR resources. On the other hand, profit-seeking, third-party aggregators are more interested in selling flexible capacity to the utility as a service. Under this objective, data mining and ensemble control based on the MDP framework can be used to robustly quantify the amount of available flexibility in a given DR ensemble, with minimal data requirements and violations of the comfort preferences of DR customers.

Regardless of their ultimate objective, any DR program must maintain stringent requirements on its cybersecurity, i.e., to ensure and constantly verify system confidentiality, integrity, and availability. While data mining and ML algorithms are generally compliant with DR cybersecurity requirements and often reduce data and communication overheads, they may also enable new entry points for causative attacks that inject manipulated data and disrupt DR system operations. Thus, effective residential DR programs have to comprehensively and continuously evaluate their always-changing cybersecurity landscape to take preventive actions for securing their customers and the power system's integrity.

For Further Reading

J. L. Mathieu, P. N. Price, S. Kiliccote, and M. A. Piette, "Quantifying changes in building electricity use, with application to demand response," *IEEE Trans. Smart Grid*, vol. 2, no. 3, pp. 507–518, 2011. doi: 10.1109/TSG.2011.2145010.

J.-H. Kim and A. Shcherbakova, "Common failures of demand response," *Energy*, vol. 36, no. 2, pp. 873–880, 2011. doi: 10.1016/j.energy.2010.12.027.

J. A. Taylor and J. L. Mathieu, "Index policies for demand response," *IEEE Trans. Power Syst.*, vol. 29, no. 3, pp. 1287–1295, 2013. doi: 10.1109/TPWRS.2013.2289972.

S. Nolan and M. O'Malley, "Challenges and barriers to demand response deployment and evaluation," *Appl. Energy*, vol. 152, pp. 1–10, Aug. 2015. doi: 10.1016/j.apenergy.2015.04.083.

S. Arora and J. W. Taylor, "Forecasting electricity smart meter data using conditional kernel density estimation," *Omega*, vol. 59, pp. 47–59, Mar. 2016. doi: 10.1016/j.omega.2014.08.008.

K. Khezeli and E. Bitar, "Risk-sensitive learning and pricing for demand response," *IEEE Trans. Smart Grid*, vol. 9, no. 6, pp. 6000–6007, 2017. doi: 10.1109/TSG.2017.2700458.

S. Mehrdad, S. Mousavian, G. Madraki, and Y. Dvorkin, "Cyber-physical resilience of electrical power systems against malicious attacks: A review," *Current Sustain./Renewable Energy Rep.*, vol. 5, no. 1, pp. 14–22, 2018. doi: 10.1007/s40518-018-0094-8]

R. Mieth and Y. Dvorkin, "Online learning for network constrained demand response pricing in distribution systems," *IEEE Trans. Smart Grid*, vol. 11, no. 3, pp. 2563–2575, 2019. doi: 10.1109/TSG.2019.2957705.

N. Tucker, A. Moradipari, and M. Alizadeh, "Constrained Thompson sampling for real-time electricity pricing with grid reliability constraints," *IEEE Trans. Smart Grid*, vol. 11, no. 6, pp. 4971–4983, 2020. doi: 10.1109/TSG.2020.3004770.

A. Hassan, S. Acharya, M. Chertkov, D. Deka, and Y. Dvorkin, "A hierarchical approach to multienergy demand response: From electricity to multienergy applications," *Proc. IEEE*, vol. 108, no. 9, pp. 1457–1474, 2020. doi: 10.1109/JPROC.2020.2983388.

A. Hassan, R. Mieth, D. Deka, and Y. Dvorkin, "Stochastic and distributionally robust load ensemble control," *IEEE Trans. Power Syst.*, vol. 35, no. 6, pp. 4678–4688, 2020. doi: 10.1109/TPWRS.2020.2992268.

A. Hassan, D. Deka, M. Chertkov, and Y. Dvorkin, "Data-driven learning and load ensemble control," *Elect. Power Syst. Res.*, vol. 189, Apr. 2020, Art. no. 106780. doi: 10.1016/j.epsr.2020.106780.

S. Acharya, Y. Dvorkin, H. Pandžić, and R. Karri, "Cybersecurity of smart electric vehicle charging: A power grid perspective," *IEEE Access*, vol. 8, p. 1, 2020. doi: 10.1109/ACCESS.2020.3041074.

Biographies

Robert Mieth (robert.mieth@nyu.edu) is with the Department of Electrical and Computer Engineering, New York University, New York, USA.

Samrat Acharya (samrat.acharya@nyu.edu) is with the Department of Electrical and Computer Engineering and Center for Cybersecurity, New York University, New York, USA.

Ali Hassan (ah3909@nyu.edu) is with the Department of Electrical and Computer Engineering, New York University, New York, USA.

Yury Dvorkin (dvorkin@nyu.edu) is with the Department of Electrical and Computer Engineering and Center for Urban Science and Progress, New York University, New York, USA.